PATENT APPLICATION TRANSMITTAL LETTER (Large Entity)	Docket No. 67539/622

COMMISSIONER FOR PATENTS

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:
BROWN, Daniel R.L. and VANSTONE, Scott A.

For: **ELLIPTIC CURVE RANDOM NUMBER GENERATION**

Enclosed are:

- ☐ Certificate of Mailing by Express Mail Label No.
- ☒ 6 (six) sheets of drawings.
- ☐ A certified copy of a application.
- ☒ Declaration ☐ Signed. ☒ Unsigned.
- ☒ Power of Attorney
- ☐ Information Disclosure Statement
- ☐ Preliminary Amendment
- ☐ Other:

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra		Rate	Fee
Total Claims	19	- 20 =	0	x	$50.00	$0.00
Indep. Claims	4	- 3 =	1	x	$200.00	$200.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
Total # of Pages in Specification		15	Total # of Drawing Sheets		6	
Total # of Pages	21				Application Size Fee	$0.00
					Search Fee	$500.00
					Examination Fee	$200.00
					Basic Fee	$300.00
					TOTAL FILING FEE	$1,200.00

- ☐ A check in the amount of to cover the filing fee is enclosed.
- ☒ The Director is hereby authorized to charge and credit Deposit Account 02-2553 as described below.
  - ☒ Charge the amount of $1,200.00 as filing fee.
  - ☒ Credit any overpayment.
  - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
  - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Dated: January 23, 2006

Signature

John R. S. Orange Reg. No. 29,725
Blake, Cassels & Graydon LLP
199 Bay Street, Commerce Court West, Suite 2800
P.O. Box 25
Toronto, Ontario, M5L 1A9
Canada

Customer Number: 27871

cc:

☐ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

PATENT APPLICATION TRANSMITTAL LETTER (Large Entity)	Docket No. 67539/622

COMMISSIONER FOR PATENTS

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:
BROWN, Daniel R.L. and VANSTONE, Scott A.

For: **ELLIPTIC CURVE RANDOM NUMBER GENERATION**

Enclosed are:

- ☐ Certificate of Mailing by Express Mail Label No.
- ☒ 6 (six) sheets of drawings.
- ☐ A certified copy of a application.
- ☒ Declaration ☐ Signed. ☒ Unsigned.
- ☒ Power of Attorney
- ☐ Information Disclosure Statement
- ☐ Preliminary Amendment
- ☐ Other:

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra		Rate	Fee
Total Claims	19	- 20 =	0	x	$50.00	$0.00
Indep. Claims	4	- 3 =	1	x	$200.00	$200.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
Total # of Pages in Specification		15	Total # of Drawing Sheets		6	
Total # of Pages	21				Application Size Fee	$0.00
					Search Fee	$500.00
					Examination Fee	$200.00
					Basic Fee	$300.00
					TOTAL FILING FEE	$1,200.00

- ☐ A check in the amount of to cover the filing fee is enclosed.
- ☒ The Director is hereby authorized to charge and credit Deposit Account 02-2553 as described below.
  - ☒ Charge the amount of $1,200.00 as filing fee.
  - ☒ Credit any overpayment.
  - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
  - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Dated: January 23, 2006

Signature

John R. S. Orange Reg. No. 29,725
Blake, Cassels & Graydon LLP
199 Bay Street, Commerce Court West, Suite 2800
P.O. Box 25
Toronto, Ontario, M5L 1A9
Canada

Customer Number: 27871

cc:

☐ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

ELLIPTIC CURVE RANDOM NUMBER GENERATION

[0001] This application claims priority from United States Provisional Patent Application No. 60/644,982 filed on January 21, 2005.

FIELD OF THE INVENTION:

[0002] The present invention relates to systems and methods for cryptographic random number generation.

DESCRIPTION OF THE PRIOR ART

[0003] Random numbers are utilised in many cryptographic operations to provide underlying security. In public key infrastructures, for example, the private key of a key pair is generated by a random number generator and the corresponding public key mathematically derived therefrom. A new key pair may be generated for each session and the randomness of the generator therefore is critical to the security of the cryptographic system.

[0004] To provide a secure source of random numbers, cryptographically secure pseudorandom bit generators have been developed in which the security of each generator relies on a presumed intractability of the underlying number-theoretical problem. The American National Standards Institute (ANSI) has set up an Accredited Standards Committee (ASC) X9 for the financial services industry, which is preparing a American National Standard (ANS) X9.82 for cryptographic random number generation (RNG). One of the RNG methods in the draft of X9.82, called Dual_EC_DRBG, uses elliptic curve cryptography (ECC) for its security. Dual_EC_DRBG will hereinafter be referred to as elliptic curve random number generation (ECRNG).

[0005] Elliptic curve cryptography relies on the intractability of the discrete log problem in cyclic subgroups of elliptic curve groups. An elliptic curve E is the set of points (x, y) that satisfy the defining equation of the elliptic curve. The defining equation is a cubic equation, and is non-

singular. The coordinates x and y are elements of a field, which is a set of elements that can be added, subtracted and divided, with the exception of zero. Examples of fields include rational numbers and real numbers. There are also finite fields, which are the fields most often used in cryptography. An example of a finite field is the set of integers modulo a prime q.

[0006] Without the loss of generality, the defining equation of the elliptic curve can be in the Weierstrass form, which depends on the field of the coordinates. When the field F is integers modulo a prime $q > 3$, then the Weierstrass equation takes the form $y^2 = x^3 + ax + b$, where a and b are elements of the field F.

[0007] The elliptic curve E includes the points (x, y) and one further point, namely the point O at infinity. The elliptic curve E also has a group structure, which means that the two points P and Q on the curve can be added to form a third point $P + Q$. The point O is the identity of the group, meaning $P + O = O + P = P$, for all points P. Addition is associative, so that $P + (Q + R) = (P + Q) + R$, and commutative, so that $P + Q = Q + R$, for all points P, Q and R. Each point P has a negative point $-P$, such that $P + (-P) = O$. When the curve equation is the Weierstrass equation of the form $y^2 = x^3 + ax + b$, the negative of $P = (x, y)$ is determined easily as $-P = (x, -y)$. The formula for adding points P and Q in terms of their coordinates is only moderately complicated involving just a handful of field operations.

[0008] The ECRNG uses as input two elliptic curve points P and Q that are fixed. These points are not assumed to be secret. Typically, P is the standard generator of the elliptic curve domain parameters, and Q is some other point. In addition a secret seed is inserted into the ECRNG.

[0009] The ECRNG has a state, which may be considered to be an integer s. The state s is updated every time the ECRNG produces an output. The updated state is computed as $u = z(sP)$, where $z()$ is a function that converts an elliptic curve point to an integer. Generally, z consists of taking the x-coordinate of the point, and then converting the resulting field element to an integer. Thus u will typically be an integer derived from the x-coordinate of the point s.

[0010] The output of the ECRNG is computed as follows: $r = t(z(sQ))$, where t is a truncation function. Generally the truncation function removes the leftmost bits of its input. In the ECRNG, the number of bits truncated depends on the choice of elliptic curve, and typically may be in the range of 6 to 19 bits.

[0011] Although P and Q are known, it is believed that the output r is random and cannot be predicted. Therefore successive values will have no relationship that can be exploited to obtain private keys and break the cryptographic functions. The applicant has recognised that anybody who knows an integer d such that $Q = dP$, can deduce an integer e such that $ed = 1 \bmod n$, where n is the order of G, and thereby have an integer e such that $P = eQ$. Suppose $U = sP$ and $R = sQ$, which are the precursors to the updated state and the ECRNG output. With the integer e, one can compute U from R as $U = eR$. Therefore, the output $r = t(z(R))$, and possible values of R can be determined from r. The truncation function means that the truncated bits of R would have to be guessed. The z function means that only the x-coordinate is available, so that decompression would have to be applied to obtain the full point R. In the case of the ECRNG, there would be somewhere between about $2^6 = 64$ and 2^{19} (i.e. about half a million) possible points R which correspond to r, with the exact number depending on the curve and the specific value of r.

[0012] The full set of R values is easy to determine from r, and as noted above, determination of the correct value for R determines $U = eR$, if one knows e. The updated state is $u = z(U)$, so it can be determined from the correct value of R. Therefore knowledge of r and e allows one to determine the next state to within a number of possibilities somewhere between 2^6 and 2^{19}. This uncertainty will invariably be eliminated once another output is observed, whether directly or indirectly through a one-way function.

[0013] Once the next state is determined, all future states of ECRNG can be determined because the ECRNG is a deterministic function. (at least unless additional random entropy is fed into the ECRNG state) All outputs of the ECRNG are determined from the determined states of the ECRNG. Therefore knowledge of r and e, allows one to determine all future outputs of the ECRNG.

[0014] It has therefore been identified by the applicant that this method potentially possesses a trapdoor, whereby standardizers or implementers of the algorithm may possess a piece of information with which they can use a single output and an instantiation of the RNG to determine all future states and output of the RNG, thereby completely compromising its security. It is therefore an object of the present invention to obviate or mitigate the above mentioned disadvantages.

SUMMARY OF THE INVENTION

[0015] In one aspect, the present invention provides a method for computing a verifiably random point Q for use with another point P in an elliptic curve random number generator comprising computing a hash including the point P as an input, and deriving the point Q from the hash.

[0016] In another aspect, the present invention provides a method for producing an elliptic curve random number comprising generating an output using an elliptic curve random number generator, and truncating the output to generate the random number.

[0017] In yet another aspect, the present invention provides a method for producing an elliptic curve random number comprising generating an output using an elliptic curve random number generator, and applying the output to a one-way function to generate the random number.

[0018] In yet another aspect, the present invention provides a method of backup functionality for an elliptic curve random number generator, the method comprising the steps of computing an escrow key e upon determination of a point Q of the elliptic curve, whereby $P = eQ$, P being another point of the elliptic curve; instituting an administrator, and having the administrator store the escrow key e; having members with an elliptic curve random number generator send to the administrator, an output r generated before an output value of the generator; the administrator logging the output r for future determination of the state of the generator.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] An embodiment of the invention will now be described by way of example only with reference to the appended drawings wherein:

[0020] Figure 1 is a schematic representation of a cryptographic random number generation scheme.

[0021] Figure 2 is a flow chart illustrating a selection process for choosing elliptic curve points.

[0022] Figure 3 is a block diagram, similar to figure 1 showing a further embodiment

[0023] Figure 4 is flow chart illustrating the process implemented by the apparatus of Figure 3.

[0024] Figure 5 is a block diagram showing a further embodiment.

[0025] Figure 6 is a flow chart illustrating yet another embodiment of the process of Figure 2.

[0026] Figure 7 is schematic representation of an administrated cryptographic random number generation scheme.

[0027] Figure 8 is a flow chart illustrating an escrow key selection process.

[0028] Figure 9 is a flow chart illustrating a method for securely utilizing an escrow key.

DETAILED DESCRIPTION OF THE INVENTION

[0029] Referring therefore to Figure 1, a cryptographic random number generator (ECRNG) 10 includes an arithmetic unit 12 for performing elliptic curve computations. The ECRNG also includes a secure register 14 to retain a state value s and has a pair of inputs 16, 18 to receive a

pair of initialisation points P, Q. The points P, Q are elliptic curve points that are assumed to be known. An output 20 is provided for communication of the random integer to a cryptographic module 22. The initial contents of the register 14 are provided by a seed input S.

[0030] This input 16 representing the point P is in a first embodiment, selected from a known value published as suitable for such use.

[0031] The input 18 is obtained from the output of a one way function in the form of a hash function 24 typically a cryptographically secure hash function such as SHA1 or SHA2 that receives as inputs the point P. The function 24 operates upon an arbitrary bit string A to produce a hashed output 26. The output 26 is applied to arithmetic unit 12 for further processing to provide the input Q.

[0032] In operation, the ECRNG receives a bit string as a seed, which is stored in the register 14. The seed is maintained secret and is selected to meet pre-established cryptographic criteria, such as randomness and Hamming weight, the criteria being chosen to suit the particular application.

[0033] In order to ensure that d is not likely to be known (e.g. such that $P = dQ$, and $ed = 1 \mod n$); one or both of the inputs 16, 18 is chosen so as to be verifiably random. In the embodiment of Figure 1, Q is chosen in a way that is verifiably random by deriving it from the output of a hash-function 24 (preferably one-way) whose input includes the point P. As shown in Figure 2 an arbitrary string A is selected at step 202, a hash H of A is computed at step 204 with P and optionally S as inputs to a hash-based function $F_H()$, and the hash H is then converted by the arithmetic unit 12 to a field element X of a desired field F at step 206. P may be pre-computed or fixed, or may also be chosen to be a verifiably random chosen value. The field element X is regarded as the x-coordinate of Q (thus a "compressed" representation of Q). The x-coordinate is then tested for validity on the desired elliptic curve E at step 208, and whether or not X is valid, is determined at step 210. If valid, the x-coordinate provided by element X is decompressed to provide point Q at step 212. The choice of which of two possible values of the y co-ordinate is generally derived from the hash value.

[0034] The points P and Q are applied at respective inputs 16, 18 and the arithmetic unit 12 computes the point sQ where s is the current value stored in the register 14. The arithmetic unit 12 converts the x-coordinate of the point (in this example point sQ) to an integer and truncates the value to obtain $r = t(z(sQ))$. The truncated value r is provided to the output 20.

[0035] The arithmetic unit 12 similarly computes a value to update the register 14 by computing sP, where s is the value of the register 14, and converting the x-coordinate of the point sP to an integer u. The integer u is stored in the register to replace s for the next iteration. {ditto above}

[0036] As noted above, the point P may also be verifiably random, but may also be an established or fixed value. Therefore, the embodiment of Figure 1 may be applied or retrofitted to systems where certain base points (e.g. P) are already implemented in hardware. Typically, the base point P will be some already existing base point, such as those recommended in Federal Information Processing Standard (FIPS) 186-2. In such cases, P is not chosen to be verifiably random.

[0037] In general, inclusion of the point P in the input to the hash function ensures that P was determined before Q is determined, by virtue of the one-way property of the hash function and since Q is derived from an already determined P. Because P was determined before Q, it is clearly understood that P could not have been chosen as a multiple of Q (e.g. where $P = eQ$), and therefore finding d is generally as hard as solving a random case of the discrete logarithm problem.

[0038] Thus, having a seed value S provided and a hash-based function $F()$ provided, a verifier can determine that $Q = F(S,P)$, where P may or may not be verifiably random. Similarly, one could compute $P = F(S,Q)$ with the same effect, though it is presumed that this is not necessary given that the value of P in the early drafts of X9.82 were identical to the base points specified in FIPS 186-2.

[0039] The generation of Q from a bit string as outlined above may be performed externally of the ECRNG 10, or, preferably, internally using the arithmetic unit 12. Where both P and Q

are required to be verifiably random, a second hash function 24 shown in ghosted outline in Figure 1 is incorporated to generate the coordinate of point P from the bit string A. By providing a hash function for at least one of the inputs, a verifiably random input is obtained.

[0040] It will also be noted that the output generated is derived from the x coordinate of the point sP. Accordingly, the inputs 16, 18 may be the x coordinates of P and Q and the corresponding values of sP and sQ obtained by using Montgomery multiplication techniques thereby obviating the need for recovery of the y coordinates.

[0041] An alternative method for choosing Q is to choose Q in some canonical form, such that its bit representation contains some string that would be difficult to produce by generating $Q = dP$ for some known d and P for example a representation of a name. It will be appreciated that intermediate forms between this method and the preferred method may also exist, where Q is partly canonical and partly derived verifiably at random. Such selection of Q, whether verifiably random, canonical, or some intermediate, can be called verifiable.

[0042] Another alternative method for preventing a key escrow attack on the output of an ECRNG, shown in Figures 3 and 4 is to add a truncation function 28 to ECRNG 10 to truncate the ECRNG output to approximately half the length of a compressed elliptic curve point. Preferably, this operation is done in addition to the preferred method of Figure 1 and 2, however, it will be appreciated that it may be performed as a primary measure for preventing a key escrow attack. The benefit of truncation is that the list of R values associated with a single ECRNG output r is typically infeasible to search. For example, for a 160-bit elliptic curve group, the number of potential points R in the list is about 2^{80}, and searching the list would be about as hard as solving the discrete logarithm problem. The cost of this method is that the ECRNG is made half as efficient, because the output length is effectively halved.

[0043] Yet another alternative method shown in Figure 5 and 6 comprises filtering the output of the ECRNG through another one-way function F_{H2},, identified as 34, such as a hash function to generate a new output. Again, preferably, this operation is performed in addition to the preferred method shown in Figure 2, however may be performed as a primary measure to prevent key escrow attacks. The extra hash is relatively cheap compared to the elliptic curve operations

performed in the arithmetic unit 12, and does not significantly diminish the security of the ECRNG.

[0044] As discussed above, to effectively prevent the existence of escrow keys, a verifiably random Q should be accompanied with either a verifiably random P or a pre-established P. A pre-established P may be a point P that has been widely publicized and accepted to have been selected before the notion of the ECRNG 12, which consequently means that P could not have been chosen as $P = eQ$ because Q was not created at the time when P was established.

[0045] Whilst the above techniques ensure the security of the system using the ECRNG by "closing" the trap door, it is also possible to take advantage of the possible interdependence of P and Q, namely where $P = eQ$, through careful use of the existence of e.

[0046] In such a scenario, the value e may be regarded as an escrow key. If P and Q are established in a security domain controlled by an administrator, and the entity who generates Q for the domain does so with knowledge of e (or indirectly via knowledge of d). The administrator will have an escrow key for every ECRNG that follows that standard.

[0047] Escrow keys are known to have advantages in some contexts. They can provide a backup functionality. If a cryptographic key is lost, then data encrypted under that key is also lost. However, encryption keys are generally the output of random number generators. Therefore, if the ECRNG is used to generate the encryption key K, then it may be possible that the escrow key e can be used to recover the encryption key K. Escrow keys can provide other functionality, such as for use in a wiretap. In this case, trusted law enforcement agents may need to decrypt encrypted traffic of criminals, and to do this they may want to be able to use an escrow key to recover an encryption key.

[0048] Figure 7 shows a domain 40 having a number of ECRNG's 10 each associated with a respective member of the domain 40. The domain 40 communicates with other domains 40a, 40b, 40c through a network 42, such as the internet. Each ECRNG of a domain has a pair of identical inputs P,Q. The domain 40 includes an administrator 44 who maintains in a secure manner an escrow key e.

[0049] The administrator 44 chooses the values of P and Q such that he knows an escrow key e such that $Q = eP$. Other members of the domain 40 use the values of P and Q, thereby giving the administrator 44 an escrow key e that works for all the members of the organization.

[0050] This is most useful in its backup functionality for protecting against the loss of encryption keys. Escrow keys e could also be made member-specific so that each member has its own escrow e' from points selected by the administrator 44.

[0051] As generally denoted as numeral 400 in Figure 8, the administrator initially selects a point P which will generally be chosen as the standard generator P for the desired elliptic curve 402. The administrator then selects a value d and the point Q will be determined as $Q = dP$ 404, for some random integer d of appropriate size. The escrow key e is computed as $e = d^{-1} \bmod n$ 406, where n is the order of the generator P and stored by the administrator.

[0052] The secure use of such an escrow key 34e is generally denoted by numeral 500 and illustrated in Figure 9. The administrator 44 is first instituted 502 and an escrow keys e would be chosen and stored 504 by the administrator44

[0053] In order for the escrow key to function with full effectiveness, the escrow administrator 44 needs direct access to an ECRNG output value r that was generated before the ECRNG output value k (i.e. 16) which is to be recovered. It is not sufficient to have indirect access to r via a one-way function or an encryption algorithm. A formalized way to achieve this is to have each member with an ECRNG 12 communicate with the administrator 44 as indicated at 46 in figure 7. and step 506 in figure 9. This may be most useful for encrypted file storage systems or encrypted email accounts. A more seamless method may be applied for cryptographic applications. For example, in the SSL and TLS protocols, which are used for securing web (HTTP) traffic, a client and server perform a handshake in which their first actions are to exchange random values sent in the clear.

[0054] Many other protocols exchange such random values, often called nonces. If the escrow administrator observes these nonces, and keeps a log of them 508, then later it may be able to determine the necessary r value. This allows the administrator to determine the

subsequent state of the ECRNG 12 of the client or server 510 (whoever is a member of the domain), and thereby recover the subsequent ECRNG 12 values. In particular, for the client who generally generates a random pre-master secret from which is derived the encryption key for the SSL or TLS session, the escrow key may allow recovery of the session key. Recovery of the session key allows recovery of the whole SSL or TLS session.

[0055] If the session was logged, then it may be recovered. This does not compromise long-term private keys, just session keys obtained from the output of the ECRNG, which should alleviate any concern regarding general suspicions related to escrows.

[0056] Whilst escrow keys are also known to have disadvantages in other contexts, their control within specific security domains may alleviate some of those concerns. For example, with digital signatures for non-repudiation, it is crucial that nobody but the signer has the signing key, otherwise the signer may legitimately argue the repudiation of signatures. The existence of escrow keys means the some other entity has access to the signing key, which enables signers to argue that the escrow key was used to obtain their signing key and subsequently generate their signatures. However, where the domain is limited to a particular organisation or part of an organisation it may be sufficient that the organisation cannot repudiate the signature. Lost signing keys do not imply lost data, unlike encryption keys, so there is little need to backup signing keys.

[0057] Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

What is claimed is:

1. A method of computing a random number for use in a cryptographic operation comprising the steps of providing a pair of inputs to an elliptic curve random number generator with each input representative of at least one coordinate of an elliptic curve point and with at least one of said inputs being verifiably random.

2. A method according to claim 1 wherein said at least one input is obtained from an output of a hash function.

3. A method according to claim 2 wherein the other of said inputs is utilized as an input to said hash function.

4. A method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

5. A method according to claim 4 wherein one of said scalar multiples is used to derive said random number and the other of said scalar multiples is used to change said secret value for subsequent use.

6. A method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input.

7. A method according to claim 6 wherein another coordinate of said point is obtained from said one coordinate for inclusion as said input.

8. A method according to claim 7 wherein said other input is a representation of an elliptic curve point.

9. A method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and truncating said coordinate to a bit string for use as said random number.

10. A method according to claim 9 wherein said one coordinate is truncated in the order of one half the length of a representation of an elliptic curve point representation.

11. A method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and hashing said one coordinate to provide a bit string for use as said random number.

12. A method according to claim 1 wherein said verifiably random input is chosen to be of a canonical form whereby a predetermined relationship between said inputs is difficult to maintain.

13. A method of computing a random number for use in a cryptographic operation, said method comprising the steps of providing a pair of inputs, each representative of at least one coordinate of a pair of elliptic curve points to an elliptic curve random number generator, obtaining an output representative of at least one coordinate of a scalar multiple of an elliptic curve point and passing said output through a one way function to obtain a bit string for use as a random number.

14. A method according to claim 13 wherein said one way function is a hash function.

15. An elliptic curve random number generator having a pair of inputs each representative of at least one coordinate of a pair of elliptic curve points and an output for use as a random number in a cryptographic operation, at least one of said inputs being verifiably random.

16. An elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function.

17. An elliptic curve random number generator according to claim 16 wherein said one way function is a hash function.

18. An elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function.

19. A method of establishing an escrow key for a security domain within a network, said method comprising the steps of establishing a pair of points PQ as respective inputs to an elliptic curve random number generator with a relationship between said point such that $P = eQ$, storing said relationship e as an escrow key with an administrator and generating from said elliptic curve random number generator a random number for use in cryptographic operations within said domain.

ABSTRACT

An elliptic curve random number generator avoids escrow keys by choosing a point Q on the elliptic curve as verifiably random. An arbitrary string is chosen and a hash of that string computed. The hash is then converted to a field element of the desired field, the field element regarded as the x-coordinate of a point Q on the elliptic curve and the x-coordinate is tested for validity on the desired elliptic curve. If valid, the x-coordinate is decompressed to the point Q, wherein the choice of which is the two points is also derived from the hash value. Intentional use of escrow keys can provide for back up functionality. The relationship between P and Q is used as an escrow key and stored by for a security domain. The administrator logs the output of the generator to reconstruct the random number with the escrow key.

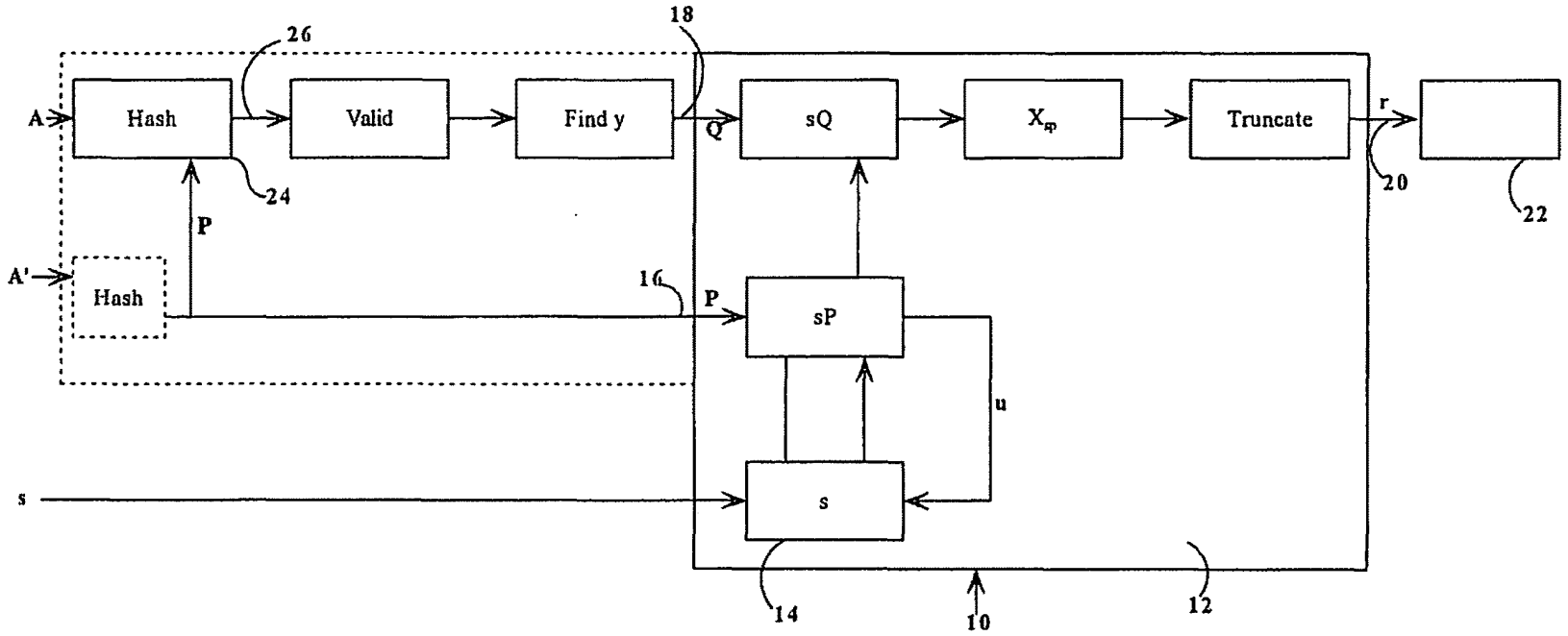

A
Hash
26
Valid
Find y
18
Q
sQ
X_{qp}
Truncate
r
20
22
24
P
A'
Hash
16
P
sP
u
s
s
14
10
12

FIGURE 1

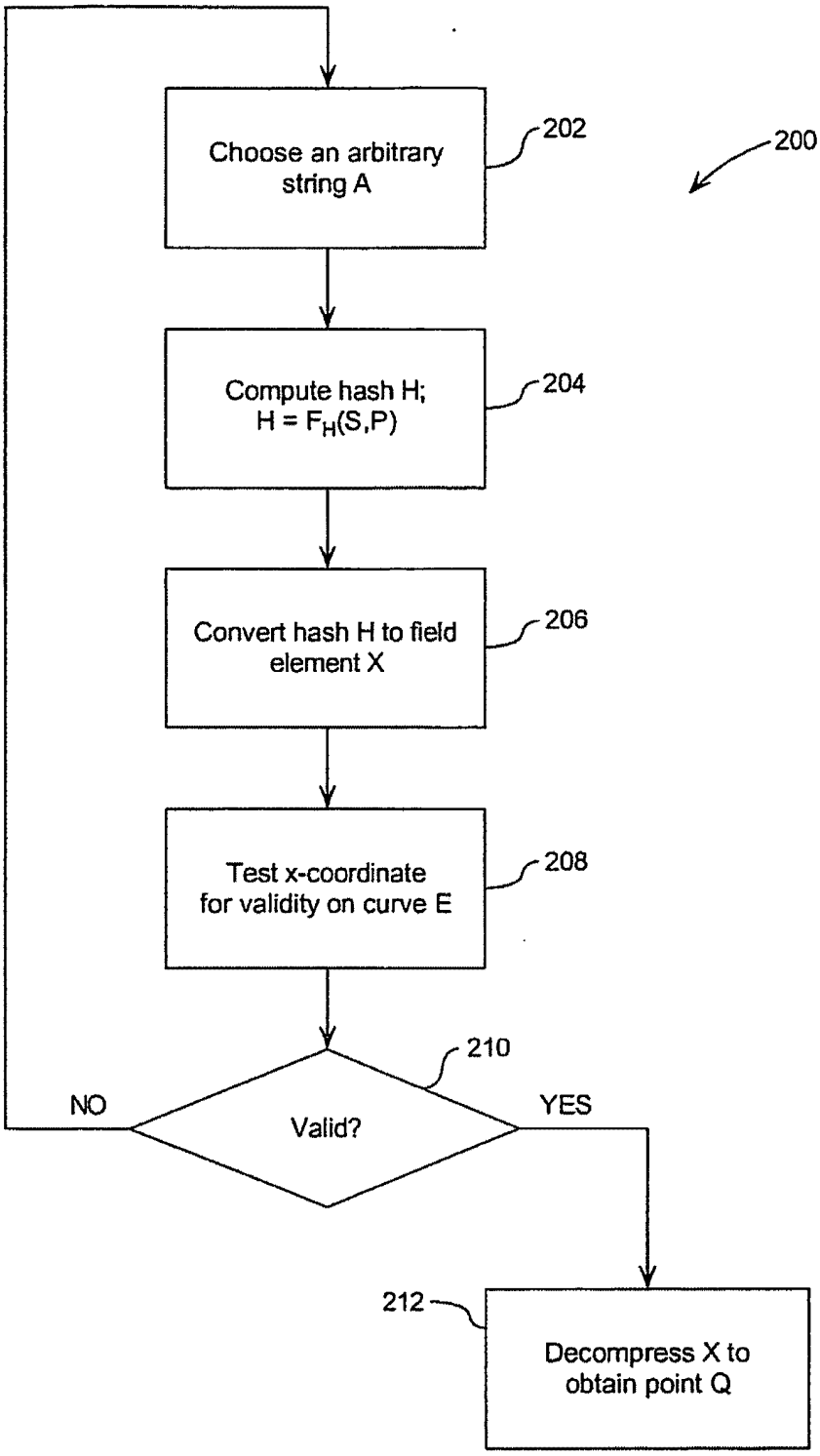

Choose an arbitrary string A
202
200
Compute hash H; H = $F_H(S,P)$
204
Convert hash H to field element X
206
Test x-coordinate for validity on curve E
208
210
Valid?
NO
YES
212
Decompress X to obtain point Q

Figure 2

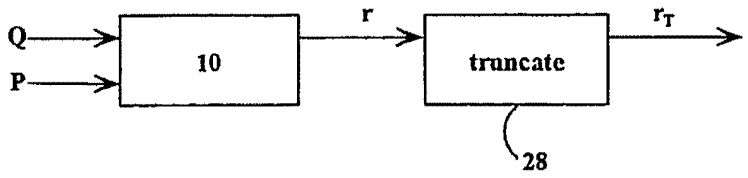


FIGURE 3

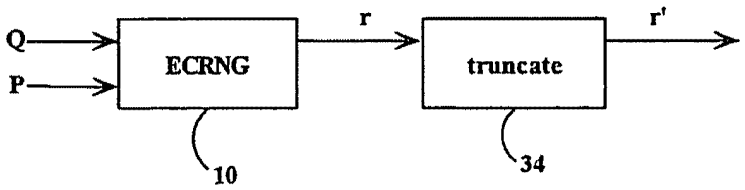


FIGURE 5

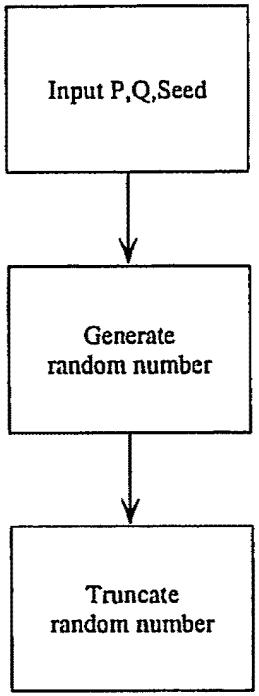


Figure 4

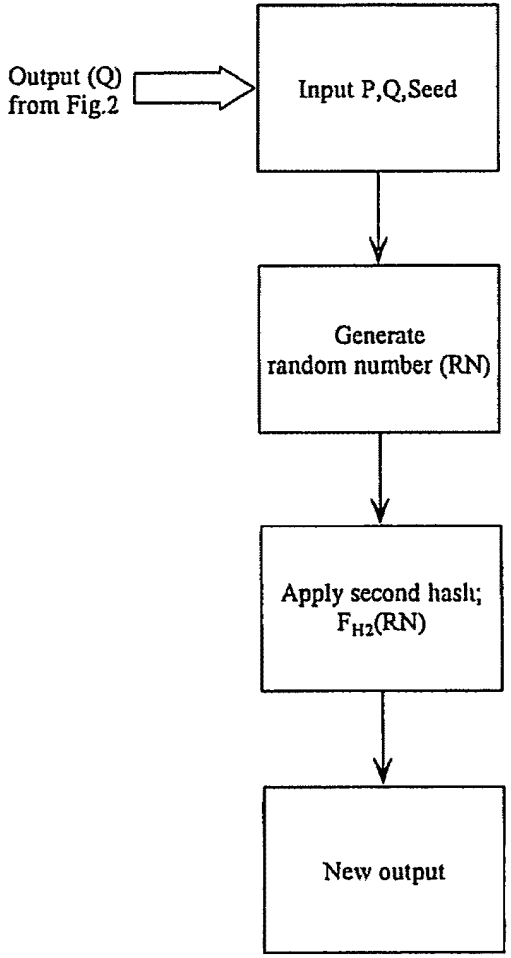


Figure 6

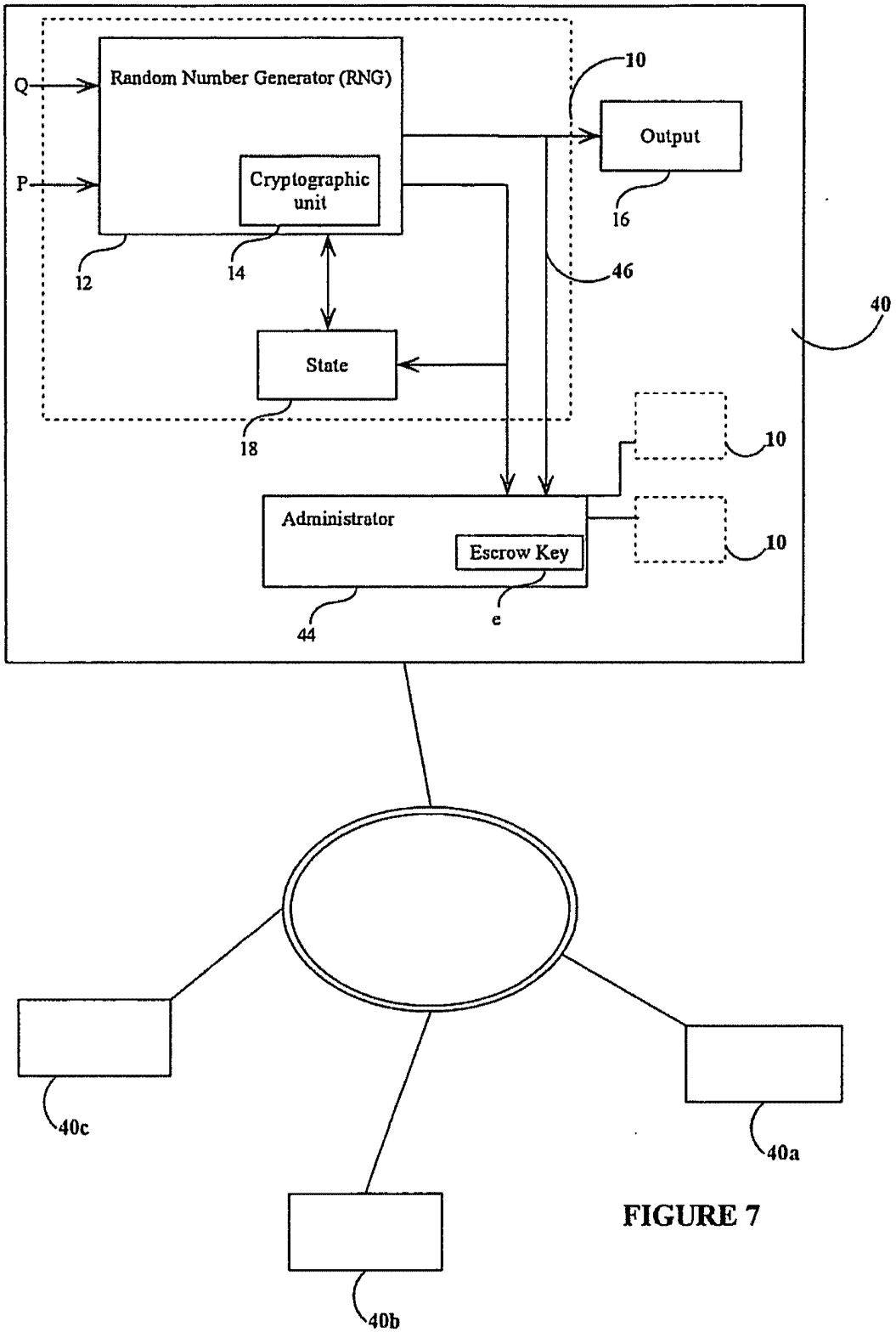

Random Number Generator (RNG)
Q
P
Cryptographic unit
Output
State
Administrator
Escrow Key
10
16
12
14
46
40
18
10
10
44
e
40c
40a
40b

FIGURE 7

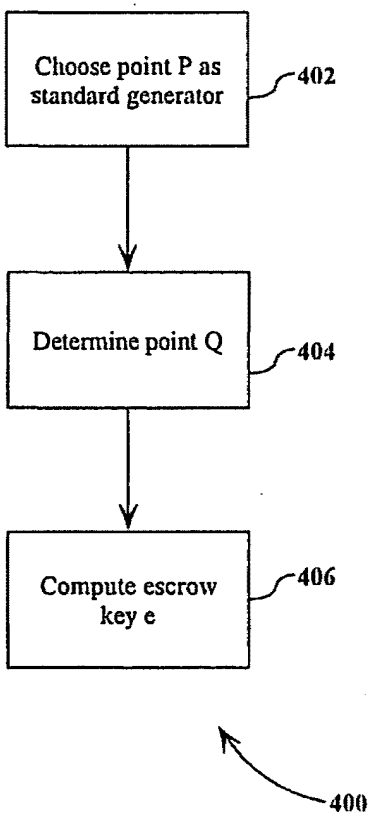


Figure 8

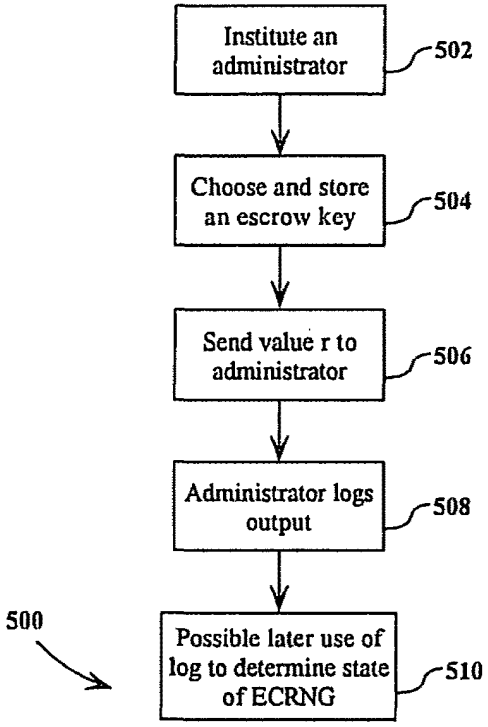


Figure 9

Docket No.
67539/622

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

ELLIPTIC CURVE RANDOM NUMBER GENERATION

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International Application Number _____

and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, or plant breeder's rights certificate(s), or 365(a) of any PCT International application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Claimed
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional

60/644,982	January 21, 2005
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Blake, Cassels & Graydon LLP
Practitioners associated with Customer No. 27871

Send Correspondence to:

Blake, Cassels & Graydon LLP
P.O. Box 25, Commerce Court West
Toronto, Ontario, M5L 1A9

Direct Telephone Calls to: *(name and telephone number)*
John R. S. Orange 416.863.3164

Full name of sole or first inventor **Daniel R. L. BROWN**
Sole or first inventor's signature Date
Residence **Mississauga, Canada**
Citizenship **Canadian**
Post Office Address **6033 Paddle Road, Mississauga, Ontario, L5N 1X8, Canada**

Full name of second inventor, if any **Scott A. VANSTONE**
Second inventor's signature Date
Residence **Campbellville, Canada**
Citizenship **Canadian**
Post Office Address **10140 Pineview Trail, Campbellville, Ontario, N0P 1B0, Canada**

PATENT APPLICATION SERIAL NO _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

01/25/2006 MWOLDGE1 00000052 022553 11336814

01 FC:1011 300.00 DA
02 FC:1111 500.00 DA
03 FC:1311 200.00 DA
04 FC:1201 200.00 DA

PTO-1556
(5/87)

U.S. Government Printing Office: 2002 — 466-247/69033

PTO/SB/06 (12-04)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875 Effective December 8, 2004

Application or Docket Number: 11/356,814

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	150.00		N/A	300.00
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	$250		N/A	$500
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	$100		N/A	$200
TOTAL CLAIMS (37 CFR 1.16(i))	19 minus 20 =	*	X$ 25 =		OR	X$50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1	X100 =			X200 =	200
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			+180=			+360=	
			TOTAL			TOTAL	1200

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622

CONFIRMATION NO. 1834

Blake, Cassels & Graydon LLP
Commerce Court West
P.O. Box 25
Toronto, ON M5L 1A9
CANADA

FORMALITIES LETTER

Date Mailed: 03/09/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$130** for a Large Entity

- **$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice <u>MUST</u> be returned with the reply.

SOW

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 3 - OFFICE COPY

Doc Code:

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	11/336,814
Filing Date	January 23, 2006
First Named Inventor	BROWN, Daniel R.L.
Art Unit	2131
Examiner Name	N/A
Attorney Docket Number	67539/622

Total Number of Pages in This Submission

ENCLOSURES *(Check all that apply)*

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment / Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [x] Response to Missing Parts/ Incomplete Application
  - [x] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Blake, Cassels & Graydon LLP		
Signature			
Printed name	John R.S. Orange		
Date	26 April 2006	Reg. No.	29,725

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria,VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

Response To Notice To File Missing Parts Of Application Filing Date Granted (PTO-1533)(Large Entity)	Docket No. 67539/622

In Re Application Of: **BROWN, Daniel R.L. et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
11/336,814	January 23, 2006	N/A	27871	2131	1834

Invention: **ELLIPTIC CURVE RANDOM NUMBER GENERATION**

Mail Stop Missing Parts

COMMISSIONER FOR PATENTS:

This is a response to the Notice to File Missing Parts of Application - Filing Date Granted (PTO-1533) mailed on March 9, 2006 (*Date*).

Enclosed herewith for filing are the following:

- ☐ A copy of the Notice to File Missing Parts of Application - Filing Date Granted (PTO-1533). **(REQUIRED)**
- ☐ An oath or declaration in compliance with 37 CFR 1.63, including residence information and identifying the application by the above Application Number and Filing Date.
- ☒ A properly signed oath or declaration in compliance with 37 CFR 1.63.
- ☐ An oath or declaration in compliance with 37 CFR 1.63 listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date.
- ☐ A verified English translation of the non-English language application papers as originally filed. It is requested that this translation be used as the copy for examination purposes in the United States Patent and Trademark Office.
- ☐ Other (list):

Response To Notice To File Missing Parts Of Application Filing Date Granted (PTO-1533)(Large Entity)	Docket No. 67539/622

In Re Application Of: **BROWN, Daniel R.L. et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
11/336,814	January 23, 2006	N/A	27871	2131	1834

Invention: **ELLIPTIC CURVE RANDOM NUMBER GENERATION**

TO THE COMMISSIONER FOR PATENTS:

Mail Stop Missing Parts

☐ Completion of application fees as calculated below:

☐ Utility application basic fee	
☐ Design application basic fee	
☐ Search Fee	
☐ Examination Fee	
☐ Total number of independent claims = _____	
☐ Total number of claims = _____	
☐ Multiple dependent claims	
☒ Surcharge for late payment of filing fee and/or late filing of original declaration or oath	$130.00
☐ Petition and fee for filing by other than all the inventors or a person not the inventor	
☐ Fee for processing an application filed with a non-English language specification	
☐ Fee for processing and retention of application	
Total completion of application fees	

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the above-identified Notice to File Missing Parts of Application. The requested extension is as follows (check time period desired). If an additional time extension is required, please consider this a petition therefor.

☐ One month ☐ Two months ☐ Three months ☐ Four months ☐ Five months

from: _____ *Date* until: _____ *Date*

Total time extension fees _____

Total fees due _____

Response To Notice To File Missing Parts Of Application Filing Date Granted (PTO-1533) (Large Entity)	Docket No. 67539/622

In Re Application Of: **BROWN, Daniel R.L. et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
11/336,814	January 23, 2006	N/A	27871	2131	1834

Invention: **ELLIPTIC CURVE RANDOM NUMBER GENERATION**

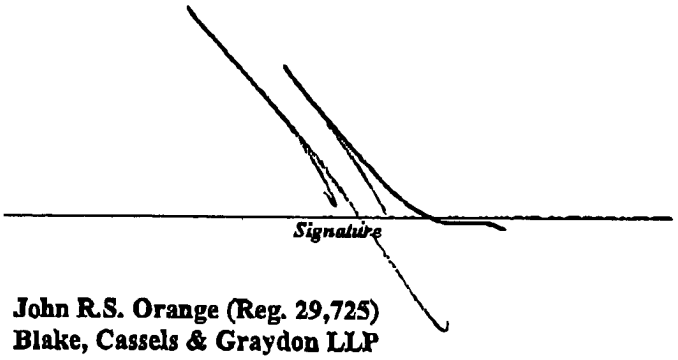
TO THE COMMISSIONER FOR PATENTS:

Mail Stop Missing Parts

The fee of **$130.00** is to be paid as follows:

- ☐ A check in the amount of the fee is enclosed.
- ☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. **02-2553**
- ☒ If an additional extension of time is required, please consider this a petition therefor and charge any additional fees which may be required to Deposit Account No. **02-2553**
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.



Signature

Dated: 26 April 06

John R.S. Orange (Reg. 29,725)
Blake, Cassels & Graydon LLP
Box 25, Commerce Court West
199 Bay Street
Toronto, Ontario
M5L 1A9
Canada

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

_____.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

cc:

P31LARGE/REV05

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622

CONFIRMATION NO. 1834

Blake, Cassels & Graydon LLP
Commerce Court West
P.O. Box 25
Toronto, ON M5L 1A9
CANADA

FORMALITIES LETTER

Date Mailed: 03/09/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

04/27/2006 SFELEKE1 00000170 022553 11336814
01 FC:1051 130.00 DA

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$130** for a Large Entity

- **$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice MUST be returned with the reply.

SOL

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 2 - COPY TO BE RETURNED WITH RESPONSE

Docket No.
67539/622

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

ELLIPTIC CURVE RANDOM NUMBER GENERATION

the specification of which

(check one)

☐ is attached hereto.

☒ was filed on **January 23, 2006** as United States Application No. or PCT International Application Number **11/336,814**

and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, or plant breeder's rights certificate(s), or 365(a) of any PCT International application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Claimed
(Number)	(Country)	(Day/Month/Year Filed)	☐
(Number)	(Country)	(Day/Month/Year Filed)	☐
(Number)	(Country)	(Day/Month/Year Filed)	☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional

60/644,982	January 21, 2005
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

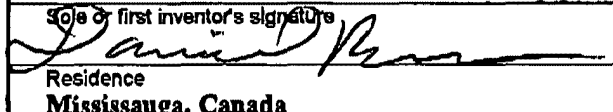
POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

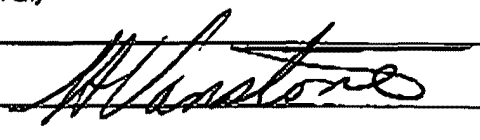
Blake, Cassels & Graydon LLP
Practitioners associated with Customer No. 27871

Send Correspondence to:

Blake, Cassels & Graydon LLP
P.O. Box 25, Commerce Court West
Toronto, Ontario, M5L 1A9

Direct Telephone Calls to: *(name and telephone number)*
John R. S. Orange 416.863.3164

Full name of sole or first inventor **Daniel R. L. BROWN**
Sole or first inventor's signature  Date April 4, 2006
Residence **Mississauga, Canada**
Citizenship **Canadian**
Post Office Address **6033 Paddle Road, Mississauga, Ontario, L5N 1X8, Canada**

Full name of second inventor, if any **Scott A. VANSTONE**
Second inventor's signature  Date April 5, 2006
Residence **Campbellville, Canada**
Citizenship **Canadian**
Post Office Address **10140 Pineview Trail, Campbellville, Ontario, N0P 1B0, Canada**

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))	Docket No. 67539/00622

In Re Application Of:

BROWN, Daniel R.L. et al.

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
11/336,814	January 23, 2006	Not known	27871	2131	1834

Title:

ELLIPTIC CURVE RANDOM NUMBER GENERATION

Address to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

37 CFR 1.97(b)

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application other than a continued prosecution application under 37 CFR 1.53(d); within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; before the mailing of a first Office Action on the merits, or before the mailing of a first Office Action after the filing of a request for continued examination under 37 CFR 1.114.

37 CFR 1.97(c)

2. ☐ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(b), provided that the Information Disclosure Statement is filed before the mailing date of a Final Action under 37 CFR 1.113, a Notice of Allowance under 37 CFR 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

   ☐ the statement specified in 37 CFR 1.97(e);

   OR

   ☐ the fee set forth in 37 CFR 1.17(p).

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))	Docket No. 67539/00622

In Re Application of:
BROWN, Daniel R.L. et al.

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
11/336,814	January 23, 2006	Not known	27871	2131	1834

Title:
ELLIPTIC CURVE RANDOM NUMBER GENERATION

Payment of Fee

(Only complete if Applicant elects to pay the fee set forth in 37 CFR 1.17(p))

- ☐ A check in the amount of is attached.
- ☐ The Director is hereby authorized to charge and credit Deposit Account No. _____ as described below.
  - ☐ Charge the amount of
  - ☐ Credit any overpayment.
  - ☐ Charge any additional fee required.
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Certificate of Transmission by Facsimile*

I certify that this document and authorization to charge deposit account is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No.) on

_____
(Date)

Signature

Typed or Printed Name of Person Signing Certificate

Certificate of Mailing by First Class Mail

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

_____.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Certificate

***This certificate may only be used if paying by deposit account.**

Dated: **July 14, 2006**

_____
Signature

John R.S. Orange **Reg. No. 29,725**

Blake, Cassels & Graydon LLP
Tel: 416-863-3164
Fax: 416-863-2653
Email: ipg@blakes.com

cc:

Customer No. 27871

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/336,814**

Applicant: **BROWN, Daniel R.L. et al.**

Filed: **January 23, 2006**

Title: **Elliptic Curve Random Number Generation**

Art Unit: **2131**

Examiner: **Not known**

Docket No.: **67539/00622**

U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INFORMATION DISCLOSURE STATEMENT

Pursuant to the duty to disclose under 37 CFR §1.56, Applicant submits herewith a Form PTO/SB/08A listing references of which the Applicant is aware and which are brought to the attention of the Examiner. In accordance with 37 CFR §1.98(a)(2), a copy of each foreign patent document and non-patent document listed in the enclosed Form PTO/SB/08A is submitted herewith.

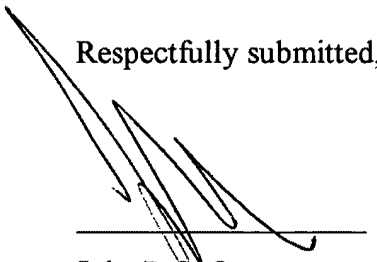
The filing of this IDS shall not be construed as a representation that a search has been made, an admission that the information cited is, or is considered to be, material for patentability, or that no other material information exists. This filing shall not be construed as an admission against interest in any matter.

This IDS is submitted pursuant to 37 CFR §1.97(b) and, accordingly, no fee is believed

to be due for consideration of the documents submitted herewith.

Applicant respectfully requests consideration of the items listed and requests the Examiner to return a copy of the attached Form PTO/SB/08A after being marked as being considered by the Examiner.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: July 14, 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164

JRO/jm

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	11/336,814
Filing Date	January 23, 2006
First named Inventor	BROWN, Daniel R.L.
Art Unit	2131
Examiner Name	Not known
Attorney Docket Number	67539/00622

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,044,388	03-28-2000	DEBELLIS ET AL.	
		US-6,243,467 B1	06-05-2001	REITER ET AL.	
		US-2004/0102242 A1	05-27-2004	POELMANN	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]	Number[4]	Kind-Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] **Applicants' unique citation designation number** (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	11/336,814
Filing Date	January 23, 2006
First named Inventor	BROWN, Daniel R.L.
Art Unit	2131
Examiner Name	Not known
Attorney Docket Number	67539/00622

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalogue, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
		LEE, Kap-piu & WONG, Kwok-wo; "Elliptic Curve Random Number Generation"; *Electrical and Electronic Technology, 2001. Tencon. Proceedings of IEEE Region 10 International Conference"*; August 19-22, 2001; pp. 239 to 241	
		KALISKI, Burton S., Jr.; "A Pseudo-Random Bit Generator Based on Elliptic Logarithms"; *Advances in Cryptology, CRYPTO 1986*; pp. 84-103, Vol. 263	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] **Applicants' unique citation designation number** (optional). [2] Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C> 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

DEPARTMENT OF DEFENSE

ACCESS ACKNOWLEDGEMENT / SECRECY ORDER RECOMMENDATION

FOR PATENT APPLICATION

Application Serial No: DP11336814 Filing Date: Date Referred: 03/13/2006

I hereby acknowledge that the Department of Defense reviewers has inspected this application in administration of 35 USC 181 on befalf of the Agencies/Commands specified below. DoD reviewers will not divulge any information from this application for any purpose other than administration of 35 USC 181.

Defense Agency	Recommendation	Reviewer Name	Reviewer Command	Date Reviewed
Navy	No Comments	Lawana Brady		03/15/2006
NSA	Secrecy Not Recommended	Eric Froehlich		04/16/2007

Type of Recommendations:	*SNR: Secrecy Not Recommended*
	SR: Secrecy Recommended
	NC: No Comment

Instructions to Reviewers:

1. All DoD personnel reviewering this application will be listed on this form regardless of whether they are making a secrecy order recommendation.

2. This form will be forwarded to USPTO once all assigned DoD entities have provided their secrecy order recommendation.

Time for Completion of Review:

Pursuant to 35 USC 184, the subject matter of this applicaiton may be filed in a foreign country for the purposed of filing a patent application without a license anytime after the expriation of six (6) months from filing date unless the application becomes the subject of a secrecy order.

The USPTO publishes patent application at 18 months from the earliest claimed filing date. The USPTO will delay the publication of a patent application made available to a defense agency under 35 USC 181 until no earlier than 6 months from the filing date or 90 days from the date of referral to that agency. This application will be cleared for publication 6 months from the filing date or 90 days from the above Date Referred, whichever is later, unless a response is is provided to the USPTO regarding the necessary recommendations as to the imposition of a secrecy order.

DoD Completion of Review: Final

Forwarded to USPTO: 04/19/2007 By: Luis Marrero

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622

CONFIRMATION NO. 1834

Blake, Cassels & Graydon LLP
Commerce Court West
P.O. Box 25
Toronto, ONM5L 1A9
CANADA

Date Mailed. 05/10/2007

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 08/16/2007. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at (703) 305-3028.

Questions relating to this Notice should be directed to the Office of Patent Publication at (571) 272-4200.

PART 1 - ATTORNEY/APPLICANT COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622

CONFIRMATION NO. 1834

Blake, Cassels & Graydon LLP
Commerce Court West
P.O. Box 25
Toronto, ONM5L 1A9
CANADA

Title: Elliptic curve random number generation

Publication No. US-2007-0189527-A1
Publication Date: 08/16/2007

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Pre-Grant Publication Division, 703-605-4283

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

7590 06/23/2009

Blake, Cassels & Graydon LLP
Commerce Court West
P.O. Box 25
Toronto, ON M5L 1A9
CANADA

EXAMINER	
LAKHIA, VIRAL S	
ART UNIT	**PAPER NUMBER**
4144	

MAIL DATE	DELIVERY MODE
06/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	4144	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *23 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/26/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1 – 19 have been examined and are pending.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449 filed July 26 2006 is attached to the instant Office action.

Claim Rejections - 35 USC § 101

Claims 1-19 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of *In Re Bilski* 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. For example, the step of providing inputs to elliptic random number generator (see claim 1) and the relationship of P=eQ (claim 19), could be done in paper or by mental step. The dependent claims 2-19 are rejected under the same reason. For example, dependent claim 2 for obtaining input from a hash function could be reading a value from a table lookup on paper. Similarly, dependent claim 5, the step of scalar multiples to derive the random number could be done in paper or by mental step.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1 – 18 rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 7,200,225 to Schroeppel et al. (hereinafter "Schroeppel").

As per claims 1 and 15, Schroeppel teaches a method and an elliptic curve random number generator for computing a random number for use in a cryptographic operation comprising the steps of providing a pair of inputs to an elliptic curve random number generator with each input representative of at least one coordinate of an elliptic curve point and with at least one of said inputs being verifiably random *(col 7 lines 40-50).*

As per claims 2 and 17, Schroeppel teaches a method and an elliptic curve random number generator according to claim 1 and 16 wherein said at least one input is obtained from an output of a hash function *(col 7 lines 50-60).*

As per claims 3 and 18, Schroeppel teaches a method and an elliptic curve random number generator according to claim 2 and 17 wherein the other of said inputs is utilized as an input to said hash function *(col 7 lines 50 – 60).*

As per claim 4 Schroeppel teaches a method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs *(col 7 lines 60 – 70)*.

As per claim 5 Schroeppel teaches a method according to claim 4 wherein one of said scalar multiples is used to derive said random number and the other of said scalar multiples is used to change said secret value for subsequent use *(col 7 – 65 -70, col 8 – lines 1 – 10).*

As per claim 6 Schroeppel teaches a method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input *(col 8 lines 35 – 40).*

As per claim 7 Schroeppel teaches a method according to claim 6 wherein another coordinate of said point is obtained from said one coordinate for inclusion as said input *(col 8 lines 30 – 40).*

As per claim 8 Schroeppel teaches a method according to claim 7 wherein said other input is a representation of an elliptic curve point *(col 8 lines 45 – 55).*

As per claim 9 Schroeppel teaches a method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and truncating said coordinate to a bit string for use as said random number *(col 9 – lines 1 -10).*

As per claim 10 Schroeppel teaches a method according to claim 9 wherein said one coordinate is truncated in the order of one half the length of a representation of an elliptic curve point representation *(col 9 – 1 – 10).*

As per claim 11 Schroeppel teaches a method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and hashing said one coordinate to provide a bit string for use as said random number *(col 9 lines 20 – 30)* .

As per claims 12 Schroeppel teaches a method according to claim 1 wherein said verifiably random input is chosen to be of a canonical form whereby a predetermined relationship between said inputs is difficult to maintain *(col 7 lines 45 – 55).*

As per claims 13 Schroeppel teaches a method of computing a random number for use in a cryptographic operation, said method comprising the steps of providing a pair of inputs, each representative of at least one coordinate of a pair of elliptic curve points to an elliptic curve random number generator *(col 7 lines 43 – 57),* obtaining an output representative of at least one coordinate of a scalar multiple of an elliptic curve point *(col 7 lines 48 – 55)* and passing said output through a one way function to obtain a bit string for use as a random number *(col 7 lines 58 – 68).*

As per claims 14 Schroeppel teaches a method according to claim 13 wherein said one way function is a hash function (col 8 lines 35 – 45).

As per claims 16 Schroeppel teaches a method an elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function *(col 7 lines 50-60)*.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 19 rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Publication 2003/0081785 to Boneh et al. (hereinafter "Boneh").

As per claims 19 Boneh teaches a method of establishing an escrow key for a security domain within a network, said method comprising the steps of establishing a pair of points PQ as respective inputs to an elliptic curve random number generator *(Boneh, para 0018 where pair of points are mapped within the system cryptographic (elliptic curve- BDH Binary Diffie-Hellman) parameters)* with a relationship between said point such that P=eQ, storing said relationship e as an escrow key with an administrator *(Boneh, para 0050)* and generating from said elliptic curve random number generator a random number *(Boneh, para 0108, where BDH Parameter Generator outputs a prime number q,)* for use in cryptographic operations within said domain *(Boneh Fig 6 and para 0044).*

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S.Patent No: 7,221,758 to Cramer, for Practical non-malleable public-key cryptosystem.

U.S. Publication No: 2008056499 to Vanstone for Split-Key Key-Agreement Protocol.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viral Lakhia whose telephone number is (571) 373-3363. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Pan Daniel can be reached on (571) 272-4172. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/VIRAL LAKHIA/ Examiner, Art Unit 4144

/Daniel Pan/

Supervisory Patent Examiner, Art Unit 4144

Notice of References Cited	Application/Control No. 11/336,814	Applicant(s)/Patent Under Reexamination BROWN ET AL.	
	Examiner VIRAL LAKHIA	Art Unit 4144	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,200,225	04-2007	Schroeppel, Richard	380/28
*	B	US-7,221,758	05-2007	Cramer et al.	380/44
*	C	US-2008/0056499	03-2008	Vanstone, Scott A.	380/278
*	D	US-2003/0081785	05-2003	Boneh et al.	380/277
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	4144

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009							
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19		✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	Art Unit
	VIRAL LAKHIA	4144

SEARCHED

Class	Subclass	Date	Examiner
380	28-30	6/17/09	V.L.
380	44-47	6/17/09	V.L.
380	277-286	6/17/09	V.L.
713	Search 713 with key word search of elliptic curve number generator	6/17/09	V.L.
726	Search 726 with key word search of elliptic curve number generator	6/17/09	V.L.

SEARCH NOTES

Search Notes	Date	Examiner
Key words and combination : elliptic curve number generator (creator, producer, intiator), message, digest, hash, random	7/17/09	V.L.
Get assistance with Fast and Focused Search department for the case	7/17/09	V.L
Get assistance from Peter Poltriak for claim interpretation and understanding of invention	7/17/09	V.L
Search Google Patents, NPL and wikipedia for elliptic curve technology	7/17/09	V.L

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L8	1	"11336816"	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/18 08:28
L10	0	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5) and exchange and escrow (backup)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 08:50
L11	79	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and escrow and key	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 08:50
L12	6	"10384328"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 08:57
L13	6	"10384328"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 09:03
L14	14	"7113594"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 09:13
S1	1	"11336814"	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/16 15:39
S2	18109	"380".clas.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52
S3	3324	380/28-30.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52
S4	2286	380/44-47.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52

S5	3939	380/277-286.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:53
S6	5	"5073935" "5142577"	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:53
S7	0	elliptic (3n) curve? ?	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:59
S8	3136	elliptic near5 curve and (number$3 or value$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:01
S9	1471899	generator or creator or producer or intiator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:03
S10	1382	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:04
S11	5042269	Hash or function or digest	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:10
S12	5042357	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)or hash or function or digest	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:10
S13	886	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11
S14	176	S2 and S3 and S4 and S5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11

S15	17	S13 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11
S16	870	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:13
S17	17	S14 and S16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14
S18	529	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5) and exchange	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14
S19	12	S14 and S18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14
S20	2	JP "2003124919"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:30
S21	2	"7327845"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 12:18
S22	2	"20070189527"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 12:18

S23	0	"2005644982"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:57
S24	2	"20070189527"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:57
S25	2	JP "2003124919"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:59
S26	6	"6934392"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:05
S27	529	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5) and exchange	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:07
S28	4	S27 and S26	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:07
S29	5666	"713".clas. and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 16:36

6/18/2009 9:21:29 AM
C:\Documents and Settings\vlakhia\My Documents\EAST\Workspaces\11336814.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1834

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/336,814	01/23/2006	380	4144	67539/622

APPLICANTS

Daniel R. L. Brown, Mississauga, CANADA;
Scott A. Vanstone, Campbellville, CANADA;

**** CONTINUING DATA ***************************

This appln claims benefit of 60/644,982 01/21/2005

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /VIRAL S LAKHIA/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CANADA	6	19	4

ADDRESS

Blake, Cassels & Graydon LLP
Commerce Court West
P.O. Box 25
Toronto, ON M5L 1A9
CANADA

TITLE

Elliptic curve random number generation

FILING FEE RECEIVED		
1330	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"11336814"	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/16 15:39
S2	18109	"380".clas.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52
S3	3324	380/28-30.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52
S4	2286	380/44-47.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52
S5	3939	380/277-286.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:53
S6	5	"5073935" "5142577"	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:53
S7	0	elliptic (3n) curve? ?	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:59
S8	3136	elliptic near5 curve and (number$3 or value$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:01
S9	1471899	generator or creator or producer or intiator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:03
S10	1382	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:04
S11	5042269	Hash or function or digest	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:10
S12	5042357	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)or hash or function or digest	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:10

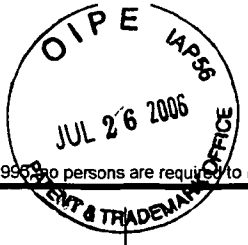
S13	886	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11
S14	176	S2 and S3 and S4 and S5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11
S15	17	S13 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11
S16	870	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:13
S17	17	S14 and S16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14
S18	529	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5) and exchange	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14
S19	12	S14 and S18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14

S20	2	JP "2003124919"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:30
S21	2	"7327845"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 12:18
S22	2	"20070189527"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 12:18
S23	0	"2005644982"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:57
S24	2	"20070189527"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:57
S25	2	JP "2003124919"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:59
S26	6	"6934392"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:05
S27	529	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5) and exchange	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:07

S28	4	S27 and S26	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:07
S29	5666	"713".clas. and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 16:36

6/17/2009 4:37:20 PM
C:\Documents and Settings\vlakhia\My Documents\EAST\Workspaces\11336814.wsp

Receipt date: 07/26/2006



/V.L/

11336814 - GAU: 4144

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	11/336,814
Filing Date	January 23, 2006
First named Inventor	BROWN, Daniel R.L.
Art Unit	2131
Examiner Name	Not known
Attorney Docket Number	67539/00622

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,044,388	03-28-2000	DEBELLIS ET AL.	
		US-6,243,467 B1	06-05-2001	REITER ET AL.	
		US-2004/0102242 A1	05-27-2004	POELMANN	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]	Number[4]	Kind-Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature	/Viral Lakhia/	Date Considered	06/17/2009

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] **Applicants' unique citation designation number** (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	11/336,814
Filing Date	January 23, 2006
First named Inventor	BROWN, Daniel R.L.
Art Unit	2131
Examiner Name	Not known
Attorney Docket Number	67539/00622

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalogue, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
		LEE, Kap-piu & WONG, Kwok-wo; "Elliptic Curve Random Number Generation"; *Electrical and Electronic Technology, 2001. Tencon. Proceedings of IEEE Region 10 International Conference"*; August 19-22, 2001; pp. 239 to 241	
		KALISKI, Burton S., Jr.; "A Pseudo-Random Bit Generator Based on Elliptic Logarithms"; *Advances in Cryptology, CRYPTO 1986*; pp. 84-103, Vol. 263	

Examiner Signature	/Viral Lakhia/	Date Considered	06/17/2009

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] **Applicants' unique citation designation number** (optional). [2] Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C> 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/336,814**

Applicant: **BROWN, Daniel R.L.; VANSTONE, Scott A.**

Filed: **January 23, 2006**

Title: **Elliptic Curve Random Number Generation**

Art Unit: **4144**

Examiner: **LAKHIA, Viral S.**

Docket No.: **67539/00622**

Mail Stop Amendment
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE

Sir:

This is further to the Office Action dated June 23, 2009. Applicants wishes to amend the above-identified application as follows:

Amendments to the Claims: are reflected in the listing of claims which begins on page 2of this paper.

Remarks: begin on page 4 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of ~~computing~~ operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of: - providing a pair of inputs to ~~an elliptic curve random number generator~~ said arithmetic unit, with each input representative of at least one coordinate of an elliptic curve point, and with at least one of said inputs being verifiably random.; performing selected elliptic curve operations on said inputs to obtain an output; and utilising said output as a random number in the cryptographic operation.

2. (original) A method according to claim 1 wherein said at least one input is obtained from an output of a hash function.

3. (original) A method according to claim 2 wherein the other of said inputs is utilized as an input to said hash function.

4. (original) A method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

5. (original) A method according to claim 4 wherein one of said scalar multiples is used to derive said random number and the other of said scalar multiples is used to change said secret value for subsequent use.

6. (original) A method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input.

7. (currently amended) A method according to claim 6 wherein another coordinate of said point is obtained from said one coordinate for inclusion as said one input.

8. (original) A method according to claim 7 wherein said other input is a representation of an elliptic curve point.

9. (original) A method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and truncating said coordinate to a bit string for use as said random number.

10. (original) A method according to claim 9 wherein said one coordinate is truncated in the order of one half the length of a representation of an elliptic curve point representation.

11. (original) A method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and hashing said one coordinate to provide a bit string for use as said random number.

12. (original) A method according to claim 1 wherein said verifiably random input is chosen to be of a canonical form whereby a predetermined relationship between said inputs is difficult to maintain.

13. (currently amended) A method of ~~computing~~ operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of: providing a pair of inputs, each representative of at least one coordinate of a pair of elliptic curve points, to said arithmetic unit; ~~an elliptic curve random number generator,~~ performing elliptic curve operations to obtain ~~obtaining~~ an output representative of at least one coordinate of a scalar multiple of an elliptic curve point; ~~and~~ passing said output through a one way function to obtain a bit string for use as a random number; and utilising said random number in the cryptographic operation.

14. (original) A method according to claim 13 wherein said one way function is a hash function.

15. (currently amended) An elliptic curve random number generator ~~having~~ comprising a pair of inputs, each of said inputs being representative of at least one coordinate of a pair of elliptic curve points; ~~and~~ an arithmetic unit to perform elliptic curve operations on said inputs; and an output to receive the results of said elliptic operations, said output representing ~~for use as~~ a random number for use in a cryptographic operation, at least one of said inputs being verifiably random.

16. (original) An elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function.

17. (original) An elliptic curve random number generator according to claim 16 wherein said one way function is a hash function.

18. (original) An elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function.

19. (currently amended) A method of establishing an escrow key for a security domain within a network, said method comprising the steps of establishing a pair of points P, Q as respective inputs to an elliptic curve random number generator with a relationship between said points such that $P = eQ$, storing said relationship e as an escrow key with an administrator ~~and generating from~~ operating said elliptic curve random number generator to obtain an output and utilising said output as a random number for use in cryptographic operations within said domain.

20. (new) A method according to claim 5 wherein said secret value is derived from a coordinate of said other scalar multiple.

21. (new) A method according to claim 20 wherein the $\bar{x}$ coordinate of said other scalar multiple is used to change said secret value.

22. (new) An elliptic curve random number generator according to claim 15 wherein said arithmetic unit operates on said inputs to obtain a scalar multiple of a coordinate of a point represented by said one input.

23. (new) An elliptic curve random number generator according to claim 23 wherein said arithmetic unit computes a coordinate of a scalar multiple of each of said points represented by said inputs

24. (new) An elliptic curve random number generator according to claim 23 wherein said coordinate of said scalar multiple of said point represented by said one input is operated on by said arithmetic unit and utilised as said output.

25. (new) An elliptic curve random number generator according to claim 24 wherein said arithmetic unit includes a register to maintain a secret value and a value derived from said coordinate of said scalar multiple of the point represented by said other input is stored in said register to provide said secret value.

26. (new) An elliptic curve random number generator according to claim 25 wherein said arithmetic unit utilises said secret value and said one input to obtain said coordinate of said scalar multiple of said point represented by said one input.

27. (new) An elliptic curve random number generator according to claim 26 wherein said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and truncates said coordinate to provide said output.

28. (new) An elliptic curve random number generator according to claim 26 wherein said arithmetic unit includes a one way function and said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and applies said one way function to said coordinate of said scalar multiple to obtain said output.

29. (new) An elliptic curve random number generator according to claim 28 wherein said arithmetic unit truncates said coordinate of said scalar multiple prior to applying said one way function.

30. (new) A method according to claim 19 wherein a preceding output is stored by said administrator.

31. (new) A method according to claim 30 wherein said security domain includes a plurality of elliptic curve random number generators each of which has a pair of inputs related by an escrow key.

32. (new) A method according to claim 31 wherein said escrow key is common for each elliptic curve random number generator.

33. (new) A security domain comprising at least one elliptic curve random number generator, said elliptic curve random number generator having a pair of inputs representative of respective elliptic curve points P,Q, said points P,Q being related by an escrow key e such

that P=eQ, and an output to represent a random number for use in a cryptographic operation; and an administrator including a memory to store said escrow key e.

34. (new) A security domain according to claim 33 wherein said memory includes a value corresponding to a preceding output to facilitate recovery of a subsequent output with said escrow key.

35. (new) A security domain according to claim 34 including a plurality of elliptic curve random number generators, and said memory includes an escrow key for each of said elliptic curve random number generators.

36. (new) A security domain according to claim 35 wherein each domain has a common escrow key.

REMARKS

In the Office Action date June 23, 2009, the Examiner objected to the claims previously on file on the basis of 35 USC 101 and 35 USC 102. The comments and amendments to the claims submitted herewith are believed to overcome the objections raised by the Examiner and place the application in condition for allowance. Additional claims dependent on claims previously submitted have been included to define more fully the scope of protection sought.

Claim Rejections under 35 USC 101

The Examiner objected to the claims previously on file on the basis of the interpretation of Re Bilski. Claim 1 previously on file is directed to a method of computing a random number for use in a cryptographic operation and sets forth certain steps of the process involving the use of an elliptic curve random number generator. As such, it is believed that claim 1 previously on file satisfied the test set forth In *Re Bilski* in that it was tied to a particular machine. The Examiner has suggested that the steps of providing inputs to the elliptic curve random number generator could be done in paper or by mental step. However, claim 1 previously on file was directed to a method of computing the random number that involved not only the provision of the pair of inputs but also the computation of a random number from that pair of inputs through the use of an elliptic curve random number generator.

Claim 1 has been amended to clarify the nature of the protection sought by explicitly directing the claim to a method of operating an elliptic curve random number generator that computes a random number. The claim specifies the steps of providing the pair of inputs and further recites the operation of an arithmetic unit of the elliptic curve random number generator to provide an output and the utilization of the output as a random number in a cryptographic operation.

It is believed that claim 1 as amended therefore clearly satisfies the tests set forth In *Re Bilski*, not only in being tied to a particular machine but also, reciting the transformation of the underlying subject matter, namely the pair of inputs to a different state or thing, namely, the random number output.

As claims 2 through 12 and new claims 20 and 21 depend directly or indirectly from claim 1, it is believed that they are also directed to statutory subject matter.

A similar amendment has been made to claim 13 that now explicitly recites the operation of the arithmetic unit of the elliptic curve random number generator and the utilization of the random number in a cryptographic operation. For the reasons set forth above, it is believed that such a claim and the claims dependent thereon clearly satisfy the requirements set forth In *Re Bilski*.

Claim 15 previously on file is directed to apparatus rather than to a process and as such, the Examiners comments as to the applicability In *Re Bilski* to the process steps do not appear to be appropriate. Claim 15 is directed to an apparatus and is clearly tied to a particular machine. As such it is statutory subject matter. Claim 15 has been amended to recite an arithmetic unit to perform elliptic curve operations on the inputs and provide the output and thereby further clarify the nature of the machine being claimed. It is believed therefore that claim 15 and the claims dependent thereon fall within one of the statutory categories of invention.

Claim 19 is directed to a method of establishing an escrow key and does not simply require the establishment of the value e but requires the step of establishing the pair of points P,Q as inputs to the elliptic curve random number generator, the storing of the relationship e as an escrow key and the operation of the elliptic curve random number generator to obtain an output that is utilized in cryptographic operations. For the reasons noted above with respect to claim 1, it is believed that the recitation previously in claim 19 satisfied the requirements set forth In *Re Bilski*, but, in any event, the claim has been amended to more explicitly recite the operation of the components within the claim and thereby clearly tie the claim to a particular machine.

New independent claim 33 is directed to a security domain having an escrow key and is clearly directed to an apparatus.

As such, it is believed that the Examiners objections under 35 USC 101 are addressed and overcome.

Rejections under 35 USC 102

The Examiner has rejected claims 1 through 18 under 35 USC 102(e) in view of US Patent 7,200,225 to Schroeppel. The Schroeppel reference discloses in Figure 3 the provision of a key number generator identified as item 72. From the description in the Schroeppel reference, it is believed that the key number generator is the random number generator referred to in the present application. A review of the teachings of Schroeppel with respect to item 72 and the careful consideration of the passage referred to by the Examiner, does not however disclose any discussion of the features recited in claim 1. The Schroeppel reference is relatively vague when it comes to the features of the key number generator 72 and indicates it may take a number of different configurations. However, none of those configurations mention or suggest the provision of a pair of inputs each of which is representative of a coordinate of an elliptic curve point and with at least one of those inputs being verifiably random. There is no disclosure in Schroeppel of any input to the random number generator nor of any verifiable random nature to such an input.

Schroeppel does not appear to disclose either the pair of inputs to the elliptic curve random number generator, or that the inputs are representative at least one coordinate of elliptic curve point and that at least one of those inputs is verifiably random.

As such, claim 1 is believed to clearly and patentably distinguish over the art applied by the Examiner.

Claims 2 through 12 and 20 through 21 depend either directly or indirectly upon claim 1 and as such are also believed to patentably distinguish over the Schroeppel reference.

Claim 13 likewise recites the provision of a pair of inputs each representative of at least one coordinate of a pair of elliptic curve points, which features cannot be found in Schroeppel. Moreover, claim 13 recites the passing of the output through a one way function to obtain a bit string for use as a random number. No such provision is taught in Schroeppel. Whilst Schroeppel does show hash functions identified generically as 78 in Figure 8, it would appear that these are utilized to operate upon the keys that have been generated rather than to be utilized in the generation of the keys themselves. It would appear that the provision of the functions identified in 78 relate to the provision of other cryptographic operations, not to the generation of random number strings for use as keys.

As such, it is believed that claim13 clearly and patentably distinguishes over the reference to Schroeppel and as such is in condition for allowance. The claims dependent upon claim 13 likewise are believed to patentably distinguish over Schroeppel and further consideration to allowance of those claims is respectfully requested.

Claim 19 is directed to the establishment of an escrow key through the operation of a random number generator in which the inputs to the random number generator are maintained in a particular relationship that is stored by an administrator as an escrow key. The Examiner has rejected claim 19 in view of a reference to Boneh. Boneh however is silent as to any provision of an escrow key obtained through a particular arrangement of elliptic curve random number generator. There is no reference cited by the Examiner of an elliptic curve random number generator, nor such a random number generator having a pair of inputs and no reference to a pair of inputs to such a generator having a particular relationship which is used as an escrow key.

Claim 19 specifically recites the nature of the inputs, the operation of the random number generator to obtain an output and the storing of the relationship between the inputs as an escrow key with an administrator. None of these features can be found in the Boneh reference as understood by the Applicants and as such it is believed that claim 19 clearly and patentably distinguishes over the Boneh reference. New claims 30 to 32 depend on claim 19 and are similarly

believed to patentably distinguish over Boneh.

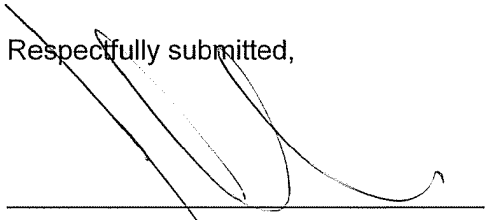
New claims 33 to 36 are directed to a security domain and recite features not found in Boneh.

In summary, the Applicants have carefully considered the references cited by the Examiner and the particular passages referred to by the Examiner. However, the teachings of those references do not appear to be relevant to the subject matter claimed in each of the independent claims submitted herewith. It is believed therefore that the claims clearly and patentably distinguish over those references.

In the event that the Applicant's have not appreciated the specific teachings upon which the Examiner relies, the Examiner is respectfully requested to provide a more detailed analysis of the references and the manner in which they are believed to teach the invention recited in the claims submitted herewith.

Further consideration of the claims and action to allowance is respectfully requested.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29725

Date: October 23, 2009

BLAKE, CASSELS & GRAYDON LLP
199 Bay Street
Suite 2800, Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: 416-863-3164
JRO/sp

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) (Large Entity)	Docket No. 67539/00622

In Re Application Of: **BROWN, Daniel R.L. et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
11/336,814	January 23, 2006	LAKHIA, Viral S.	27871	4144	1834

Invention: **ELLIPTIC CURVE RANDOM NUMBER GENERATION**

COMMISSIONER FOR PATENTS:

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the Office Action of **June 23, 2009** (*Date*) in the above-identified application.

The requested extension is as follows (check time period desired):

☒ One month ☐ Two months ☐ Three months ☐ Four months ☐ Five months

from: **September 23, 2009** (*Date*) until: **October 23, 2009** (*Date*)

The fee for the extension of time is **$130** and is to be paid as follows:

☐ A check in the amount of the fee is enclosed.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. **02-2553**

☐ If an additional extension of time is required, please consider this a petition therefor and charge any additional fees which may be required to Deposit Account No. **02-2553**

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **October 23, 2009**

John R.S. Orange (Registration No. 29,725)
Blake, Cassels & Graydon LLP
Box 25, Commerce Court West
199 Bay Street
Toronto, Ontario
M5L 1A9 Canada

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

_____.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

cc:

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	John Robert Scoley Orange/Judith Martin
Attorney Docket Number:	67539/622

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	1202	16	52	832
Independent claims in excess of 3	1201	1	220	220
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	130	130
Miscellaneous:				
			Total in USD ($)	**1182**

Electronic Acknowledgement Receipt

EFS ID:	6323698
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Correspondence Address:	Blake, Cassels & Graydon LLP - Commerce Court West P.O. Box 25 Toronto ON M5L 1A9 CA - -
Filer:	John Robert Scoley Orange/Judith Martin
Filer Authorized By:	John Robert Scoley Orange
Attorney Docket Number:	67539/622
Receipt Date:	23-OCT-2009
Filing Date:	23-JAN-2006
Time Stamp:	17:40:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1182

RAM confirmation Number	4064
Deposit Account	022553
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		35404-US-PAT_OAresponse.pdf	691585 98ecba94f47668285b3edf81c1272da385ece888	yes	11

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	10
Extension of Time	11	11

Warnings:

Information:

2	Fee Worksheet (PTO-875)	fee-info.pdf	33492 2b16c824056aae972a85f35e70dba7827a61cec0	no	2

Warnings:

Information:

Total Files Size (in bytes):	725077

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/336,814	Filing Date 01/23/2006	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	10/23/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 36	Minus	** 20	= 16	X $ =		OR	X $52=	832
	Independent (37 CFR 1.16(h))	* 5	Minus	***4	= 1	X $ =		OR	X $220=	220
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**1052**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/JAMES ELLIOTT/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
11/336,814		2431	

OC000000039112394

Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 91704 on 12/04/2009

- **Correspondence Address**
- **Maintenance Fee Address**
- **Power of Attorney Address**

The address of record for Customer Number 91704 is:

91704
Blake, Cassels & Graydon LLP
199 BAY STREET , SUITE 2800
COMMERCE COURT WEST
TORONTO, ON M5L 1A9
CANADA

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	11/336,814
Filing Date	January 23, 2006
First named Inventor	BROWN, Daniel R.L.
Art Unit	4144
Examiner Name	LAKHIA, Viral S.
Attorney Docket Number	67539/00622

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3]	Number[4]	Kind-Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		WO	01/13218	A1	02-22-2001	SIEMENS AG		
		CA	2,381,397	A1	02-22-2001	SIEMENS AG		

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] **Applicants' unique citation designation number** (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	11/336,814
Filing Date	January 23, 2006
First named Inventor	BROWN, Daniel R.L.
Art Unit	4144
Examiner Name	LAKHIA, Viral S.
Attorney Docket Number	67539/00622

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalogue, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
		JOHNSON, Don B.; "X9.82 Part 3 – Number Theoretic DRBGs"; NIST RNG Workshop; July 20, 2004; Retrieved from http://csrc.nist.gov/groups/ST/toolkit/documents/rng/NumberTheoreticDRBG.pdf	
		PRINS, Leendert; supplementary European Search Report from corresponding EP Application No. 06704329.9; search completed October 29, 2009	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] **Applicants' unique citation designation number** (optional). [2] Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C> 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. Februar 2001 (22.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/13218 A1

(51) Internationale Patentklassifikation[7]: G06F 7/58, H04L 9/32 // G06F 7/72

(21) Internationales Aktenzeichen: PCT/DE00/02776

(22) Internationales Anmeldedatum:
16. August 2000 (16.08.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 39 059.2 18. August 1999 (18.08.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HESS, Erwin** [DE/DE]; Gottfried-Keller-Strasse 36, D-85521 Ottobrunn (DE). **SERF, Pascale** [DE/DE]; Max-Löw-Strasse 61, D-85579 Neubiberg (DE).

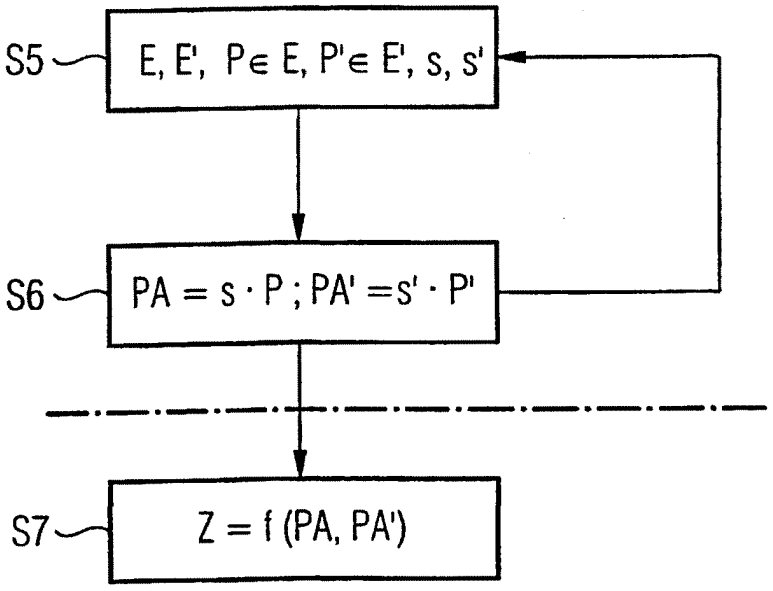
(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, D-80506 München (DE).

(81) Bestimmungsstaaten *(national)*: CA, JP, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR GENERATING PSEUDO RANDOM NUMBERS AND METHOD FOR ELECTRONIC SIGNATURES

(54) Bezeichnung: VERFAHREN ZUM ERZEUGEN VON PSEUDOZUFALLSZAHLEN UND VERFAHREN FÜR ELEKTRONISCHE SIGNATUR



(57) Abstract: The invention relates to a method for generating pseudo random numbers and a method for electronic signatures. According to the inventive method for generating pseudo random numbers, points are determined on at least two different elliptical curves. A pseudo random number is produced respectively by linking the points. The linking of points of different elliptical curves to generate a pseudo random number makes it impossible to deduce the individual elliptical curves on the basis of the pseudo random numbers. The cryptographic security of the inventive method is thus tremendously increased because the computation of discrete logarithms is made impossible.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Erzeugen von Pseudozufallszahlen, sowie ein Verfahren für elektronische Signatur. Bei dem erfindungsgemäßen Verfahren zum Erzeugen von Pseudozufallszahlen werden Punkte auf zumindest zwei verschiedenen elliptischen Kurven bestimmt, und durch Verknüpfen der Punkte wird jeweils eine Pseudozufallszahl erzeugt. Das Verknüpfen der Punkte von unterschiedlichen elliptischen Kurven zu einer Pseudozufallszahl macht Rückschlüsse aus den so erzeugten Pseudozufallszahlen auf die einzelnen elliptischen Kurven unmöglich, wodurch die kryptographische Sicherheit des erfindungsgemäßen Verfahrens erheblich erhöht wird, weil die Berechnung diskreter Logarithmen unmöglich gemacht wird.

WO 01/13218 A1

(84) **Bestimmungsstaaten** *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:

— *Mit internationalem Recherchenbericht.*

— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Verfahren zum Erzeugen von Pseudozufallszahlen und Verfahren für elektronische Signatur

Die Erfindung betrifft ein Verfahren zum Erzeugen von Pseudozufallszahlen und ein Verfahren für elektronische Signatur.

Zufallszahlen werden in der Kryptographie zum Verschlüsseln oder Signieren von Nachrichten benötigt. Im Artikel „Vom diplomatischen Code zur Falltürfunktion" von Otto Leiberich, Spektrum der Wissenschaft, Juni 1999, Seite 26 bis 34 wird ein Überblick über die Entwicklung der Kryptographie in Deutschland gegeben. Hierin ist ein früher verwendetes Wurm- oder Stromchiffrierverfahren beschrieben, bei dem eine sehr lange Zeichenfolge, die keinerlei innere Struktur aufweist, ein sogenannter Zeichenwurm oder Zeichenstrom, Zeichen für Zeichen zu einer zu verschlüsselnden Nachricht, dem Klartext, addiert wird. Sind es Buchstaben, werden sie zunächst nach dem Schema a = 0, b = 1, ..., z = 25 in Zahlen verwandelt. Damit keine größeren Zahlen als 25 entstehen, wird eine Addition modulo 26 durchgeführt. Im Zeitalter der Computer werden die Texte in binäre Zahlen verwandelt und Nullen und Einsen modulo 2 addiert. Der Empfänger subtrahiert vom empfangenen Geheimtext den Zeichenstrom - modulo 26 bzw. 2 - und gewinnt dadurch den Klartext zurück.

Der Zeichenstrom wird mit Hilfe von Zufallszahlengeneratoren erzeugt. Diese beruhten früher auf hochfrequenten Spannungsschwankungen bestimmter Röhren, sogenannter Thyratrons, und später auf radioaktiven Zerfallsereignissen.

Da jedoch die Zeichenströme jeweils parallel vom Sender zum Empfänger sicher übertragen werden müssen, ist ein erheblicher Durchsatz an sicherem Datentransfer notwendig.

Man hat deshalb Verfahren zum Erzeugen von Pseudozufallszahlen, sogenannte Pseudozufallszahlengeneratoren, entwikkelt, die in Abhängigkeit von einem Schlüssel eine im wesentlichen beliebig lange Folge von Pseudozufallszahlen erzeugen können. Hierdurch mußte bei obigem Codierverfahren lediglich ein Schlüssel zwischen den Kommunikationspartnern geheim übermittelt werden, was wesentlich einfacher handhabbar ist, als jeweils einen kompletten Zeichenstrom zu übermitteln.

Für heutige offene Netze, insbesondere das Internet, sind Verfahren entwickelt worden, bei denen zwei Kommunikationspartner, die zum ersten Mal miteinander kommunizieren wollen, sich verschlüsselte Nachrichten übersenden können. Diese Verfahren sind sogenannte asymmetrische Schlüsselverfahren, die auch als Public-Key-Verfahren bezeichnet werden, bei welchen der Empfänger seinen Schlüssel, den sogenannten Public Key, veröffentlicht.

Eines der bekanntesten Verfahren dieses Typs ist das sogenannte RSA-Verfahren, bei dem Teile der Schlüssel, die sogenannten Schlüsselmoduln, Produkte zweier großer Primzahlen sind. Der Sender der Nachricht kennt lediglich den Schlüsselmodul, also das Produkt, und kann mit diesem nach einer bestimmten mathematischen Funktion die Nachricht verschlüsseln. Zur Entschlüsselung der Nachricht genügt jedoch nicht die Kenntnis des Produktes, sondern man benötigt die beiden Primzahlen. Mit Hilfe dieser Primzahlen und einer entsprechenden Umkehrfunktion kann nur der richtige Empfänger, der den Schlüssel erzeugt hat, die verschlüsselte Nachricht entschlüsseln.

Die Zerlegung des Schlüsselmoduls in seine Teiler, die beiden Primzahlen, ist bei großen Moduln mit normalem Rechenaufwand praktisch nicht möglich. In „Faktorisierung großer Zahlen" von Johannes Buchmann, Spektrum der Wissenschaft, September 1996, Seite 80 - 88 ist das Problem der Zerlegung großer Zahlen in ihre Primzahlen ausführlich beschrieben und der Auf-

wand zur Zerlegung einer 129stelligen Zahl dargelegt. Diese Zahl wurde mit Hilfe von 600 Freiwilligen, die ihre Computer zur Verfügung gestellt haben, in die einzelnen Primzahlen zerlegt.

Nachteilig an dem RSA-Verfahren ist, daß es zu langsam für die Nachrichtenverschlüsselung ist, da zur Gewährleistung einer ausreichenden Sicherheit sehr große Zahlen - ungefähr 1000 Binär- oder 300 Dezimalstellen - verwendet werden müssen. Es sind derart große Zahlen mit anderen gleicher Größenordnung zu potenzieren, was zur Verschlüsselung von zu übertragenden Daten nicht schnell genug erfolgen kann. Das RSA-Verfahren wird deshalb lediglich zur verschlüsselten Übertragung von geheimzuhaltenden Schlüsseln für ein herkömmliches Verfahren verwendet, das dann die eigentliche Verschlüsselung vollzieht.

Als Alternative zu dem RSA-Verfahren sind Verfahren auf Grundlage von elliptischen Kurven entwickelt worden. Für die Kryptographie sind lediglich elliptische Kurven über endlichen Körpern relevant. Diese elliptischen Kurven über endlichen Körpern bilden Punktgruppen, in denen eine Addition und eine Multiplikation definiert sind, die mit der landläufigen Addition und Multiplikation nichts gemeinsam haben als die Rechenregeln. Die Multiplikation auf einer elliptischen Kurve über einem endlichen Körper ist eine Einwegfunktion, das heißt, daß die Umkehrung - die Berechnung sogenannter diskreter Logarithmen - im Normalfall rechentechnisch undurchführbar ist, wohingegen die Multiplikation sehr einfach und schnell ausgeführt werden kann. Diese Tatsache wird bei den auf elliptischen Kurven basierenden kryptographischen Verfahren ausgenutzt, indem der Empfänger sich eine Zufallszahl t wählt und auf Grundlage dieser Zufallszahl t und einer Multiplikation mit t auf der elliptischen Kurve einen Kurvenpunkt T bestimmt. Der Kurvenpunkt T wird als Schlüssel veröffentlicht, wohingegen die Zufallszahl t vom Empfänger geheimgehalten wird. Ein Sender kann mit Hilfe des Kurvenpunktes T

seine Nachricht verschlüsseln, die dann lediglich der Empfänger, der die dem Kurvenpunkt T zugrundeliegende Zufallszahl t kennt, entschlüsseln kann.

Solche auf elliptischen Kurven basierende Verfahren benötigen bei gleicher Sicherheit wie das RSA-Verfahren wesentlich weniger Rechenleistung. Derartige Verfahren können in Kleinstrechnern implementiert werden, wie z.B. in Chipkarten. Die Siemens AG vertreibt eine Chipkarte mit der Markenbezeichnung SLE44CR80S, in der ein Signaturverfahren auf der Basis elliptischer Kurven implementiert ist.

Zur Erzeugung der Schlüssel, des öffentlichen Schlüssels, den der Empfänger veröffentlicht, und seines entsprechenden privaten Schlüssels, werden wiederum Zufallszahlen benötigt.

Der Erfindung liegt deshalb die Aufgabe zugrunde, auf Basis elliptischer Kurven ein Verfahren zum Erzeugen von Pseudozufallszahlen zu schaffen, das einfach und schnell ausführbar ist und mit dem eine große Menge qualitativ hochwertiger Zufallszahlen erzeugt werden kann.

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 1 gelöst.

Ferner liegt der Erfindung die Aufgabe zugrunde, ein Verfahren für elektronische Signatur auf Basis elliptischer Kurven sowie eine entsprechende Vorrichtung zu schaffen, die weniger Speicherplatz als bekannte Verfahren und Vorrichtungen für elektronische Signatur auf Grundlage elliptischer Kurven benötigen und auf kleinen Rechensystemen, insbesondere Chipkarten, implementiert werden können.

Die Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 11 und eine Vorrichtung mit den Merkmalen des Anspruchs 12 gelöst.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

Beim erfindungsgemäßen Verfahren nach Anspruch 1 zum Erzeugen von Pseudozufallszahlen werden Paare von Punkten bestimmt, die auf zumindest zwei unterschiedlichen elliptischen Kurven über einem endlichen Körper liegen, und in Abhängigkeit von jeweils einem solchen Paar von Punkten wird eine Zufallszahl ermittelt.

Da erfindungsgemäß zwei verschiedene elliptische Kurven benutzt werden, und die Pseudozufallszahl aus einem Paar von Punkten abgeleitet wird, wobei die beiden Punkte des Paares auf unterschiedlichen elliptischen Kurven liegen, ist es unmöglich, aus den derart ermittelten Pseudozufallszahlen auf die Kurvenpunkte zurückzuschließen. Bei Verwendung lediglich einer einzigen elliptischen Kurve zum Ableiten von Pseudozufallszahlen könnte durch Berechnen diskreter Logarithmen aus den Pseudozufallszahlen auf die Kurvenpunkte zurückgeschlossen werden. Hierdurch wäre es möglich, daß Dritte die Rechenregel der Pseudozufallszahlen bestimmen könnten und die weiteren Pseudozufallszahlen voraussagen könnten. Dies würde ein erhebliches Sicherheitsrisiko darstellen, das mit der vorliegenden Erfindung vermieden wird.

Das erfindungsgemäße Verfahren für elektronische Signatur kombiniert ein an sich bekanntes Signaturverfahren mit dem erfindungsgemäßen Verfahren zum Erzeugen von Pseudozufallszahlen. Die gleichen Routinen bzw. Einrichtungen können sowohl beim Signaturverfahren als auch bei der Erzeugung der Zufallszahlen verwendet werden, wodurch erheblich Programmcode und Speicherplatz eingespart werden kann. Zudem wirkt sich eine Optimierung der EC(=elliptic curve)-Arithmetik sowohl bei der Erzeugung der Pseudozufallszahlen als auch bei der unmittelbaren Ausführung des Signaturverfahrens vorteilhaft aus. Durch diese doppelte Verwendung der

Routinen und Einrichtungen auf Basis elliptischer Kurven werden somit Synergieeffekte erzielt.

Ferner sind die erfindungsgemäß erzeugten Pseudozufallszahlen nicht von Zufallszahlen eines echten Zufallsgenerators zu unterscheiden und können mit relativ geringem Rechenaufwand erzeugt werden.

Die Erfindung wird nachfolgend beispielhaft anhand der Zeichnungen näher erläutert. In denen zeigen schematisch:

Fig. 1 eine elliptische Kurve über den reellen Zahlen,

Fig. 2 eine elliptische Kurve über einem endlichen Körper,

Fig. 3 die Addition zweier Punkte einer elliptischen Kurve über den reellen Zahlen,

Fig. 4 die Punkte der elliptischen Kurve $y^2=x^3+2x+9$ über dem Körper mod 13, die eine zyklische Gruppe mit 17 Punkten bilden,

Fig. 5 den Verfahrensablauf eines Ausführungsbeispiels der Erfindung in einem Flußdiagramm,

Fig. 6 das Grundprinzip des erfindungsgemäßen Verfahrens zum Erzeugen von Pseudozufallszahlen in einem Flußdiagramm, und

Fig. 7 den Aufbau eines Programmes zum Ausführen eines erfindungsgemäßen Signaturverfahrens.

Zunächst werden kurz die mathematischen Grundlagen zum Rechnen auf elliptischen Kurven erläutert. Eine elliptische Kurve E über einem Körper K ist eine Kurve, die durch eine kubische Gleichung der Form:

$y^2=x^3+ax+b$,

beschrieben werden kann mit a und b aus K, $4a^3+27b^2 \neq 0$. Paare (x, y) aus K x K, welche die Gleichung erfüllen, sowie das formale Paar (∞,∞) nennt man Punkte der Kurve E über K.

Eine elliptische Kurve über den reellen Zahlen ist in Fig. 1 gezeigt. Man beachte, daß elliptische Kurven keine Ellipsen sind.

Fig. 2 zeigt eine elliptische Kurve über einem endlichen Körper. Der algebraische Begriff Körper definiert einen „Zahlenbereich", in dem man nach den von den rationalen Zahlen bekannten formalen Rechenregeln addieren, subtrahieren, multiplizieren und dividieren kann. Es gibt unendliche Körper, wie z.B. die rationalen Zahlen, die reellen Zahlen, die komplexen Zahlen, und endliche Körper. Endliche Körper sind z.B. der Körper GF(p) der Zahlen mod p, wobei p eine Primzahl ist, bzw. der Körper $GF(2^n)$ der Binärvektoren der Länge n. („GF" steht für „Galois field", was ein Synonym für „endlicher Körper" ist.) Für die Kryptographie sind nur elliptische Kurven über endlichen Körpern relevant.

Fig. 3 zeigt die Addition zweier Punkte P_1, P_2 auf einer elliptischen Kurve über den reellen Zahlen, wobei sich der Punkt P_3 ergibt. Bei dieser Addition wird die Verbindungsgerade der Punkte P_1 und P_2 gebildet und deren 3. Schnittpunkt mit der elliptischen Kurve ermittelt. Dieser Schnittpunkt wird an der x-Achse gespiegelt und ergibt das Resultat P_3 der Addition von P_1 und P_2.

Diese Addition der Punkte auf elliptischen Kurven kann durch folgende Formeln ausgedrückt werden:

$x_3=r^2-x_1-x_2$, $y_3=r(x_1-x_3)-y_1$ mit
$r=(y_2-y_1)/(x_2-x_1)$, falls $x_1 \neq x_2$
$r=(3x_1^2+a)/2y_1$, falls $P_1=P_2$

wobei x_i, y_i die Koordinaten des Punktes P_i (i=1,2,3) sind.

Diese Formeln gelten auch für elliptische Kurven über endlichen Körpern.

Durch Iteration der Punktaddition wird eine Multiplikation von Kurvenpunkten mit ganzen Zahlen k definiert:

k*P=P+P+...+P (k-fache Summe).

Diese Multiplikation von Kurvenpunkten mit ganzen Zahlen kann leicht und schnell ausgeführt werden, wohingegen die Umkehraufgabe, die Berechnung sogenannter diskreter Logarithmen, normalerweise nur mit außergewöhnlichem Rechenaufwand gelöst werden kann. Hierfür gibt es keinen Algorithmus mit subexponentieller Laufzeit. Diese Punktmultiplikation stellt somit eine Einwegfunktion dar, weshalb sie bei Verfahren mit öffentlichen Schlüsseln, den sogenannten Public-Key-Verfahren, verwendet wird.

Nachfolgend wird anhand eines in Fig. 5 gezeigten Ausführungsbeispieles das erfindungsgemäße Verfahren zum Erzeugen von Pseudozufallszahlen erläutert.

Eine erste elliptische Kurve E über dem Körper GF(p) ist durch die folgende Gleichung gegeben:

$(y^2) \bmod p = (x^3 + 6x +$
$60506790344184654738821496604545520695293840677 1) \bmod p,$
wobei $p = 2^{160}-47=$
1461501637330902918203684832716283019655932542929.
p ist eine Primzahl mit 160 Bits.

Die elliptische Kurve E über GF(p) besitzt als Gruppenordnung
#E(GF(p)) = 7*q mit
q=208785948190128988314812461240940947434505754881.
q ist wiederum eine Primzahl mit 128 Bits.

Die Gruppenordnung einer elliptischen Kurve ist die Anzahl der Elemente der Punktgruppe, also die Anzahl der Lösungen der definierenden Gleichung der elliptischen Kurve E über GF(p). Je größer der maximale Primteiler der Gruppenordnung ist, desto schwieriger ist die Berechnung diskreter Logarithmen. Die Größe der Gruppenordnungen und ihrer maximalen Primteiler stellt somit ein Qualitätsmerkmal des erfindungsgemäßen Verfahrens dar, wobei die Gruppenordnungen vorzugsweise zumindest 2^{100} oder besser 2^{130} betragen sollten.

Eine zweite elliptische Kurve E' über GF(p) ist durch folgende Gleichung gegeben:

$(y^2) \bmod p = (x^3 + 3x + 168756385740498547400152923318200148712149363991) \bmod p.$

Die Kurve E' ist isogen zur Kurve E, das heißt, wenn die Kurve E die Form

$$y^2=x^3+ax+b$$

aufweist, besitzt die Kurve E' die Form

$$y^2=x^3+ac^2x+bc^3,$$

mit a, b, c aus GF(p), wobei c ein quadratischer Nichtrest modulo p ist. Im vorliegenden Fall gilt für c:

$c= 503145425704462245322517599589013227703324936803.$

Die Verwendung zweier isogener Kurven statt zweier beliebiger Kurven bietet wesentliche Vorteile. So kann man die Ordnung der elliptischen Kurve E' über GF(p) einfach aus der Gruppenordnung von E ableiten, da nämlich die Summe der beiden Ordnungen 2p+2 ist, womit sich folgende Gleichung ergibt:

$$\#E'(GF(p)) = 2p+2 - \#E(GF(p))$$

Im vorliegenden Fall ergibt sich für die Gruppenordnung von E':

$$\#E'(GF(p)) = 2p+2 - \#E(GF(p)) = 11 * 19 * q'$$

mit

$$q' = 458150983489311259624978820296545268736778934 7.$$

q' ist eine Primzahl mit einer Länge von 152 Bits.

Man wählt nun zwei Punkte P, P' der Kurven E, E', wie z.B.:

P =(27,1199480719563308855489368355308026541006624847440)

P' =(318,767790262932904318810390534329377261151321453045),

und

zwei Startwerte s, s', z.B. s=s'=2.

Durch die Bestimmung der elliptischen Kurven E, E', der Punkte P, P' und der Startwerte s, s' ist der Schritt S1 aus Fig. 5 abgeschlossen. Der Verfahrensablauf geht nun auf den Schritt S2 über, bei dem die Punkte P, P' mit s bzw. s' multipliziert werden, wobei das Ergebnis als PA bzw. PA' bezeichnet wird. Die Multiplikation wird als s-fache bzw. s´-fache Addition gemäß der in Fig. 3 gezeigten Addition ausgeführt.

Die Punkte PA und PA' werden der Vorschrift zum Ermitteln von Zufallsbits übergeben (Schritt S3). Im vorliegenden Fall werden die x-Koordinaten der beiden Punkte PA und PA' mit XOR verknüpft und durch c geteilt.

Für isogene elliptische Kurven E und E´ gilt, daß für ein beliebiges x aus GF(p) x entweder x-Koordinate von zwei verschiedenen Punkten auf E ist, oder aber x ist x-Koordinate eines Punktes auf E und cx ist x-Koordinate eines Punktes auf E', oder aber x ist nicht x-Koordinate eines Punktes auf E,

aber cx ist x-Koordinate von zwei Punkten auf E'. Wenn man also die x-Koordinaten auf E' durch c teilt, dann kommt jedes beliebige x aus GF(p) genau 2x als x-Koordinate vor. Das heißt, wenn man eine x-Koordinate auf E mit einer x-Koordinate auf E' geteilt durch c verknüpft, ist das äquivalent zum Verknüpfen zweier beliebiger, zufälliger Werte zwischen 0 und p-1. Die hierdurch abgeleiteten Pseudozufallsbits verhalten sich also wie echte Zufallsbits.

Vom Schritt S2 werden die Punkte PA und PA' auch an den Schritt S4 übergeben, bei dem die Punkte P, P' unverändert bleiben und s bzw. s' jeweils um eins erhöht wird.

Vom Schritt S4 geht der Verfahrensablauf wieder auf den Schritt S2 über, bei dem wiederum neue Punkte PA und PA' gebildet werden, die dann wieder an den Schritt S3 zur Berechnung weiterer Zufallsbits und an den Schritt S4 übergeben werden. Dieser Verfahrensablauf kann vielfach wiederholt werden, wobei immer wieder neue Zufallsbits erzeugt werden.

Die Erfinder der vorliegenden Erfindung haben mit dem oben beschriebenen Verfahren zum Erzeugen von Zufallszahlen 20 x eine Million Zufallsbits erzeugt und diese Zufallsbits verschiedenen statistischen Tests unterzogen. Mit den Tests konnten keine Abweichungen von echten Zufallsbits festgestellt werden.

Für die Erfindung ist wesentlich, daß im Schritt S3 die Zufallszahl Z aus den beiden Punkten PA und PA' ermittelt wird, die von unterschiedlichen elliptischen Kurven E und E' stammen. Durch das Verknüpfen dieser beiden Punkte PA und PA' wird sichergestellt, daß anhand der erzeugten Pseudozufallszahlen nicht die der Berechnung der Punkte PA und PA' zugrunde liegenden Punkte P und P´ durch diskrete Logarithmen ermittelt werden können. Von dem Ergebnis aus S3 kann somit nicht auf das Verfahren zum Erzeugen der Punkte PA, PA' mit

den Schritten S1, S2 und S4 geschlossen werden, was durch die gestrichelte Linie in Fig. 5 dargestellt ist.

Die Erfindung ist nicht auf das in Fig. 5 dargestellte Ausführungsbeispiel beschränkt. Im Rahmen der Erfindung ist es z.B. möglich, im Schritt S3 eine andere Verknüpfung der x-Koordinaten zu wählen. So können z.B. die beiden x-Koordinaten durch eine Addition modulo p miteinander verknüpft werden. Oder aber man verknüpft die y-Koordinaten. Oder aber x- und y-Koordinaten. Im Rahmen der Erfindung ist es auch möglich, daß anstelle von fest vorgegebenen elliptischen Kurven E, E' mit Punkten P, P' nach jeder Berechnung von PA und PA' neue Kurven E*, E*' und Punkte P*, P*' bestimmt werden, die zur Berechnung der nächsten Punkte PA* und PA*' herangezogen werden. Auch die Werte s, s' können an sich beliebig verändert werden. Für die Erfindung ist lediglich wesentlich, daß die Werte s, s' ganze Zahlen sind. Zu Beginn des Verfahrens können sie beispielsweise mit einem einfachen Zufallsgenerator erzeugt werden, der keinen hohen Ansprüchen genügen muß. In Fig. 6 ist das grundsätzliche Prinzip der vorliegenden Erfindung dargestellt, das eine Schleife bestehend aus den Schritten S5 und S6 aufweist, wobei in Schritt S5 zwei elliptische Kurven E, E', zwei Punkte P, P' auf den beiden Kurven und zwei Startwerte s, s' gewählt werden. Im Schritt S6 werden die Punkte P, P' mit s bzw. s' multipliziert, woraus sich PA und PA' ergibt. Bei jeder Wiederholung der Schleife S5, S6 wird zumindest eines der Paare E, E' bzw. P, P' bzw. s, s' verändert. Es ist auch möglich, zwei oder alle 3 Paare nach einer festzulegenden Regel zu verändern.

Bei jeder Wiederholung der Schleife wird ein neues Zahlenpaar PA, PA' erzeugt und dem Verfahrensschritt S7 übergeben, bei dem die beiden Punkte PA und PA' jeweils zu einer Pseudozufallszahl Z verknüpft werden.

Verfahren auf Basis elliptischer Kurven verwenden als Einwegfunktion die Multiplikation auf elliptischen Kurven, weshalb

Vorrichtungen zum Durchführen solcher Verfahren mit Routinen und Einrichtungen für Arithmetik auf elliptischen Kurven versehen sind. Solche Verfahren benötigen zudem Zufallszahlen zum Erstellen der privaten und öffentlichen Schlüssel. Durch Verwenden des erfindungsgemäßen Verfahrens zum Erzeugen dieser Zufallszahlen können zum einen qualitativ hochwertige Pseudozufallszahlen erzeugt, und zum anderen kann der Programmcode gering gehalten werden, da die vorhandenen Routinen doppelt verwendet werden können. Hierdurch werden erhebliche Ressourcen eingespart, und gleichzeitig wird die Sicherheit des Verfahrens deutlich gesteigert.

Fig. 7 zeigt schematisch den Aufbau eines Programmes zum Ausführen des erfindungsgemäßen Verfahrens in einem Blockschaltbild. Das Programm besteht aus einem Teil P1 zum Durchführen des Signaturverfahrens, das auf einen Programmteil P2 zurückgreift, mit dem Multiplikationen auf elliptischen Kurven über endlichen Körpern durchgeführt werden. Der Programmteil P1 wird von einem weiteren Programmteil P3 mit Zufallszahlen versorgt, wobei der Programmteil P3 wiederum auf den Programmteil P2 zum Multiplizieren auf elliptischen Kurven zurückgreift. Am Programmteil P1 ist ein Dateneingangsstrom I und ein Datenausgangsstrom O dargestellt, wobei der Dateneingangsstrom eine zu signierende Nachricht sein kann und der Datenausgangsstrom die Signatur. Ferner kann der Programmteil P1 am Datenausgangsstrom O seinen privaten und öffentlichen Schlüssel ausgeben. Diese Funktionen des Programmteils P1 entsprechen den an sich bekannten Signaturverfahren und -vorrichtungen auf Basis elliptischer Kurven. Das erfindungsgemäße Verfahren kann insbesondere bei Recheneinrichtungen mit geringerer Rechenkapazität, wie z.B. Chipkarten eingesetzt werden, da der entsprechende Programmcode äußerst kompakt ist und die Länge der zu verarbeitenden Zahlen wesentlich kürzer als bei einem RSA-Verfahren gleicher Sicherheitsstufe. Es ist jedoch auch möglich, die Programme auf elektronisch lesbaren Datenträgern zu vertreiben.

Patentansprüche

1. Verfahren zum Erzeugen von Pseudozufallszahlen, bei dem zumindest zwei Punkte (P, P´) von zumindest zwei unterschiedlichen elliptischen Kurven (E, E´) über einem endlichen Körper (GF) bestimmt werden und eine Pseudozufallszahl durch Verknüpfen dieser Punkte (P, P´) erzeugt wird.

2. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 1, d a d u r c h g e k e n n z e i c h n e t, daß zur Bestimmung der Pseudozufallszahl jeweils ein Paar von Punkten (P, P´) bestimmt wird, wobei zur Bestimmung der einzelnen Paare jeweils dieselben zwei elliptischen Kurven (E, E´) verwendet werden.

3. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 2, d a d u r c h g e k e n n z e i c h n e t, daß die beiden elliptischen Kurven (E, E´) zueinander isogen sind.

4. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 3,
d a d u r c h g e k e n n z e i c h n e t, daß die Punkte (P, P´) eines ersten Paares in Abhängigkeit zweier Startwerte (s, s´) bestimmt werden.

5. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 4,
d a d u r c h g e k e n n z e i c h n e t, daß die Punkte (P, P´) der weiteren Paare durch Variieren der Startwerte gemäß einer vorbestimmten Regel bestimmt werden.

6. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 4,
d a d u r c h g e k e n n z e i c h n e t, daß die weiteren Paare von Punkten (P, P´) durch Variieren der elliptischen

Kurven und/oder der Punkte (P, P´) nach einer vorbestimmten Regel bestimmt werden.

7. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 6,
d a d u r c h g e k e n n z e i c h n e t, daß zum Ermitteln einer Zufallszahl die Koordinaten der beiden Punkte (P, P´) miteinander verknüpft werden.

8. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 7,
d a d u r c h g e k e n n z e i c h n e t, daß die x-Koordinaten der beiden Punkte (P, P´) miteinander verknüpft werden, wobei die beiden elliptischen Kurven (E, E´) isogen sind.

9. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 8,
d a d u r c h g e k e n n z e i c h n e t, daß die Punktgruppen (E(GF (p)), E´(GF (p))) der elliptischen Kurven (E, E´) über einem endlichen Körper GF(p) Gruppenordnungen (q bzw. q´) von zumindest 2^{100} und vorzugsweise mindestens 2^{130} aufweisen.

10. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 9,
d a d u r c h g e k e n n z e i c h n e t, daß die elliptischen Kurven über dem endlichen Körper GF(p) definiert sind, wobei p eine Primzahl ist, die größer als 3 ist.

11. Verfahren für elektronische Signatur auf Basis elliptischer Kurven, bei dem die Schlüssel auf Grundlage von Zufallszahlen erzeugt werden,
d a d u r c h g e k e n n z e i c h n e t, daß die Zufallszahlen nach einem Verfahren der Ansprüche 1 bis 10 ermittelt werden.

12. Vorrichtung zur Durchführung des Verfahrens für elektronische Signatur auf Basis elliptischer Kurven nach Anspruch 11, mit

einer Einrichtung zum Ausführen von Multiplikationen in der Punktgruppe einer elliptischen Kurve (E, E´) über einem endlichen Körper (GF(p)),

einer Einrichtung zum Signieren, die die Einrichtung zum Ausführen der Multiplikation verwendet, und

einer Einrichtung zum Erzeugen von Pseudozufallszahlen nach dem Verfahren nach einem der Ansprüche 1 bis 9, wobei auch diese Einrichtung die Einrichtung zum Ausführen der Multiplikation verwendet.

FIG 1

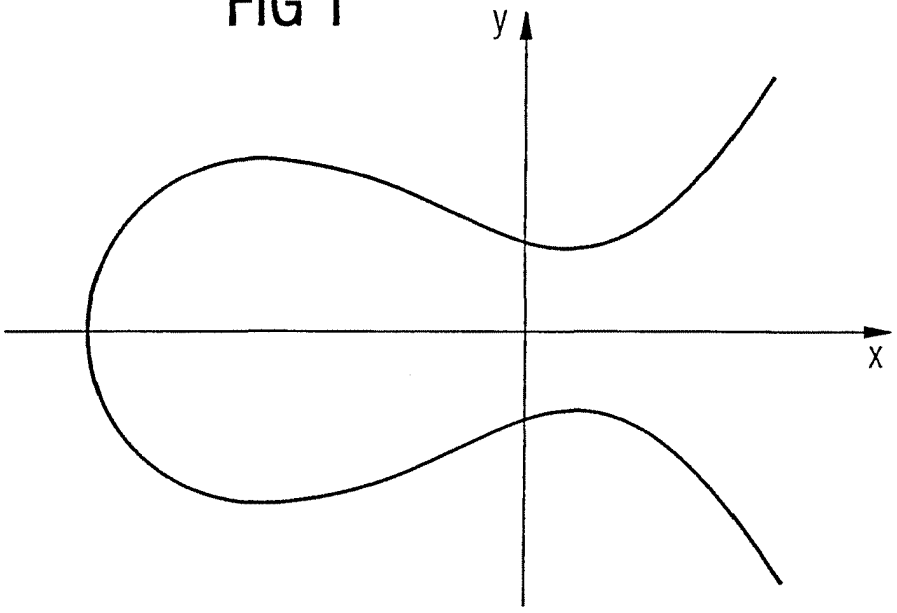


FIG 2

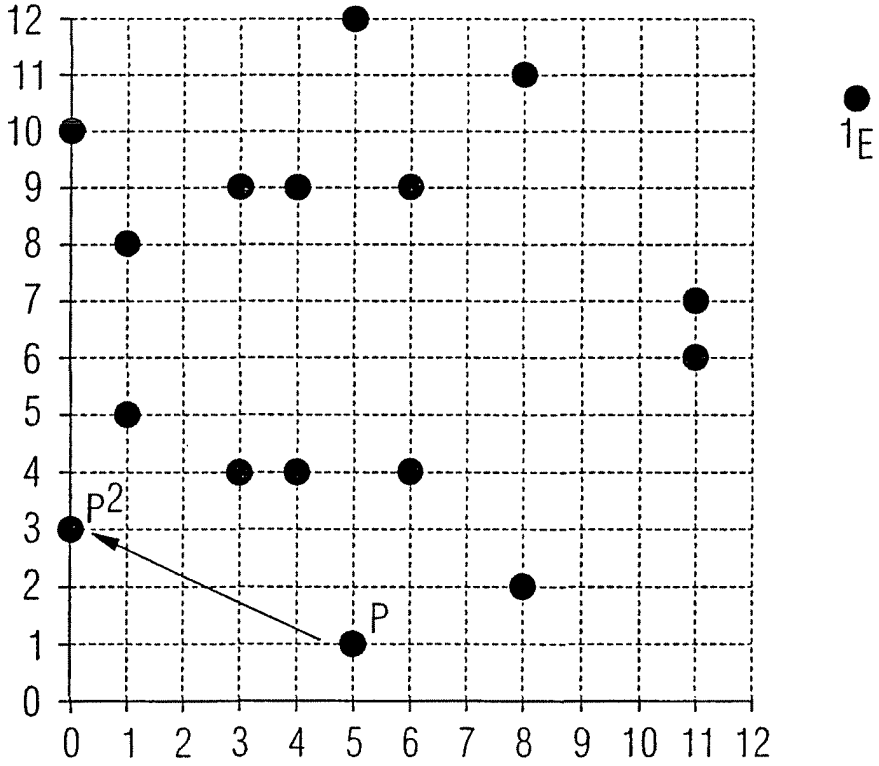


FIG 3

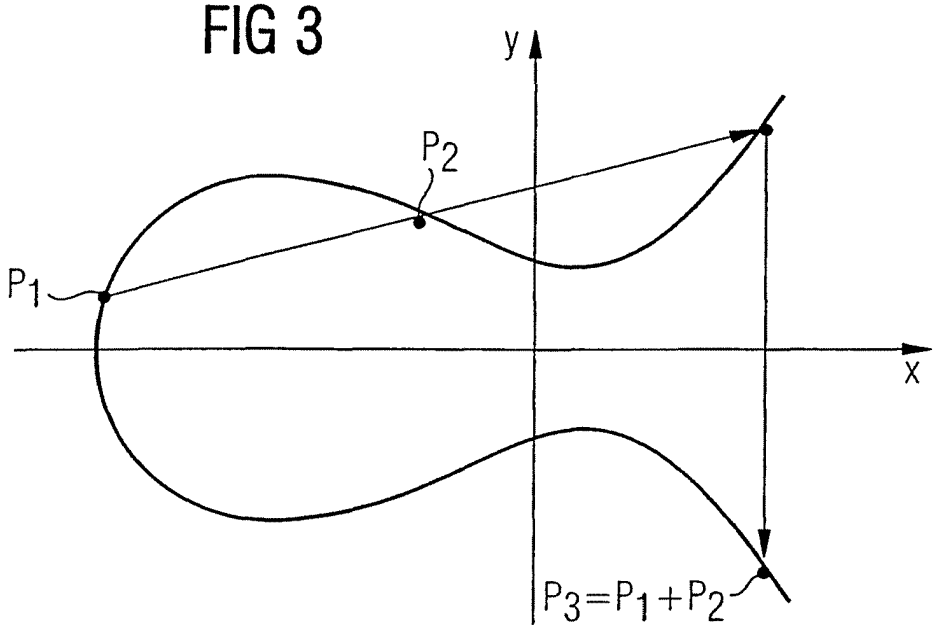


FIG 4

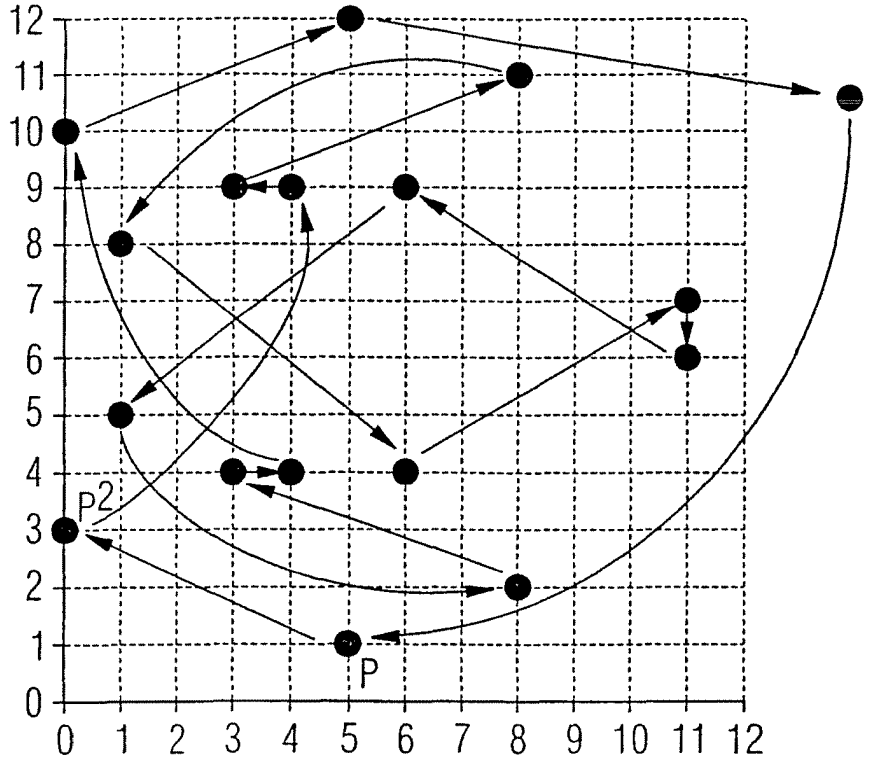


FIG 5

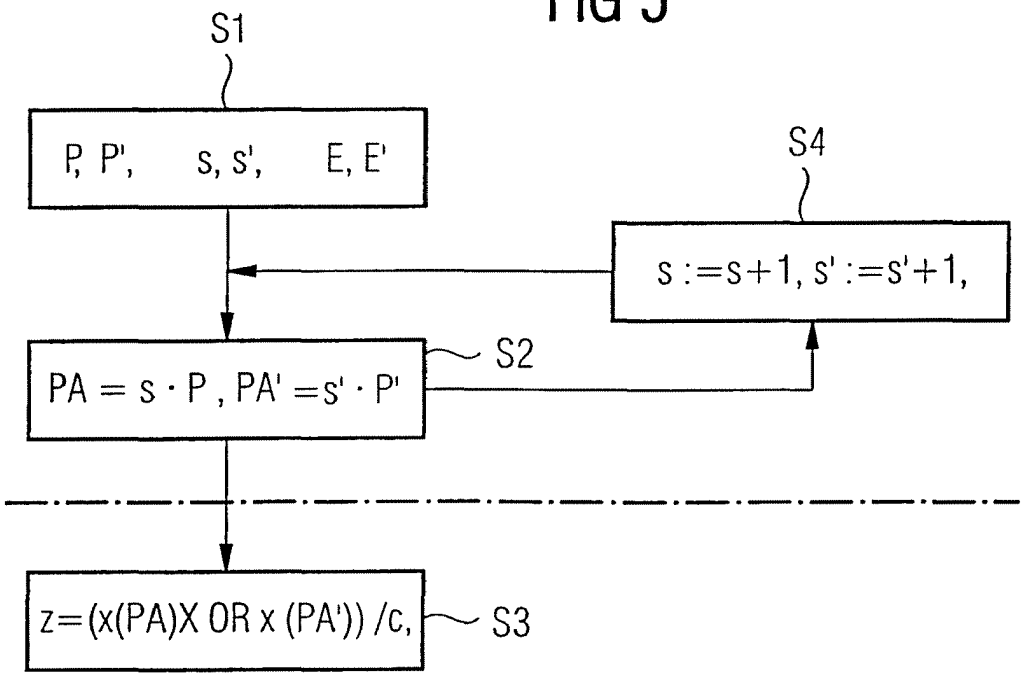

S1
P, P', s, s', E, E'
S4
s :=s+1, s' :=s'+1,
PA = s · P , PA' =s' · P'
S2
z=(x(PA)X OR x (PA')) /c,
S3

FIG 6

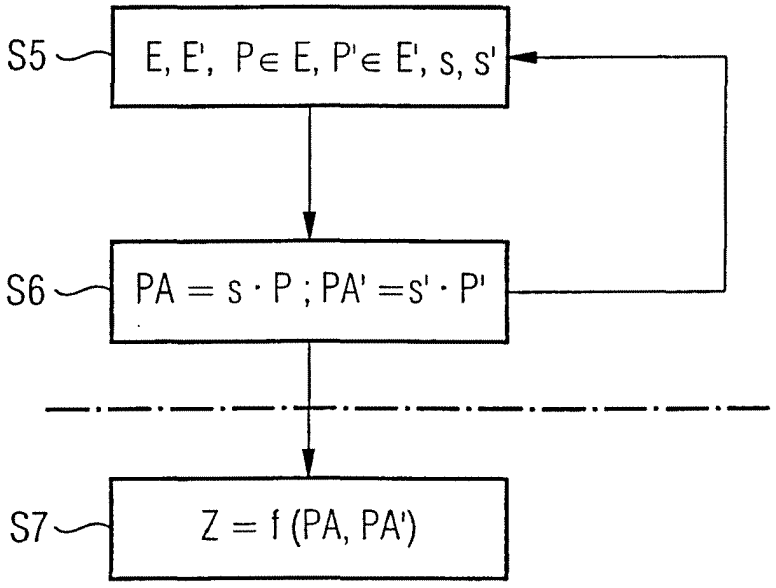
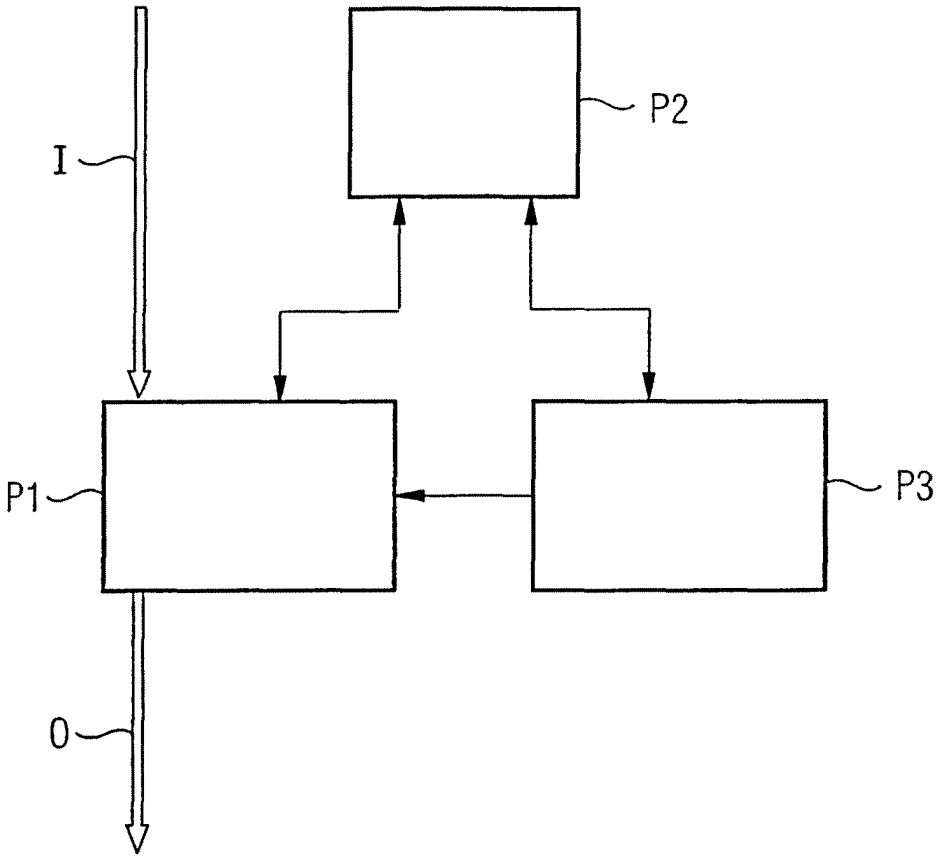

S5
E, E', P∈ E, P'∈ E', s, s'
S6
PA = s · P ; PA' =s' · P'
S7
Z = f (PA, PA')

FIG 7



INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/DE 00/02776

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58 H04L9/32 //G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H03K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KALISKI B S JR: "One-way permutations on elliptic curves" JOURNAL OF CRYPTOLOGY, 1991, USA, vol. 3, no. 3, pages 187-199, XP000972491 ISSN: 0933-2790 page 187, paragraph 1 page 188, paragraph 7 page 194, paragraph 2 -page 196, paragraph 1 ---	1-12
X	KALISKI B S: "A PSEUDO-RANDOM BIT GENERATOR BASED ON ELLIPTIC LOGARITHMS" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 6, 1986, pages 84-103, XP000090665 page 98, line 20 - line 33 -----	1-12

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 December 2000	20/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Verhoof, P

1

INTERNATIONALER RECHERCHENBERICHT

Intern nales Aktenzeichen
PCT/DE 00/02776

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F7/58 H04L9/32 //G06F7/72

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F H03K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	KALISKI B S JR: "One-way permutations on elliptic curves" JOURNAL OF CRYPTOLOGY, 1991, USA, Bd. 3, Nr. 3, Seiten 187-199, XP000972491 ISSN: 0933-2790 Seite 187, Absatz 1 Seite 188, Absatz 7 Seite 194, Absatz 2 -Seite 196, Absatz 1 ---	1-12
X	KALISKI B S: "A PSEUDO-RANDOM BIT GENERATOR BASED ON ELLIPTIC LOGARITHMS" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, Bd. CONF. 6, 1986, Seiten 84-103, XP000090665 Seite 98, Zeile 20 - Zeile 33 -----	1-12

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☐ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
8. Dezember 2000	20/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Verhoof, P

1

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2381397 A1 2001/02/22

(21) 2 381 397

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2000/08/15
(87) Date publication PCT/PCT Publication Date: 2001/02/22
(85) Entrée phase nationale/National Entry: 2002/02/18
(86) N° demande PCT/PCT Application No.: US 2000/022299
(87) N° publication PCT/PCT Publication No.: 2001/013441
(30) Priorité/Priority: 1999/08/16 (09/375,073) US

(51) Cl.Int.^{7}/Int.Cl.^{7} H01M 8/02

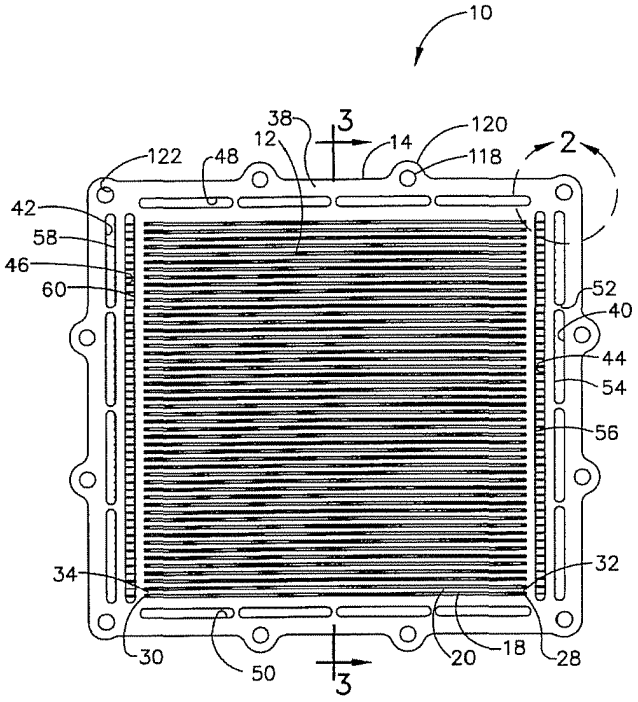
(71) Demandeur/Applicant:
ALLIEDSIGNAL INC., US

(72) Inventeurs/Inventors:
YANG, JEFFERSON, US;
REHG, TIMOTHY, US;
WOODCOCK, GORDON, US;
DESANCTIS, GARETH, US

(74) Agent: CRAIG WILSON AND COMPANY

(54) Titre : PILE A COMBUSTIBLE PRESENTANT DES CAPACITES AMELIOREES DE GESTION DE PRODUIT DE REACTION ET DE CONDENSATION

(54) Title: FUEL CELL HAVING IMPROVED CONDENSATION AND REACTION PRODUCT MANAGEMENT CAPABILITIES



(57) Abrégé/Abstract:
A fuel cell bipolar plate including a plurality of reactant channels (18, 24) defining respective inlets and outlets and at least two flow restrictors (54, 56) respectively associated with at least two adjacent reactant channels.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 February 2001 (22.02.2001)

PCT

(10) International Publication Number
WO 01/13441 A3

(51) International Patent Classification[7]: H01M 8/02

(21) International Application Number: PCT/US00/22299

(22) International Filing Date: 15 August 2000 (15.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/375,073 16 August 1999 (16.08.1999) US

(71) Applicant: **ALLIEDSIGNAL INC.** [US/US]; 101 Columbia Avenue, P.O. Box 2245, Morristown, NJ 07960 (US).

(72) Inventors: **YANG, Jefferson**; 7217 Dapple Circle, Orange, CA 92869 (US). **REHG, Timothy**; 26756 Basswood Avenue, Rancho Palos Verdes, CA 90275 (US). **WOODCOCK, Gordon**; 125 2nd Street, Hermosa Beach, CA 90254 (US). **DESANCTIS, Gareth**; 2556 Aberdeen Avenue, Los Angeles, CA 90027 (US).

(74) Agents: **CRISS, Roger, H.** et al.; AlliedSignal Inc., 101 Columbia Avenue, P.O. Box 2245, Morristown, NJ 07960 (US).

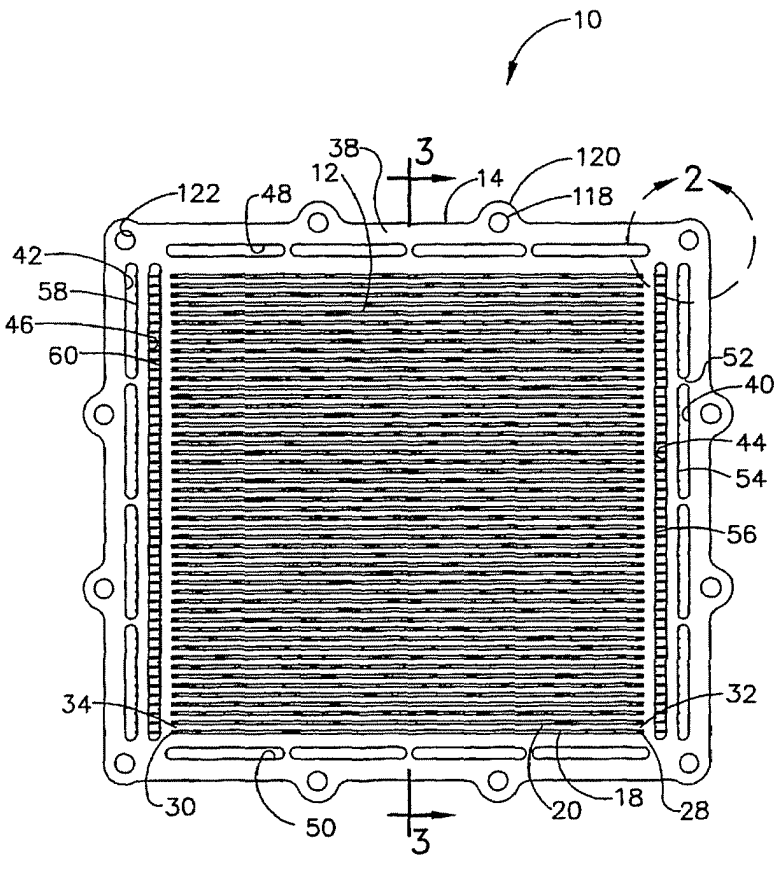
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: FUEL CELL HAVING IMPROVED CONDENSATION AND REACTION PRODUCT MANAGEMENT CAPABILITIES

(57) Abstract: A fuel cell bipolar plate including a plurality of reactant channels (18, 24) defining respective inlets and outlets and at least two flow restrictors (54, 56) respectively associated with at least two adjacent reactant channels.



WO 01/13441 A3

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

(88) Date of publication of the international search report:
7 June 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

FUEL CELL HAVING IMPROVED CONDENSATION AND REACTION PRODUCT MANAGEMENT CAPABILITIES

BACKGROUND OF THE INVENTIONS

1. Field of Inventions

The present inventions relate generally to fuel cells and, more specifically, to the management of condensation and reaction product within fuel cells.

2. Description of the Related Art

A fuel cell converts fuel and oxidant (collectively "reactants") into electricity and a reaction product. Many fuel cells employ hydrogen as the fuel and oxygen as the oxidant. Here, the reaction product is water. One such fuel cell is the proton exchange membrane (PEM) fuel cell. Each individual cell in a PEM fuel cell includes an anode and a cathode separated by a thin, ionically conducting membrane, which together are often referred to as a membrane electrode assembly (MEA). The anode and cathode, on opposing faces of the ionically conducting membrane, are comprised of a thin catalyst containing film and a gas diffusion layer. Hydrogen is supplied to the anode and oxygen supplied to the cathode. The gas diffusion layer insures that hydrogen is effectively transported to the anode catalyst and that oxygen is effectively transported to the cathode catalyst. The hydrogen is electrochemically oxidized at the anode catalyst, thereby producing protons that migrate across the conducting membrane and react with the oxygen at the cathode catalyst to produce water. The individual MEAs

are stacked in electrical series with impermeable electrically conductive bipolar plates therebetween that conduct current between the anode of one MEA and the cathode of the adjacent MEA. The bipolar plates have channels formed on one side for transporting fuel over one MEA and channels formed on the other side for transporting oxidant over an adjacent MEA. The reactants, such as hydrogen and oxygen, are pumped through the channels from respective inlet manifolds to respective outlet manifolds.

Fuel cells are considered an attractive energy source for a variety of reasons. As compared to batteries, fuel cells are advantageous in that they can maintain a specific power output as long as fuel is continuously supplied and are not hampered by a charge/discharge cycle. Fuel cells are also relatively small and lightweight and produce virtually no environmental emissions. PEM fuel cells are particularly advantageous because they have relatively low operating temperatures and employ a non-liquid, non-corrosive electrolyte.

Despite these advantages, conventional fuel cells are susceptible to improvement. For example, reaction products such as water can accumulate within the channels and block reactant flow. Humidity in the reactants can also condense and accumulate within the channels. Conventional fuel cells seek to clear reaction products and condensed humidity from the channels by creating a pressure differential (or drop) between the inlet manifolds and the outlet manifolds. A desirable pressure differential is one that is sufficiently large to prevent reaction products and/or condensate from accumulating in one or more of the channels of the bipolar plate. The requisite pressure drop, which depends on a number of

factors including fuel cell operating conditions (i.e. flow rate and temperature), the material and construction of the bipolar plate channels, and channel geometry, is typically between a few inches of water and 15 PSI.

Pressure is reduced in conventional fuel cells by the effects of wall friction as the reactants move through the channels. More specifically, the conventional method of creating a sufficient wall friction-based pressure differential is to make the reactant channels in the bipolar plates long and tortuous or of a small hydraulic diameter. Alternatively, the reactant flow rates can be increased in order to create greater frictional losses and pressure drops.

The inventor herein has determined that the long, tortuous reactant flow channel method of creating a pressure differential is less than optimal. For example, although it is important that the pressure differential be uniform from channel to channel to insure uniform reactant flow, it is difficult and expensive to create a series of long, tortuous channels of equal length. There are also instances where the use of long, tortuous channels is either impracticable or impossible. For example, hexagonal bipolar plates often include z-shaped flow channels which are not particularly long or tortuous. The geometry of a hexagonal bipolar plate requires the long, tortuous channels to be too far apart to achieve acceptable diffusion of the reactants into the gas diffusion electrode. As such, it is difficult to obtain the requisite pressure differential using conventional long, tortuous channels. In addition, recent advances in bipolar plate technology have resulted in relatively straight reactant flow channels. One such bipolar plate is disclosed in concurrently filed commonly assigned application Serial Number _____, entitled

"Fuel Cell and Bipolar Plate For Use With Same," which is incorporated herein by reference.

The inventor herein has also determined that creating a pressure differential through the use of reactant channels with a small hydraulic diameter is less than optimal. The use of small hydraulic diameter reactant channels requires very tight manufacturing tolerances because without the tight tolerances friction can vary from channel to channel, which results in non-uniform reactant flow. Accordingly, although bipolar plates having small hydraulic diameters are available, their manufacture requires the use of relatively laborious and expensive manufacturing processes.

The inventor herein has also determined that increasing reactant flow rates is a less than optimal method of creating pressure differentials. Increasing the fuel flow rate results in wasted fuel, thereby reducing the efficiency of the fuel cell. Increasing the oxidant flow rate further reduces the efficiency of the fuel cell because of the additional power that is required by the associated compressor or fan.

SUMMARY OF THE INVENTIONS

Accordingly, one object of the present inventions is to provide a fuel cell that is capable of clearing reaction products and condensed humidity from the reactant channels. Another object of the present invention is to provide a bipolar plate assembly that creates a sufficient pressure differential between the inlet and outlet manifolds to clear reaction products and condensed humidity from the reactant channels without resorting to long, tortuous channels. Still another object of the present invention is to provide a bipolar plate assembly that creates a sufficient pressure drop

between the inlet and outlet manifolds to clear reaction products and condensed humidity from reactant channels without resorting to small hydraulic diameter channels. Yet another object of the present invention is to provide a bipolar plate assembly that creates a uniform pressure differential from channel to channel and plate to plate.

In order to accomplish some of these and other objectives, a bipolar plate assembly in accordance with a preferred embodiment of a present invention includes a plurality of reactant channels defining respective inlets and outlets, the inlets of adjacent channels being adjacent one another and the outlets of adjacent channels being adjacent one another, and at least two flow restrictors respectively associated with at least two adjacent reactant channels. In one implementation, the inlets are associated with a common inlet manifold and the outlets are associated with a common outlet manifold.

The present inventions provide a number of advantages over conventional bipolar plates and fuel cells. For example, the flow restrictors create a pressure drop sufficient to clear reaction product and condensed humidity from the channels, thereby eliminating the need for the long, tortuous channels, channels of small hydraulic diameter, and excessive flow rates that create the pressure drop in conventional fuels cells. It is also relatively easy to fabricate uniformly sized flow restrictors, which results in uniform pressure differentials and uniform reactant flow through the channels without the difficulty and expense associated with the creation of channels of identical length with tight tolerances.

In those implementations of the present inventions where the inlets and outlets are associated with common inlet and outlet manifolds, the pressure differential will

be determined by the flow rate and geometry of the restrictors. Should one channel become blocked, the pressure differential across the manifolds will be substantially unchanged and the pressure drop across the flow restrictor associated with the blocked channel will be zero because there is no flow. Consequently, the pressure drop across the blockage itself will be equal to the pressure drop across the inlet and outlet manifolds. Such a pressure differential will be sufficient to clear all of the channels of reaction product and condensed humidity.

The above described and many other features and attendant advantages of the present inventions will become apparent as the inventions become better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Detailed description of preferred embodiments of the inventions will be made with reference to the accompanying drawings.

FIGURE 1 is a plan view of a bipolar plate assembly in accordance with a preferred embodiment of a present invention.

FIGURE 2 is an enlarged view of a portion of the bipolar plate assembly illustrated in FIGURE 1.

FIGURE 3 is a partial section view taken along line 3-3 in FIGURE 1.

FIGURE 4 is a plan view of a cathode plate in accordance with a preferred embodiment of a present invention.

FIGURE 5 is a partial section view taken along line 5-5 in FIGURE 4.

FIGURE 6 is a an enlarged view of a portion of the bipolar plate assembly illustrated in FIGURE 4.

FIGURE 7 is an exploded view of a fuel cell module in accordance with a preferred embodiment of a present invention.

FIGURE 8 is a partial section view of the fuel cell module illustrated in FIGURE 7 in an assembled state.

FIGURE 9 is a perspective view of a fuel cell stack in accordance with a preferred embodiment of a present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following is a detailed description of the best presently known modes of carrying out the inventions. This description is not to be taken in a limiting sense, but is made merely for the purpose of illustrating the general principles of the inventions.

As illustrated for example in FIGURES 1-3, a bipolar plate assembly 10 in a accordance with a preferred embodiment of a present invention includes a bipolar plate 12 and a frame 14. The bipolar plate 12 and frame 14 may be separate structural elements that are welded, glued or otherwise mechanically fastened to one another, as is shown, or formed as an integral unit. The exemplary bipolar plate 12 includes an oxidant side 16, having an alternating series of oxidant channels 18 and oxidant side ridges 20, and a fuel side 22 having an alternating series of fuel channels 24 and fuel side ridges 26. The oxidant channels 18 include inlets 28 and outlets 30 and the fuel channels include inlets 32 and outlets 34. Adjacent channels are separated by side walls 36. The exemplary frame 14 includes a frame member 38 that extends around the periphery of the bipolar plate 12. Fuel inlet and outlet manifolds 40 and 42, oxidant inlet and outlet

manifolds 44 and 46, and coolant inlet and outlet manifolds 48 and 50 are formed in the frame member 38. Each of the manifolds preferably includes a plurality of strengthening members 52.

As shown by way of example in FIGURE 2, the exemplary bipolar plate 12 has a corrugated construction. There is essentially no overlap between adjacent oxidant channels 18 and fuel channels 24. The corrugated construction, which results in a compact and light bipolar plate, is discussed in greater detail in the aforementioned application entitled "Fuel Cell and Bipolar Plate For Use With Same." Additionally, although other configurations may be employed, each channel is substantially trapezoidally-shaped in cross-section. A substantially square-shaped cross-section could alternatively be employed as could a cross-section that is partially or completely curved. Nevertheless, for best current collection, the ridges 20 and 26 (which will be in contact with the MEAs) should be substantially flat in order to maximize the contact area for current collection.

Flow restrictors, which create a pressure differential between the inlet manifolds 40 and 44 and outlet manifolds 42 and 46, are associated at least some, and preferably all, of the channels 18 and 24. In the exemplary embodiment illustrated in FIGURES 1-3, the flow restriction is accomplished through the use of fuel inlet tubes 54, which pass through the frame member 38 and connect the fuel inlet manifold 40 to the fuel channel inlets 32, and oxidant inlet tubes 56, which pass through the frame member and connect the oxidant inlet manifold 44 to the oxidant channel inlets 28. Fuel outlet tubes 58 connect the fuel channel outlets 34 to the fuel outlet manifold 42 and oxidant outlet tubes 60 connect the oxidant channel outlets 30 to the oxidant outlet manifold

46. The cross-sectional (or flow) areas of the inlet tubes 54 and 56 are such that they create a flow restriction and, therefore, a pressure differential between the inlet manifolds and the channel inlets. Although other shapes may be used, the inlet tubes 54 and 56 and outlet tubes 58 and 60 in the illustrated embodiment are round in cross-section and the internal diameter of the outlet tubes is approximately twice that of the inlet tubes. As such, the flow areas of the outlet tubes 58 and 60 are approximately four times that of the inlet tubes 54 and 56 and are large enough that they do not create any appreciable flow restriction.

The flow restrictors (tubes 54 and 56 in the embodiment illustrated in FIGURES 1-3) create a pressure drop sufficient to clear reaction product and condensed humidity from the channels 18 and 24. This eliminates the need for the conventional long, tortuous channels, channels with small hydraulic diameters and excessive flow rates. At least 50%, and preferably all of the pressure drop should occur at the flow restrictors. Moreover, where the channel inlets and outlets are associated with common inlet and outlet manifolds, the pressure differential between the manifolds will be determined by the restrictor geometry and the reactant flow rate. When one channel becomes obstructed with reactant products or condensate, flow in that channel ceases and flow continues in the remaining unblocked channels. The pressure differential between the inlet and outlet manifolds increases because the reactants that normally flow through the blocked channel are now flowing through the remaining unblocked channels. In the blocked channel, there is no pressure differential across the restrictor because there is no flow. Consequently, the pressure differential across the blockage itself is equal to the pressure differential

across the inlet and outlet manifolds. Such a pressure differential will be sufficient to clear any blocked channels of reaction product and condensed humidity. The restrictors are also preferably uniformly sized, which provides uniform pressure differentials and reactant flow through the channels and from plate to plate.

It should be noted that flow restrictors are not limited to the relatively small inlet tube arrangement illustrated in FIGURES 1-3. For example, the cathode plate 62 illustrated in FIGURES 4-6 includes a series of z-shaped channels 64 that extend from the inlet manifold 66 to the outlet manifold 68. Constrictions 70, which are narrower than the z-shaped channels 64, are formed at the inlet end 72 of each channel. In the exemplary embodiment, the cross-sectional area of the constrictions 70 is approximately one-tenth that of the channels 64. The constrictions 70 create a pressure drop in the same manner as the inlet tubes 54 and 56 illustrated in FIGURES 1-3.

Other types of flow restrictors may also be employed. For example, the flow areas of the inlet and outlet tubes could all be large enough that they will not create any appreciable pressure drop. Here, baffles could be located within the channels to act as flow restrictors. Baffles could also be added to the channels in the embodiments illustrated in FIGURES 1-6 in order to increase the pressure differential between the inlet and outlet manifolds. In addition, although the preferred location of the flow restrictors is at or near the inlet end of the reactant channels, the location may be changed as applications require.

With respect to materials and manufacture, the bipolar plate 12 and frame 14 illustrated in FIGURES 1-3 are preferably formed from aluminum, titanium, or steel and fabricated using hydroforming, coining, bending,

stamping, or other common metal forming processes. The cathode plate 62 illustrated in FIGURES 4-6 is preferably formed from aluminum, titanium, steel, graphite, or conductive plastic and can be fabricated by machining, casting and molding processes. The surfaces of these components may be coated with a corrosion protective coating that is suitable for a PEM fuel cell environment such as gold, platinum, palladium, titanium nitride, or titanium aluminum nitride. These materials may be electrochemically deposited or vapor deposited. The tubes may be formed from metal, plastic or other suitable materials.

Although other configurations are within the scope of the present inventions, the exemplary bipolar plate assembly 10 illustrated in FIGURES 1-3 is configured as follows. The frame member 14 is about 10.3 inches in length and about 9.6 inches in width (not including the protrusions 56), while the bipolar plate 12 is about 8.0 inches in length and about 8.0 inches in width. There are 50 equally spaced oxidant channels 18 and 50 equally spaced fuel channels 24. The width of each channel is about 0.055 inch, the depth is about 0.02 inch and the thickness' of the ridges 20 and 26 are about 0.01 inch. Thus, the thickness of the illustrated bipolar plate 12 is about 0.03 inch. The side walls 28 are about 0.01 inch to about 0.03 inch thick and define an angle of about 100° with the bottom surface of the associated fuel or oxidant channel.

The exemplary cathode plate 62 illustrated in FIGURES 4-6 is hexagonal in shape that is about 2.0 inches in length on each side and about 0.40 inch thick. The width of the channels 64 is about 0.03 inch and the depth is about 0.01 inch to about 0.03 inch. The width of the

constrictions 70 is about 0.008 inch and the depth is about 0.01 inch.

The present bipolar plates may be incorporated into a variety of fuel cell devices. As illustrated for example in FIGURES 7 and 8, one use of the bipolar plate assembly 10 illustrated in FIGURES 1-3 is in a PEM fuel cell module 74. PEM fuel cell modules preferably consist of one to ten individual cells. In the exemplary embodiment illustrated in FIGURES 7 and 8, the fuel cell module 74 consists of five cells. More specifically, the exemplary fuel cell module 74 includes a separator plate 76, a coolant plate 78, six bipolar plate assemblies 10 (each including a bipolar plate 12 and a frame 14) and five MEAs 80 that are stacked in the manner shown. The bottom bipolar plate assembly 10 will typically rest upon the separator plate of an adjacent fuel cell module in a multi-module stack. In those instances where a particular module comprises the bottom module in a stack or is used in a one module stack, a bottom separator plate (not shown) may be provided below the bottom bipolar plate assembly 10.

The exemplary separator plate 76, which may be formed from materials such as aluminum, titanium, steel, graphite or conductive plastic, includes fuel manifolds, oxidant manifolds, coolant manifolds, and assembly apertures that correspond to those of the exemplary bipolar plate assembly 10. The exemplary coolant plate 78 also includes fuel manifolds, oxidant manifolds, coolant manifolds, and assembly apertures that correspond to those of the exemplary bipolar plate assembly 10. The coolant plate 78 is flat on one face and includes coolant channels 81 on the other face 82 that are in communication with the coolant manifolds 48 and 50. Suitable coolants include water, ethylene glycol, and polyalphaolefins.

Turning to the MEAs 80, the present inventions may be practiced with conventional MEAs. For example, the membrane electrolyte may be formed from perfluorinated sulfonic acid polymer sold under the name NAFION™ by E. I. DuPont de Nemours & Co. or Gore-Select™ by W. L. Gore. The anode and cathode films may be formed from catalytic particles in a NAFION™ or polytetrafluoroethylene binder. An appropriate material for the gas diffusion layer is ELAT™ by E-Tek and Carbel™ by W. L. Gore. In the illustrated embodiment, the MEAs 80 include tabs 84 that are used during the assembly process. Alternatively, commercial MEAs, such as those sold by W. L. Gore (Primea™), E-Tek and DeGussa-Huls, can be used.

As shown by way of example in FIGURE 9, a fuel cell stack 86 in accordance with a preferred embodiment of a present invention includes an end plate 88, a current collector 90, between one and two hundred fuel cell modules 74, a current collector 92 and an end plate assembly 94 that consists of an end plate 96 and a gasket 98. The end plate 88 is provided with fuel inlet and outlet ports 100 and 102, oxidant inlet and outlet ports 104 and 106 and coolant inlet and outlet ports 108 and 110. The ports connect sources of fuel, oxidant and coolant (not shown) to manifolds in the fuel cell modules 74. Here, the fuel is hydrogen and the oxidant is oxygen. The exemplary fuel cell stack 86 is also provided with a positive current collector terminal 112 and a negative current collector terminal 114. The various components may be secured to one another through the use of nut and bolt arrangements 116 or other mechanical fasteners. The bolts pass through a series of apertures 118 formed in protrusions 120 on the bipolar plate frame 14 and through apertures 122 in the corners of the frame (note FIGURE

1), as well as through aligned apertures in the other components of the stack.

Although the present inventions have been described in terms of the preferred embodiment above, numerous modifications and/or additions to the above-described preferred embodiments would be readily apparent to one skilled in the art. For example, bipolar plates in accordance with a present invention may include flow restrictors associated with each of the channels on the cathode side and none on the anode side or, alternatively, may include flow restrictors associated with each of the channels on the anode side and none on the cathode side. It is intended that the scope of the present inventions extend to all such modifications and/or additions.

I claim:

1. In a bipolar plate assembly for use in a fuel cell including a plurality of reactant channels (18, 24) defining respective inlets (28, 32) and outlets (30, 34), the inlets (28, 32) of adjacent reactant channels (18, 24) being adjacent one another and the outlets (30, 34) of adjacent reactant channels (18, 24) being adjacent one another, the improvement comprising:

at least two flow restrictors (54, 56)respectively associated with at least two adjacent reactant channels (18, 24).

2. A bipolar plate assembly as claimed in claim 1, wherein each of the reactant channels (18, 24) includes a flow restrictor (54, 56).

3. A bipolar plate assembly as claimed in claim 1, wherein the flow restrictors (54, 56) are associated with the reactant channel inlets (28, 32).

4. A bipolar plate assembly as claimed in claim 1, wherein the flow restrictors (54, 56) are substantially identical to one another.

5. A bipolar plate assembly as claimed in claim 1, wherein the bipolar plate assembly defines a first side (16) and a second side (22) and the plurality of reactant channels comprises a plurality of first reactant channels (18) on the first side (16) and a plurality of second reactant channels (24) on the second side (22).

6. A bipolar plate assembly as claimed in claim 1, wherein the plurality of channels comprises a plurality of first reactant channels (18) and a plurality of second reactant channels (24), the bipolar plate assembly further comprising:

first and second inlet manifolds (44, 40) respectively associated with the inlets (28, 32) of the first and second reactant channels (18, 24); and

first and second outlet manifolds (30, 34) respectively associated with the outlets (34, 30) of the first and second reactant channels (18, 24);

wherein the at least two adjacent reactant channels comprise first reactant channels.

7. A bipolar plate assembly as claimed in claim 6, wherein the flow restrictors comprise first fluid connectors (54, 56) extending from the first and second inlet manifolds (44, 40) to the inlets of the first and second reactant channels (18, 24), the first fluid connectors (54, 56) defining respective first flow areas, the bipolar plate assembly further comprising:

a plurality of second fluid connectors (58, 60) extending from outlets of the first and second reactant channels (18, 24) to the first and second outlet manifolds (46, 44), the second fluid connectors (58, 60) defining respective second flow areas, the second flow areas being greater than the first flow areas.

8. A bipolar plate assembly as claimed in claim 7, wherein the first and second fluid connectors (54, 56, 58, 60) comprise tubular members.

9. A bipolar plate assembly as claimed in claim 1, wherein the plurality of reactant channels (18, 24)

comprises a plurality of substantially linear reactant channels.

10. A bipolar plate assembly as claimed in claim 1, wherein bipolar defines an anode side and a cathode side and the at least two adjacent reactant channels (18 or 24) are located on the same side.

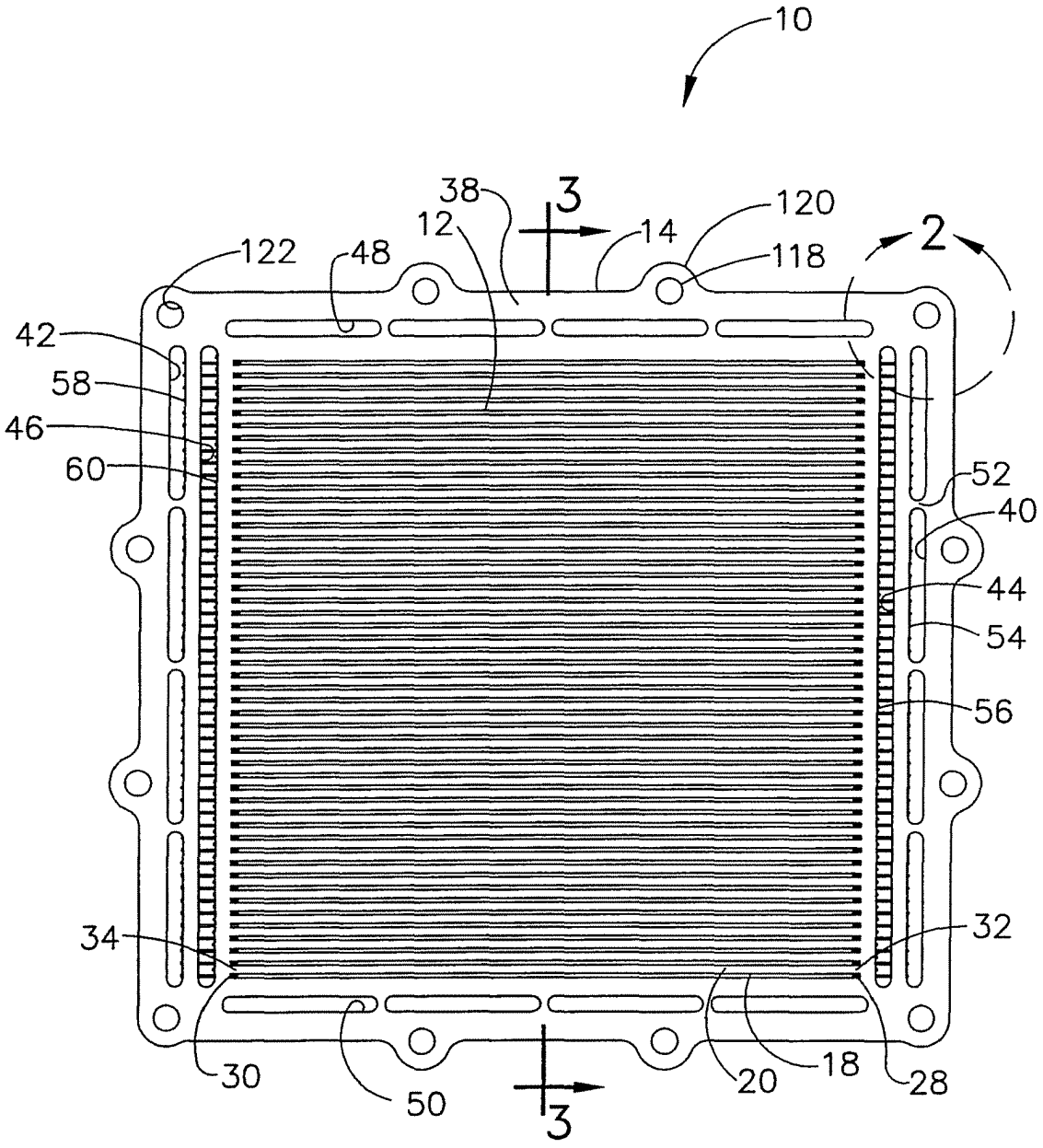

10
38
3
12
14
120
118
2
122
48
42
58
46
60
52
40
44
54
56
34
32
30
50
3
20
18
28

FIG. 1

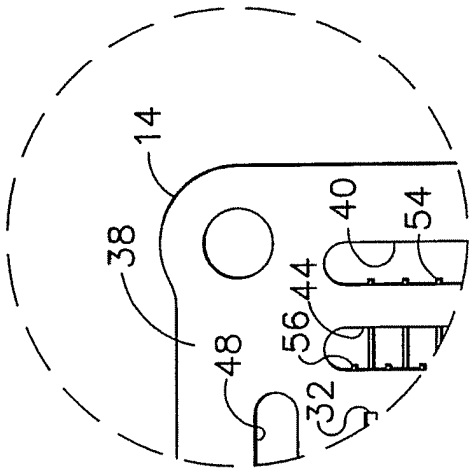


FIG. 2

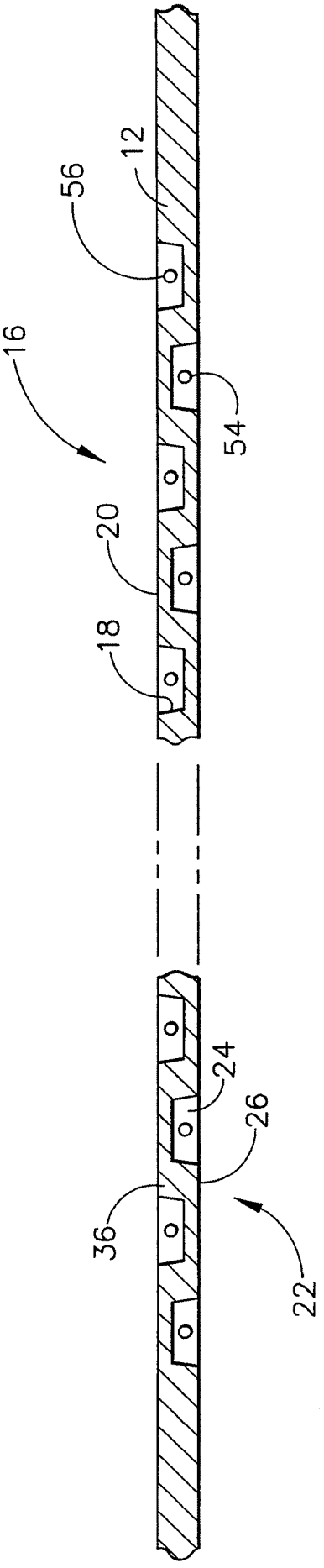


FIG. 3

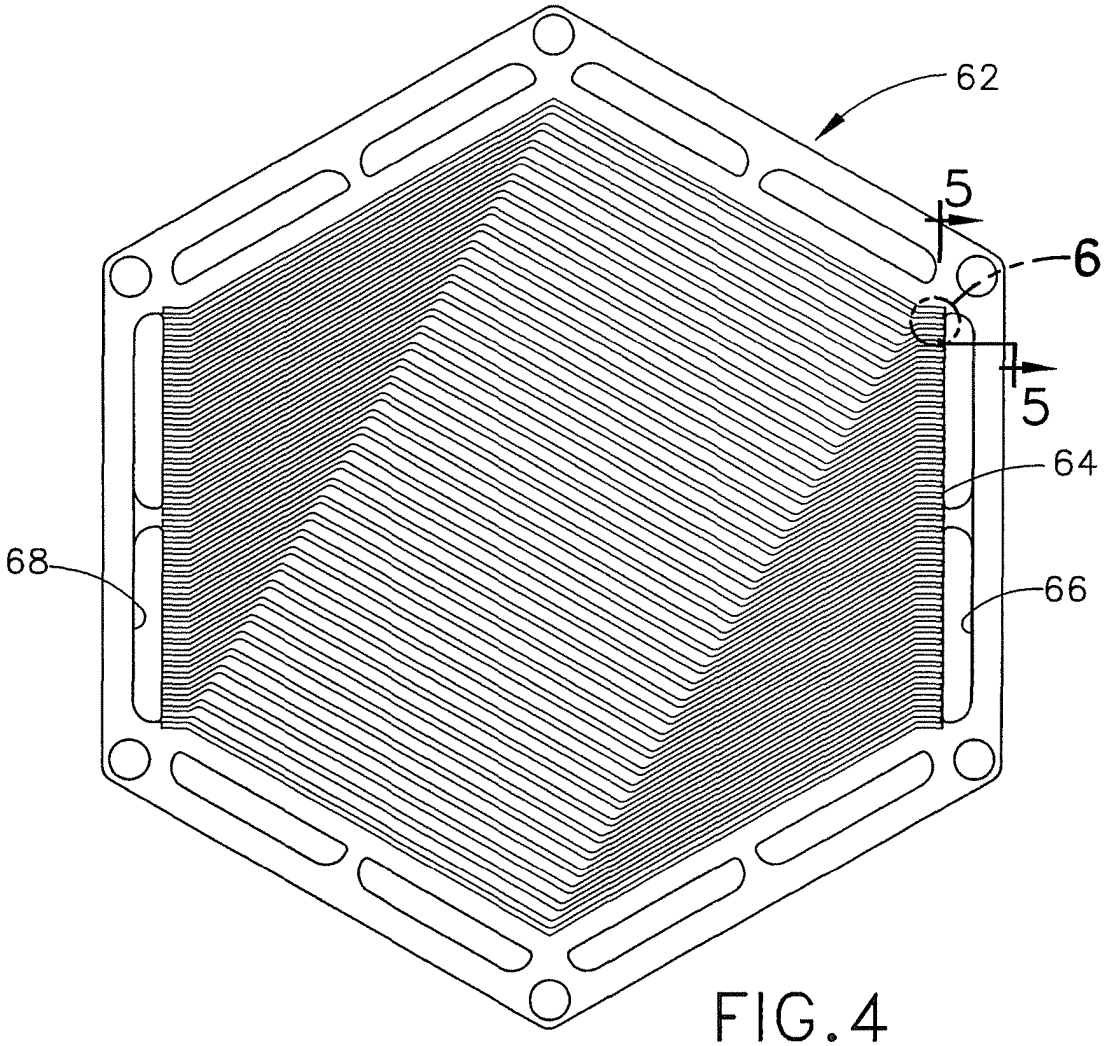


FIG.4

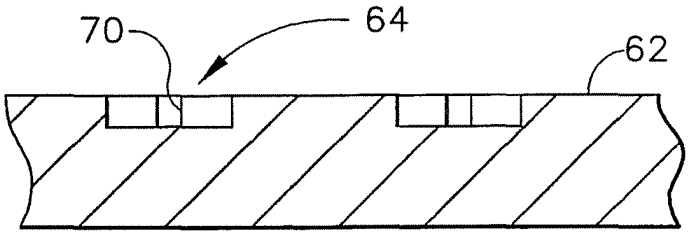


FIG. 5

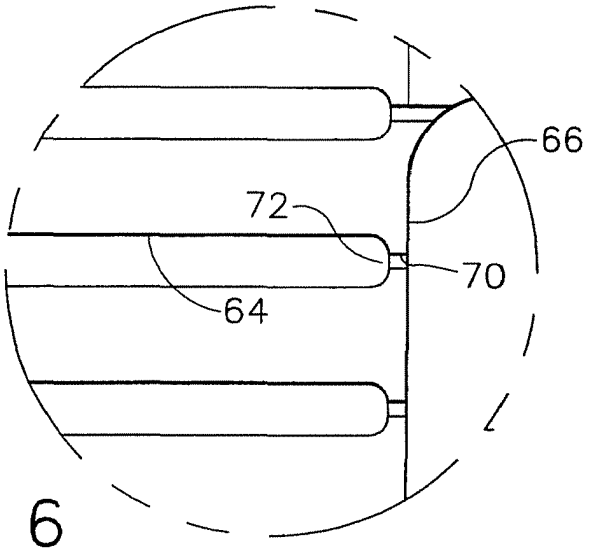


FIG. 6

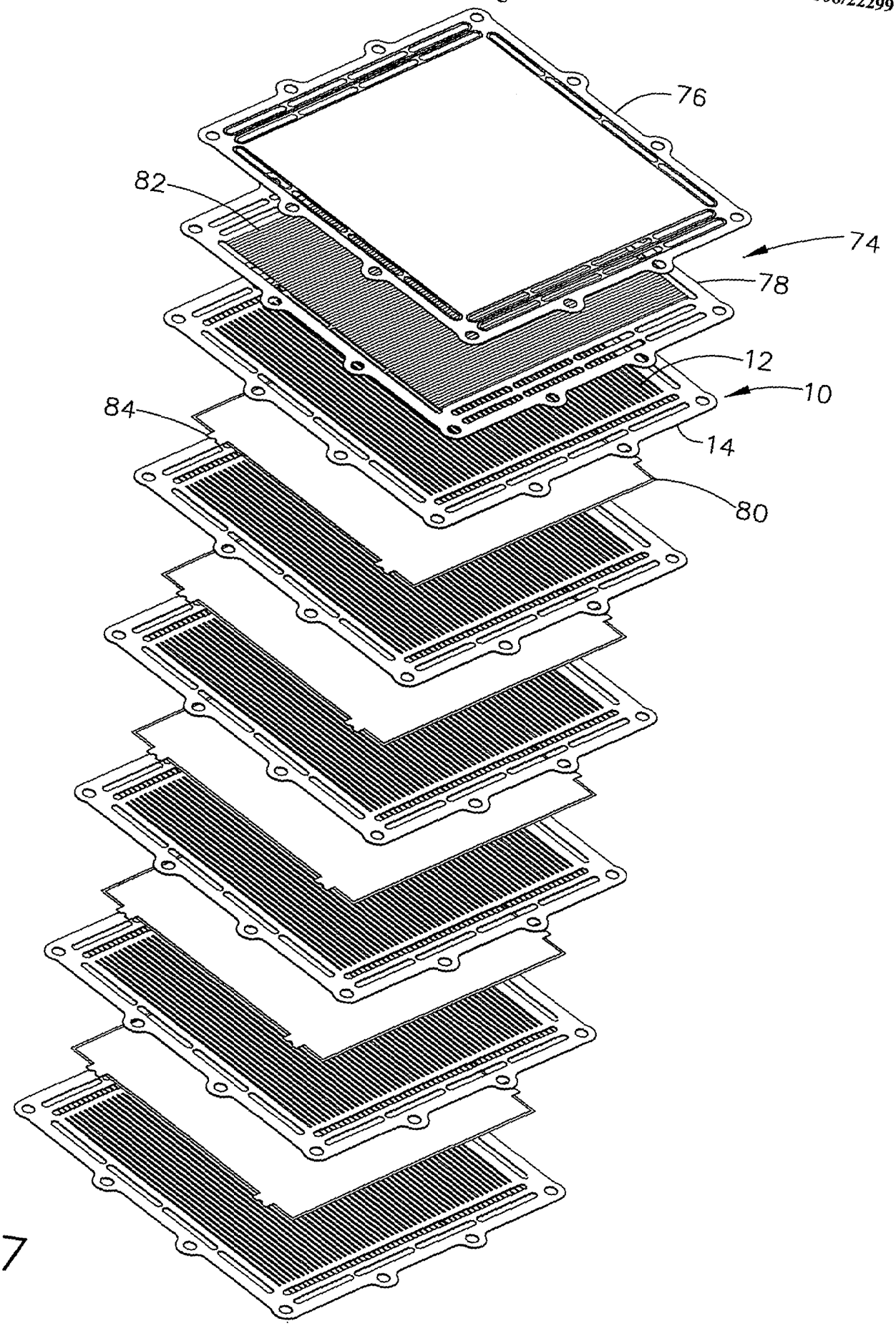


FIG. 7

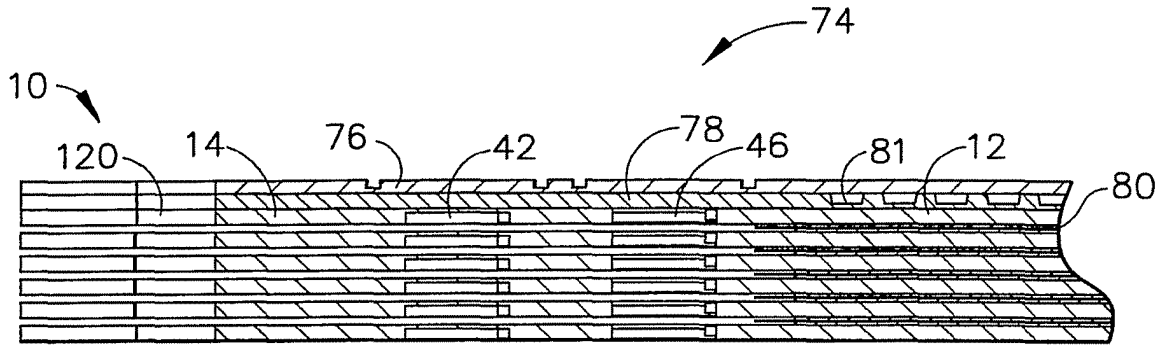

74
10
120
14
76
42
78
46
81
12
80

FIG. 8

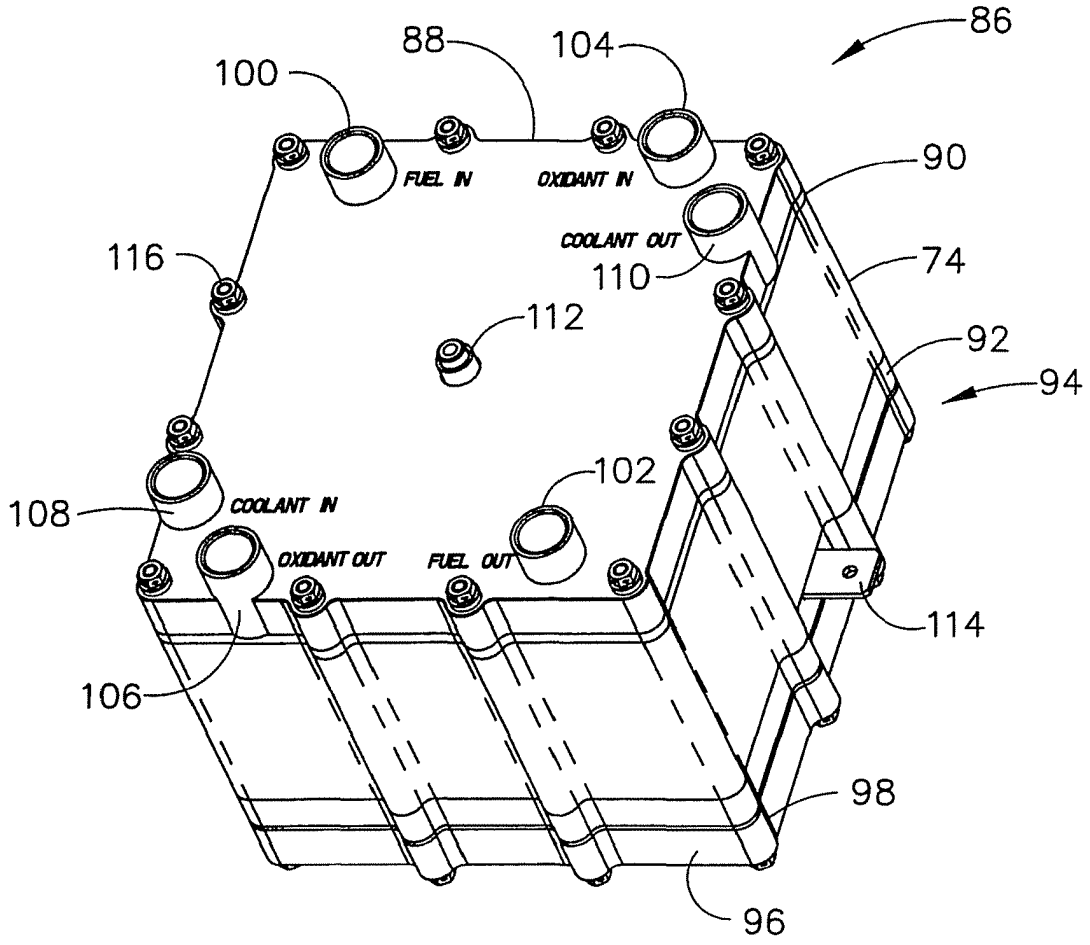

86
88
104
100
90
FUEL IN
OXIDANT IN
COOLANT OUT
116
110
74
112
92
94
102
108
COOLANT IN
OXIDANT OUT
FUEL OUT
114
106
98
96

FIG. 9

Electronic Acknowledgement Receipt

EFS ID:	6613196
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	91704
Filer:	John Robert Scoley Orange/Judith Martin
Filer Authorized By:	John Robert Scoley Orange
Attorney Docket Number:	67539/622
Receipt Date:	10-DEC-2009
Filing Date:	23-JAN-2006
Time Stamp:	16:37:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		35404-US-1st_sIDS.pdf	318874 6ba9ac92d1f70c29aa817528267a15a9a45b7464	yes	4

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Filed (SB/08)		3	4	
Warnings:					
Information:					
2	Foreign Reference	35404-US-PAT_reference1.pdf	1445121 c79b100dea5aab92cfab1f32c6ad9168c717ec4f	no	24
Warnings:					
Information:					
3	Foreign Reference	35404-US-PAT_reference2.pdf	1726963 e4482e411d3a3319f2c659e355797cbf2bc0dc26	no	25
Warnings:					
Information:					
4	NPL Documents	35404-US-PAT_reference3.pdf	782572 24f5eb444b1cda58ed68c1e2cdae7a7f6c0ba6f8	no	23
Warnings:					
Information:					
5	NPL Documents	35404-US-PAT_reference4.pdf	90212 a70530e46af8e996d3dc41e13ad0de73a9a8821e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4363742		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/336,814**

Applicant: **BROWN, Daniel R.L.; VANSTONE, Scott A.**

Filed: **January 23, 2006**

Title: **Elliptic Curve Random Number Generation**

Art Unit: **4144**

Examiner: **LAKHIA, Viral S.**

Docket No.: **67539/00622**

Mail Stop Amendment
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

FIRST SUPPLEMENTAL
INFORMATION DISCLOSURE STATEMENT

Pursuant to the duty to disclose under 37 CFR §1.56, Applicant submits herewith a Form PTO/SB/08 listing references of which the Applicant is aware and which are brought to the attention of the Examiner. In accordance with 37 CFR §1.98(a)(2), a copy of each foreign patent document and non-patent reference document listed in the enclosed Form PTO/SB/08 is submitted herewith.

Included in the listed references is non-English language PCT application cited in a search report from the corresponding European application. For the Examiner's convenience, Applicant has, additionally, included in the listed references an English language equivalent – Canadian Application No. 2,381,397, which is a national entry of the afore-mentioned PCT application.

The filing of this IDS shall not be construed as a representation that a search has been made, an admission that the information cited is, or is considered to be, material for patentability, or that no other material information exists. This filing shall not be construed as an admission against interest in any matter.

This IDS is being submitted pursuant to 37 CFR 1.97(c) prior to the issuance of a final action or a Notice of Allowance. Applicant hereby certifies that each item of information contained in the present Information Disclosure Statement was cited in a communication from a foreign Patent Office

in a counterpart foreign application not more than 3 months prior to the filing of the present Statement. Accordingly, no fee is believed to be due for consideration of the documents submitted herewith.

Applicant respectfully requests consideration of the items listed and requests the Examiner to return a copy of the attached Form PTO/SB/08 after being marked as being considered by the Examiner.

Respectfully submitted,

Date: 10 Dec 09,

John R.S. Orange
Registration No. **29,725**
Agent for Applicant

BLAKE, CASSELS & GRAYDON LLP
199 Bay Street
Suite 2800, Commerce Court West
Toronto, Ontario, M5L 1A9
Canada

Tel 416-863-3164
Fax 416-863-2653

JRO/jm

(✓) encl.

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 91704

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 91704

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

Certicom Corp.
5520 Explorer Drive
Mississauga, Ontario L4W 5L1 CANADA

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	[signature]	Date	Nov 3/09
Name	Brian Bidulka	Telephone	(519) 888-7465
Title	Chief Accounting Officer.		

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Legal OK

RIM OK

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: **BROWN, Daniel R.L. et al.**

Application No./Patent No.: **11/336,814** Filed/Issue Date: **January 23, 2006**

Titled: **Elliptic Curve Random Number Generation**

Certicom Corp. , a **corporation**

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☑ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title and interest in
(The extent (by percentage) of its ownership interest is _____ %); or

3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above by virtue of either:

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel **017559** , Frame **0263** , or for which a copy therefore is attatched.

OR

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____ , Frame _____ , or for which a copy thereof is attached.

2. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____ , Frame _____ , or for which a copy thereof is attached.

3. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____ , Frame _____ , or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature	21 Dec 09 Date
John R.S. Orange (Registration No. 29,725) Printed or Typed Name	**(416) 863-3164** Telephone number

Electronic Acknowledgement Receipt

EFS ID:	6693911
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	91704
Filer:	John Robert Scoley Orange/Judith Martin
Filer Authorized By:	John Robert Scoley Orange
Attorney Docket Number:	67539/622
Receipt Date:	22-DEC-2009
Filing Date:	23-JAN-2006
Time Stamp:	18:06:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		35404-US-PAT_poa_assignee-statement.pdf	301184 ee8ef97c5529e158a3e850772bd85cf978e8ccdf	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Power of Attorney	1	1
	Assignee showing of ownership per 37 CFR 3.73(b).	2	2
Warnings:			
Information:			
	Total Files Size (in bytes):	301184	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622

CONFIRMATION NO. 1834

POWER OF ATTORNEY NOTICE

91704
Blake, Cassels & Graydon LLP
199 BAY STREET , SUITE 2800
COMMERCE COURT WEST
TORONTO, ON M5L 1A9
CANADA

OC000000039410954

Date Mailed: 01/05/2010

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/22/2009.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/ttkim/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622

CONFIRMATION NO. 1834

POA ACCEPTANCE LETTER

91704
Blake, Cassels & Graydon LLP
199 BAY STREET , SUITE 2800
COMMERCE COURT WEST
TORONTO, ON M5L 1A9
CANADA

Date Mailed: 01/05/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/22/2009.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ttkim/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PLUS Search Results for S/N 11336814, Searched Tue Feb 16 13:03:29 EST 2010

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

20070189527 99
20080025500 57
5442707 65
6078667 65
6088798 65
6263081 65
6307935 65
6341349 65
7308469 65
20030072443 65
20040228478 65
20060285682 65
20070121933 65
20080080710 65
5271061 58
5463690 58
5581616 58
5805703 58
6049610 58
6195433 58
6285760 58
6345098 58
7023990 58
20040228484 58
20060126828 58
5955717 57
6611597 57
6704867 57
6738899 57
6847951 57
6876745 57
6910058 57
7127063 57
7218735 57
7512233 57
7593527 57
20030123668 57
20030152218 57
20040098436 57
20060153364 57
20060153365 57
20060153366 57
20060153367 57
20060153368 57
20060165231 57
20060280296 57
20060282491 57
20070110234 57
20070177721 57
20070206789 57

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

91704 7590 03/22/2010

Blake, Cassels & Graydon LLP
199 BAY STREET , SUITE 2800
COMMERCE COURT WEST
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
LAKHIA, VIRAL S	
ART UNIT	**PAPER NUMBER**
2431	

NOTIFICATION DATE	DELIVERY MODE
03/22/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

rimpatent@blakes.com
brett.slaney@blakes.com

Office Action Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL S. LAKHIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *1* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 October 2009*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *1-36* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *1/23/2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-12, 13-14, 15-18, 20-21 and 22-29 are drawn to a method for generating an elliptic curve random number, classified in class 380, and subclass 44.

II. Claims 19, 30-32, 33-36 are drawn to establishing escrow key with elliptical curve random number generator, classified in class 380, and subclass 286.

2. Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable. In the instant case, subcombination II has separate utility such as the establishing escrow key with elliptical curve random generator of group II does not need to be evaluated with the method of group I. See MPEP § 806.05(d).

The examiner has required restriction between subcombinations usable together. Where applicant elects a subcombination and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

3. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a

serious search and examination burden if restriction were not required because one or more of the following reasons apply:

(a) the inventions have acquired a separate status in the art in view of their different classification;

(b) the inventions have acquired a separate status in the art due to their recognized divergent subject matter;

(c) the inventions require a different field of search (for example, searching different classes/subclasses or electronic resources, or employing different search queries);

(d) the prior art applicable to one invention would not likely be applicable to another invention;

(e) the inventions are likely to raise different non-prior art issues under 35 U.S.C. 101 and/or 35 U.S.C. 112, first paragraph.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of a invention to be examined even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

A telephone call was made to John Orange on 3/12/2010 to request an oral election to the above restriction requirement, but did not result in an election being made. Examiner tried to reach to applicant but received a fax tone after pressing zero on the phone system of the applicant's attorney; as a result examiner was not able to leave a detailed voice message regarding the election. Further above circumstances resulted in an election not being made.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of a species or invention to be examined even though the requirement may be traversed (37 CFR 1.143) and (ii) identification of the claims encompassing the elected invention.

The election of an invention or species may be made with or without traverse. To preserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable on the elected invention.

If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

Should applicant traverse on the ground that the inventions are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

4. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viral Lakhia whose telephone number is (571) 373-3363. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch, can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Viral S Lakhia/
Examiner, Art Unit 2431

/Matthew T Henning/
Primary Examiner, Art Unit 2431

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	Art Unit
	VIRAL LAKHIA	4144

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010						
	1	✓		÷						
	2	✓		÷						
	3	✓		÷						
	4	✓		÷						
	5	✓		÷						
	6	✓		÷						
	7	✓		÷						
	8	✓		÷						
	9	✓		÷						
	10	✓		÷						
	11	✓		÷						
	12	✓		÷						
	13	✓		÷						
	14	✓		÷						
	15	✓		÷						
	16	✓		÷						
	17	✓		÷						
	18	✓		÷						
	19		✓	÷						
	20			÷						
	21			÷						
	22			÷						
	23			÷						
	24			÷						
	25			÷						
	26			÷						
	27			÷						
	28			÷						
	29			÷						
	30			÷						
	31			÷						
	32			÷						
	33			÷						
	34			÷						
	35			÷						
	36			÷						

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	Art Unit
	VIRAL LAKHIA	4144

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/336,814**

Applicant: **BROWN, Daniel R.L.; VANSTONE, Scott A.**

Filed: **January 23, 2006**

Title: **Elliptic Curve Random Number Generation**

Art Unit: **2431**

Examiner: **LAKHIA, Viral S.**

Docket No.: **67539/00622**

Mail Stop Amendment
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE

Sir:

In response to the Office Action of March 22, 2010 the Applicant's elect herewith group I, namely claims 1 – 12, 13 – 14, 15 – 18, 20 – 21 and 22 – 29.

The Applicant's reserve the right to file the cancelled claims 19, 30 – 32, 33 – 36 as a divisional application during the pendency of the present or any continuing application.

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (previously amended) A method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of:

providing a pair of inputs to said arithmetic unit, with each input representative of at least one coordinate of an elliptic curve point, and with at least one of said inputs being verifiably random;

performing selected elliptic curve operations on said inputs to obtain an output; and utilising said output as a random number in the cryptographic operation.

2. (original) A method according to claim 1 wherein said at least one input is obtained from an output of a hash function.

3. (original) A method according to claim 2 wherein the other of said inputs is utilized as an input to said hash function.

4. (original) A method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

5. (original) A method according to claim 4 wherein one of said scalar multiples is used to derive said random number and the other of said scalar multiples is used to change said secret value for subsequent use.

6. (original) A method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input.

7. (previously amended) A method according to claim 6 wherein another coordinate of said point is obtained from said one coordinate for inclusion as said one input.

8. (original) A method according to claim 7 wherein said other input is a representation of an elliptic curve point.

9. (original) A method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and truncating said coordinate to a bit string for use as said random number.

10. (original) A method according to claim 9 wherein said one coordinate is truncated in the order of one half the length of a representation of an elliptic curve point representation.

11. (original) A method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and hashing said one coordinate to provide a bit string for use as said random number.

12. (original) A method according to claim 1 wherein said verifiably random input is chosen to be of a canonical form whereby a predetermined relationship between said inputs is difficult to maintain.

13. (previously amended) A method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of:

providing a pair of inputs, each representative of at least one coordinate of a pair of elliptic curve points, to said arithmetic unit;

performing elliptic curve operations to obtain an output representative of at least one coordinate of a scalar multiple of an elliptic curve point;

passing said output through a one way function to obtain a bit string for use as a random number; and

utilising said random number in the cryptographic operation.

14. (original) A method according to claim 13 wherein said one way function is a hash function.

15. (previously amended) An elliptic curve random number generator comprising a pair of inputs, each of said inputs being representative of at least one coordinate of a pair of elliptic curve points; an arithmetic unit to perform elliptic curve operations on said inputs; and an output to receive the results of said elliptic operations, said output representing a random number for use in a cryptographic operation, at least one of said inputs being verifiably random.

16. (original) An elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function.

17. (original) An elliptic curve random number generator according to claim 16 wherein said one way function is a hash function.

18. (original) An elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function.

19. (cancelled)

20. (previously presented) A method according to claim 5 wherein said secret value is derived from a coordinate of said other scalar multiple.

21. (previously presented) A method according to claim 20 wherein the $\bar{x}$ coordinate of said other scalar multiple is used to change said secret value.

22. (previously presented) An elliptic curve random number generator according to claim 15 wherein said arithmetic unit operates on said inputs to obtain a scalar multiple of a coordinate of a point represented by said one input.

23. (previously presented) An elliptic curve random number generator according to claim 23 wherein said arithmetic unit computes a coordinate of a scalar multiple of each of said points represented by said inputs

24. (previously presented) An elliptic curve random number generator according to claim 23 wherein said coordinate of said scalar multiple of said point represented by said one input is operated on by said arithmetic unit and utilised as said output.

25. (previously presented) An elliptic curve random number generator according to claim 24 wherein said arithmetic unit includes a register to maintain a secret value and a value derived from said coordinate of said scalar multiple of the point represented by said other input is stored in said register to provide said secret value.

26. (previously presented) An elliptic curve random number generator according to claim 25 wherein said arithmetic unit utilises said secret value and said one input to obtain said coordinate of said scalar multiple of said point represented by said one input.

27. (previously presented) An elliptic curve random number generator according to claim 26 wherein said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and truncates said coordinate to provide said output.

28. (previously presented) An elliptic curve random number generator according to claim 26 wherein said arithmetic unit includes a one way function and said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and applies said one way function to said coordinate of said scalar multiple to obtain said output.

29. (previously presented) An elliptic curve random number generator according to claim 28 wherein said arithmetic unit truncates said coordinate of said scalar multiple prior to applying said one way function.

30. (cancelled)

31. (cancelled)

32. (cancelled)

33. (cancelled)

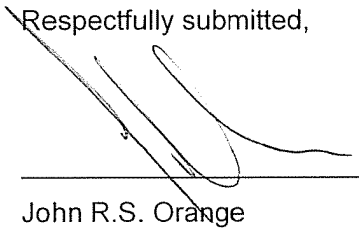
34. (cancelled)

35. (cancelled)

36. (cancelled)

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: April 22, 2010

BLAKE, CASSELS & GRAYDON LLP
199 Bay Street
Suite 2800, Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: 416-863-3164

JRO/lxi

Electronic Acknowledgement Receipt

EFS ID:	7467964
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	91704
Filer:	John Robert Scoley Orange/Judith Martin
Filer Authorized By:	John Robert Scoley Orange
Attorney Docket Number:	67539/622
Receipt Date:	22-APR-2010
Filing Date:	23-JAN-2006
Time Stamp:	15:19:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		35404-US-PAT_OAresponse.pdf	278510 770153d18ee719512f9b0918fad825b1c0e653d6	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Response to Election / Restriction Filed	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	6
Warnings:			
Information:			
	Total Files Size (in bytes):	278510	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/336,814	Filing Date 01/23/2006	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	04/22/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 28	Minus	** 36	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***5	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/SHERRY A. DAVIS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/336,814	Filing Date 01/23/2006	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	04/22/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 28	Minus	** 36	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***5	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/SHERRY A. DAVIS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

91704 7590 08/23/2010

Blake, Cassels & Graydon LLP
199 BAY STREET , SUITE 2800
COMMERCE COURT WEST
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
LAKHIA, VIRAL S	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
08/23/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

rimpatent@blakes.com
brett.slaney@blakes.com

Office Action Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL S. LAKHIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18 and 20-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18, 20-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 4/22/2010.

Response to Arguments

Applicant's election without traverse of claims 1-18, 20 - 29 in the reply filed on 4/22/2010 is acknowledged.

Claims 1 – 18, 20 - 29 have been examined.

All objections and rejections not set forth below have been withdrawn.

Claim Objections

Claim 23 is objected to because of the following informalities: Claim 23 is dependent on claim 23, suggested update of changing in dependency to claim 22. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 12, 15 and 22 - 24 are rejected under 35 U.S.C. 102(b) as being anticipated by article as cited in IDS – Lee et al., "Elliptical Curve Random Number Generation" Electrical and Electronic Technology 2001. Tencon Proceedings of IEEE Region 10 International conference on 19 - 22 August 2001. Volume 1, pages 239 to 241.

As per claim 1, Lee teaches a method of computing operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation *(page 239 Fig 1 - "use elliptic curves ... be the point of infinity"),* said method comprising the steps of :-

providing a pair of inputs to said arithmetic unit, with each input representative of at least one coordinate of an elliptic curve point *(page 239 – Fig 1 - "a block diagram .. in fig 1")*, and with at least one of said inputs being verifiably random *(page 239 – Fig 1 - "a block diagram ... in fig 1")*;

performing selected elliptic curve operations on said inputs to obtain an output; and utilizing said output as a random number in the cryptographic operation *(page 239 – 240)*.

As per claim 12 Lee teaches a method according to claim 1 wherein said verifiably random input is chosen to be of a canonical form whereby a predetermined relationship between said inputs is difficult to maintain *(Lee page 239 – 240).*

As per claim 15 Lee teaches an elliptic curve random number generator comprising a pair of inputs, each of said inputs being representative of at least one coordinate of a pair of elliptic curve points *(Lee Fig 1, page 239 - 240)*; an arithmetic unit to perform elliptic curve operations on said inputs *(Lee Fig 1, page 239 - 240)*; and an output to receive the results of said elliptic operations, said output representing a random number for use in a cryptographic operation *(Lee Fig 1, page 239 - 240)*, at least one of said inputs being verifiably random *(Lee Fig 1, page 239 - 240)*.

As per claim 22 Lee teaches an elliptic curve random number generator according to claim 15 wherein said arithmetic unit operates on said inputs to obtain a scalar multiple of a coordinate of a point represented by said one input *(Lee – Fig 1 - page 239 – 240).*

As per claim 23 Lee teaches an elliptic curve random number generator according to claim 23 wherein said arithmetic unit computes a coordinate of a scalar multiple of each of said points represented by said inputs *(Lee – Fig 1 - page 239 – 240).*

As per claim 24 Lee teaches an elliptic curve random number generator according to claim 23 wherein said coordinate of said scalar multiple of said point

represented by said one input is operated on by said arithmetic unit and utilized as said output *(Lee – Fig 1 - page 239 – 240).*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2 – 4, 6, 13 – 14, 16 – 18, 25 - 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. (IDS) and in view of U.S. Patent 6,044,388 to DeBellis et al. (hereinafter "DeBellis").

13, 16, 17, 18

As per claim 2 Lee teaches a method according to claim 1.

Lee does not teach wherein said at least one input is obtained from an output of a hash function.

DeBellis teaches wherein said at least one input is obtained from an output of a hash function *(DeBellis Fig 1 and 2 col 7 – lines 15 – 32).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of DeBellis in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee combining a time - dependent value with secret value and

passing the result through a one-way hash function to generate a hash value from which random value is generated. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

As per claim 3 Lee teaches elliptical curve random number generation.

Lee does not teach a method wherein the other of said inputs is utilized as an input to said hash function.

DeBellis teaches, a method wherein the other of said inputs is utilized as an input to said hash function *(DeBellis Fig 1 and 2 col 7 – lines 15 – 40).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of DeBellis in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee combining a time - dependent value with secret value and passing the result through a one-way hash function to generate a hash value from which random value is generated. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

As per claim 4 Lee teaches wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points

represented by said inputs *(Lee Fig 1 - page 239 "Multiplying ... done rapidly" where integer k can be a secret value which reads on the above limitation).*

As per claim 6 Lee teaches elliptical curve random number generation.

Lee does not teach wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input.

DeBellis teaches wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input *(DeBellis Fig 1 and 2 col 7 – lines 15 – 40, col 11 – lines 50 – 67).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of DeBellis in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee by combining a one – way hash function as a to generate a hash value from which a random number is generated by validating as a coordinate of a point. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to provide integrity and secrecy and to avoid replay attacks.

As per claim 13 Lee teaches a method of computing operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation *(Lee 239*

Fig 1 - "use elliptic curves ... be the point of infinity"), said method comprising the steps of:-

providing a pair of inputs, each representative of at least one coordinate of a pair of elliptic curve points to said arithmetic unit *(page 239 – Fig 1 - "a block diagram .. in fig 1");*

an elliptic curve random number generator *(Lee – Fig 1 – page 239 – 240)*, performing elliptic curve operations to obtain obtaining an output representative of at least one coordinate of a scalar multiple of an elliptic curve point *(Lee page 239 – "Multiplying .. done rapidly").*

and utilizing said random number in the cryptographic operation *(Lee page 239 – 240).*

Lee does not teach, however DeBellis teaches passing said output through a one way function to obtain a bit string for use as a random number *(DeBellis Fig 1 and 2 col 7 – lines 15 – 32).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of DeBellis in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee combining a time - dependent value with secret value and passing the result through a one-way hash function to generate a hash value from which random value is generated. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

As per claim 14 Lee teaches a method according to claim 13.

Lee does not teach wherein said one way function is a hash function.

However DeBellis teaches wherein said one way function is a hash function.

(DeBellis Fig 1 and 2 col 7 – lines 15 – 32).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of DeBellis in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee combining a time - dependent value with secret value and passing the result through a one-way hash function to generate a hash value from which random value is generated. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

As per claim 16 Lee teaches an elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function *(DeBellis Fig 1 and 2 col 7 – lines 15 – 32 and as explained in claim 13 – 14).*

As per claim 17 Lee teaches an elliptic curve random number generator according to claim 16 wherein said one way function is a hash function *(DeBellis Fig 1 and 2 col 7 – lines 15 – 32 and as explained in claim 13 – 14).*

As per claim 18 Lee teaches an elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function *(DeBellis Fig 1 and 2 col 7 – lines 15 – 32 and as explained in claim 13 – 14).*

As per claim 25 Lee teaches an elliptic curve random number generator. Lee does not teach wherein said arithmetic unit includes a register to maintain a secret value and a value derived from said coordinate of said scalar multiple of the point represented by said other input is stored in said register to provide said secret value.

However DeBellis teaches wherein said arithmetic unit includes a register to maintain a secret value and a value derived from said coordinate of said scalar multiple of the point represented by said other input is stored in said register to provide said secret value *(Fig 7 – col 6 – lines 55 – 67).*

As per claim 26 Lee teaches an elliptic curve random number generator according to claim 25 wherein said arithmetic unit utilizes said secret value and said one input to obtain said coordinate of said scalar multiple of said point represented by said one input *(Lee – Fig 1 - page 239 – 240).*

Claims 5, 7 – 9, 27 - 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. (IDS) and in view of U.S. Patent 6,044,388 to

DeBellis et al. (hereinafter "DeBellis") and further in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant").

As per claim 5 Combination of Lee and DeBellis teaches a method according scalar multiples is used to change said secret value for subsequent use *(Lee Fig 1 - page 239 "Multiplying ... done rapidly" where integer k can be a secret value which reads on the above limitation).*

Combination of Lee and DeBellis does not teach wherein one of said scalar multiples is used to derive said random number.

However Gallant teaches wherein one of said scalar multiples is used to derive said random number *(Gallant para 0054 – 0055).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of combination of Lee and DeBellis by accelerating multiplication of an elliptical curve point by a scalar over a finite field. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

As per claim 7 Combination of Lee and DeBellis teaches a method of combination of scalar multiples and secret key Lee does not teach wherein another

coordinate of said point is obtained from said one coordinate for inclusion as said one input.

However Gallant teaches wherein another coordinate of said point is obtained from said one coordinate for inclusion as said one input *(Gallant Fig 2 and 3 para 0039 – 0044).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of combination of Lee and DeBellis by accelerating multiplication of an elliptical curve point by a scalar over a finite field. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of accelerating multiplication of an elliptical curve point.

As per claim 8 Combination of Lee and DeBellis teaches a method wherein said other input is a representation of an elliptic curve point *(Lee page 239 "a block diagram ... infinity").*

As per claim 9 Combination of Lee and DeBellis teaches a method of scalar multiples used to change said secret value wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple *(Lee – Fig 1 - page 239)* and

Combination of Lee and DeBellis does not teach truncating said coordinate to a bit string for use as said random number.

However Gallant teaches truncating said coordinate to a bit string for use as said random number *(Gallant – para 0054 and 0068).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of combination of Lee and DeBellis by decreasing the bit-length to use as random number. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of random number generation system.

As per claim 27 Combination of Lee and DeBellis teaches an elliptic curve random number generator wherein said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple.

Combination of Lee and DeBellis does not teach truncating said coordinate to provide said output.

However Gallant teaches truncating said coordinate to provide said output *(Gallant – para 0054 and 0068).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve

Cryptography system of combination of Lee and DeBellis by decreasing the bit-length to use as random number. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of random number generation system.

As per claim 28 Combination of Lee and DeBellis teaches an elliptic curve random number generator according to claim 26 wherein said arithmetic unit includes a one way function and said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and applies said one way function to said coordinate of said scalar multiple to obtain said output *(Lee – Fig 1 - page 239 – 240).*

As per claim 29 Combination of Lee and DeBellis teaches an elliptic curve random number generator.

Combination of Lee and DeBellis Lee does not teach wherein said arithmetic unit truncates said coordinate of said scalar multiple prior to applying said one way function.

However Gallant teaches wherein said arithmetic unit truncates said coordinate of said scalar multiple prior to applying said one way function.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of combination of Lee and DeBellis by decreasing the bit-length to

use as random number. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of random number generation system.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. (IDS) and in view of U.S. Patent 6,044,388 to DeBellis et al. and in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant") and further in view of U.S. Publication 2005/0251680 to Brown et al. (hereinafter "Brown").

As per claim 10 Lee –DeBellis - Gallant teach a method wherein said one coordinate is truncated.

Lee –DeBellis - Gallant do not teach wherein the order of one half the length of a representation of an elliptic curve point representation.

However Brown teaches wherein the order of one half the length of a representation of an elliptic curve point representation *(para 0204)*.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Brown in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee –DeBellis - Gallant by calculation reducing abscissa value of x and y – coordinate. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of accelerating multiplication of an elliptical curve point.

Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. (IDS) and in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant") and further in view of U.S. Patent 6,044,388 to DeBellis et al. (hereinafter "DeBellis").

As per claim 11 Lee and Gallant teach a method wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple *(Gallant para 0054 – 0055 and as explained in claim 5).*

Lee and Gallant do not teach hashing said one coordinate to provide a bit string for use as said random number.

However DeBellis teaches hashing said one coordinate to provide a bit string for use as said random number *(DeBellis Fig 1 and 2 col 7 – lines 30 - 40).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of DeBellis in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee and Gallant by hashing point coordinate of an elliptical curve point. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

Claims 20 - 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. (IDS) and in view of U.S. Patent 6,044,388 to DeBellis et al. and in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant") and further in view of U.S. Patent 6,738,478 to Vanstone et al. (hereinafter "Vanstone").

As per claim 20 Lee –DeBellis - Gallant teach a method according to claim 5. Lee and Gallant do not teach wherein said secret value is derived from a coordinate of said other scalar multiple.

However Vanstone teaches where said secret value is derived from a coordinate of said other scalar multiple (Fig 2 - col 3 – lines 30 – 42).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Lee and Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee –DeBellis - Gallant by establishing an algorithm where scalar (k) is a private vector or secret value. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to minimizing the risk of successful timing attack by constantly changing value of scalar multiple and private key operations.

As per claim 21 Lee –DeBellis - Gallant teach elliptical curve random number generation. Lee and Gallant do not teach a method wherein the x coordinate of said other scalar multiple is used to change said secret value.

However Vanstone teaches wherein the x coordinate of said other scalar multiple is used to change said secret value *(Fig 2, col 3 – lines 42 – 67).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Lee and Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lee –DeBellis - Gallant by incorporating Montgomery method to derive x – coordinate of an ordered pair to change secret value. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to initialize a unique method to generate unique power signatures by involving multiple operations by changing scalar – secret value.

Conclusion

Claims 1 – 18, 20 - 29 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Since the Lee et al., "Elliptical Curve Random Number Generation" Electrical and Electronic Technology 2001. Tencon Proceedings of IEEE Region 10 International conference on 19 - 22 August 2001. Volume 1, pages 239 to 241 reference used in the above rejection was submitted by applicant in the prior art statement filed 7/26/2006, no copy thereof is provided with this Office action.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viral Lakhia whose telephone number is (571) 270 - 3363. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Korzuch William can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free)?

/Viral S Lakhia/

Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/336,814	Applicant(s)/Patent Under Reexamination BROWN ET AL.	
	Examiner VIRAL S. LAKHIA	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,044,388	03-2000	DeBellis et al.	708/254
*	B	US-2002/0044649	04-2002	Gallant et al.	380/30
*	C	US-2005/0251680	11-2005	Brown et al.	713/171
*	D	US-6,738,478	05-2004	Vanstone et al.	380/28
*	E	US-7,171,000	01-2007	Toh et al.	380/278
*	F	US-5,442,707	08-1995	Miyaji et al.	380/30
*	G	US-2007/0248224	10-2007	Buskey et al.	380/030
*	H	US-7,650,507	01-2010	Crandall et al.	713/176
*	I	US-6,243,467	06-2001	Reiter et al.	380/30
*	J	US-6,088,798	07-2000	Shimbo, Atsushi	713/176
*	K	US-6,477,254	11-2002	Miyazaki et al.	380/286
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	Art Unit
	VIRAL LAKHIA	4144

SEARCHED

Class	Subclass	Date	Examiner
380	28-30	6/17/09	V.L.
380	44-47	6/17/09	V.L.
380	277-286	6/17/09	V.L.
713	Search 713 with key word search of elliptic curve number generator	6/17/09	V.L.
726	Search 726 with key word search of elliptic curve number generator	6/17/09	V.L.

SEARCH NOTES

Search Notes	Date	Examiner
Key words and combination : elliptic curve number generator (creator, producer, intiator), message, digest, hash, random	7/17/09	V.L.
Get assistance with Fast and Focused Search department for the case	7/17/09	V.L
Get assistance from Peter Poltriak for claim interpretation and understanding of invention	7/17/09	V.L
Search Google Patents, NPL and wikipedia for elliptic curve technology	7/17/09	V.L
Update East with key word search	7/15/2010	V.L.

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/V. S. L./ Examiner.Art Unit 2431	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	4144

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010					
	1	✓		÷						
	2	✓		÷						
	3	✓		÷						
	4	✓		÷	✓					
	5	✓		÷	✓					
	6	✓		÷	✓					
	7	✓		÷	✓					
	8	✓		÷	✓					
	9	✓		÷	✓					
	10	✓		÷	✓					
	11	✓		÷	✓					
	12	✓		÷	✓					
	13	✓		÷	✓					
	14	✓		÷	✓					
	15	✓		÷	✓					
	16	✓		÷	✓					
	17	✓		÷	✓					
	18	✓		÷	✓					
	19		✓	÷	-					
	20			÷	✓					
	21			÷	✓					
	22			÷	✓					
	23			÷	✓					
	24			÷	✓					
	25			÷	✓					
	26			÷	✓					
	27			÷	✓					
	28			÷	✓					
	29			÷	✓					
	30			÷	-					
	31			÷	-					
	32			÷	-					
	33			÷	-					
	34			÷	-					
	35			÷	-					
	36			÷	-					

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	11/336,814
Filing Date	January 23, 2006
First named Inventor	BROWN, Daniel R.L.
Art Unit	4144
Examiner Name	LAKHIA, Viral S.
Attorney Docket Number	67539/00622

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]	Number[4]	Kind-Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		WO	01/13218	A1	02-22-2001	SIEMENS AG		
		CA	2,381,397	A1	02-22-2001	SIEMENS AG		

Examiner Signature	/Viral Lakhia/	Date Considered	03/08/2010

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] **Applicants' unique citation designation number** (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	11/336,814
Filing Date	January 23, 2006
First named Inventor	BROWN, Daniel R.L.
Art Unit	4144
Examiner Name	LAKHIA, Viral S.
Attorney Docket Number	67539/00622

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalogue, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
		JOHNSON, Don B.; "X9.82 Part 3 – Number Theoretic DRBGs"; NIST RNG Workshop; July 20, 2004; Retrieved from http://csrc.nist.gov/groups/ST/toolkit/documents/rng/NumberTheoreticDRBG.pdf	
		PRINS, Leendert; supplementary European Search Report from corresponding EP Application No. 06704329.9; search completed October 29, 2009	

Examiner Signature	/Viral Lakhia/	Date Considered	03/08/2010

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] **Applicants' unique citation designation number** (optional). [2] Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C> 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	62	(input$3) same (escrow $2 near4 key$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:11
L3	1	(input$3 near5 point $2) same (escrow$2 near4 key$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:11
L4	2107	(elliptical adj curve$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:12
L5	2107	(elliptical adj curve$2) 2 and 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:14
L6	0	2 and 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:14
L7	208786	(input$3) near5 (point $4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:22
L8	208	(relat$4 associat$4 referen$4) same (escrow near5 key$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:24

L9	122	5 and 7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:24
L10	0	8 and 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:24
L11	809	(escrow$3) near5 (key $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:27
L12	2	4 and 11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:27
L13	0	4 same 11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/10 10:28
S1	1	"11336814"	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/16 15:39
S2	18109	"380".clas.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52
S3	3324	380/28-30.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52
S4	2286	380/44-47.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:52
S5	3939	380/277-286.ccls.	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:53
S6	5	"5073935" "5142577"	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:53
S7	0	elliptic (3n) curve? ?	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/17 08:59
S8	3136	elliptic near5 curve and (number$3 or value$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:01

S9	1471899	generator or creator or producer or intiator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:03
S10	1382	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:04
S11	5042269	Hash or function or digest	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:10
S12	5042357	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)or hash or function or digest	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:10
S13	886	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11
S14	176	S2 and S3 and S4 and S5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11
S15	17	S13 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:11
S16	870	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:13

S17	17	S14 and S16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14
S18	529	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5) and exchange	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14
S19	12	S14 and S18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:14
S20	2	JP "2003124919"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 09:30
S21	2	"7327845"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 12:18
S22	2	"20070189527"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 12:18
S23	0	"2005644982"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:57
S24	2	"20070189527"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:57

S25	2	JP "2003124919"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 14:59
S26	6	"6934392"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:05
S27	529	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5) and exchange	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:07
S28	4	S27 and S26	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 15:07
S29	5666	"713".clas. and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/17 16:36
S30	1	"11336816"	US-PGPUB; USPAT; FPRS	ADJ	ON	2009/06/18 08:28
S31	0	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and function and (crypto$5 or encrypt$5) and exchange and escrow (backup)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 08:50
S32	79	elliptic near5 curve and (number$3 or value$3) and (generator or creator or producer or initiator or maker)and (hash or digest)and escrow and key	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 08:50

S33	6	"10384328"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 08:57
S34	6	"10384328"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 09:03
S35	14	"7113594"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2009/06/18 09:13
S36	34	"6044388"	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:17
S37	1	"6044388".pn.	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:17
S38	57	"5442707"	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:25
S39	1	"20070248224"	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:25
S40	1	"7650507"	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:25
S41	10	"6243467"	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:25
S42	5	"6477254"	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:25
S43	9	"6088798"	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:25
S44	0	"5442707.pn."	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/08 09:26
S45	1	scalar near4 (random adj generat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/08 12:17
S46	0	scalar near4 (random adj generat$4) and (elliptic$4 adj curve)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/08 12:21

S47	2	scalar same (random adj generat$4) and (elliptic$4 adj curve)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/08 12:22
S48	6	scalar same4 (random adj generat$4) same4 (elliptic$4 adj curve)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/08 12:26
S49	4	((secret or hid$4) adj (value number)) same (scala$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 07:45
S50	0	(plural$3 multiple) same (elliptical adj curve adj random adj number) same (escrow) same (key$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:06
S51	0	(elliptical adj curve adj random adj number) same (escrow) same (key$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:07
S52	958	(escrow) same (key$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:07
S53	15	((escrow) same (key $2)) with (random adj number)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:07
S54	1462	(elliptical adj curve)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:08

S55	0	S53 and S54	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:08
S56	5	(save store) same (escrow adj key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:11
S57	110195	(administrator)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:11
S58	2	S56 and S57	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:11
S59	0	(elliptical adj curve adj random adj number) same (escrow) same (key$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:52
S60	0	(elliptical adj curve adj random adj number)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:52
S61	103	(escrow) adj (key$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:52
S62	0	S60 and S61	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2010/03/09 09:53
S63	558	(half) same (coordinate) same (curve)	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/09 13:12

S64	6	(half) same (coordinate) same (curve) same (elliptical $2)	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/09 13:13
S65	27	(half) same (coordinate) same (curve) same (elliptic $2)	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/09 13:13
S66	0	(escrow adj key$3) same (secur$2 near4 (domain field area))	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/09 13:38
S67	0	(escrow adj key$3) same (secur$2 near4 (domain field area)) same (common)	US-PGPUB; USPAT; FPRS	ADJ	ON	2010/03/09 13:38

3/10/2010 11:32:21 AM
C:\Documents and Settings\vlakhia\My Documents\EAST\Workspaces\11336814.wsp

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	"11336814"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 13:58
L2	11	(elliptical curve random number generator)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	WITH	ON	2010/07/15 14:04
L3	178	(elliptical with curve with cryptography)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 14:57
L4	28369	(random near2 number near2 generator$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 14:57
L5	12	3 same 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 14:57
L6	28461	((random pseudo) near2 number near2 generator$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 14:58
L7	41	3 and 6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 14:58

S1	3	"11336814"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 11:57

7/15/2010 3:43:53 PM
C:\Documents and Settings\vlakhia\My Documents\EAST\Workspaces\11336814.i..wsp

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/336,814**

Applicant: **BROWN, Daniel R.L.; VANSTONE, Scott A.**

Filed: **January 23, 2006**

Title: **Elliptic Curve Random Number Generation**

Art Unit: **2431**

Examiner: **LAKHIA, Viral S.**

Docket No.: **67539/00622**

Mail Stop AF
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE

Sir:

In response to the Office Action dated August 23, 2010 the Applicant's wish to amend the application in the following manner.

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Remarks: begin on page 7 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of:

providing obtaining a first pair of input[[s]] to said arithmetic unit, with each input representative of at least one coordinate of an elliptic curve point, a second input representative of at least one coordinate of another of said pair of points, said inputs being obtained in a manner to ensure that one point of said pair of points would not have been chosen as a known multiple of the other point of the pair of points and with at least one of said inputs being verifiably random;

providing said first input and said second input as inputs to said arithmetic unit;

performing selected elliptic curve operations on said inputs to obtain an output; and utilising said output as a random number in the cryptographic operation.

2. (currently amended) [[A]] The method according to claim 1 wherein said at least one of said inputs is obtained from an output of a hash function.

3. (currently amended) [[A]] The method according to claim 2 wherein the other of said inputs is utilized as an input to said hash function.

4. (currently amended) [[A]] The method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

5. (currently amended) [[A]] The method according to claim 4 wherein one of said scalar multiples is used to derive said random number and the other of said scalar multiples is used to change said secret value for subsequent use.

6. (currently amended) [[A]] The method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input.

7. (currently amended) [[A]] The method according to claim 6 wherein another coordinate of said point is obtained from said one coordinate for inclusion as said one input.

8. (currently amended) [[A]] The method according to claim 7 wherein said other input is a representation of an elliptic curve point.

9. (currently amended) [[A]] The method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and truncating said coordinate to a bit string for use as said random number.

10. (currently amended) [[A]] The method according to claim 9 wherein said one coordinate is truncated in the order of one half the length of a representation of an elliptic curve point representation.

11. (currently amended) [[A]] The method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and hashing said one coordinate to provide a bit string for use as said random number.

12. (currently amended) [[A]] The method according to claim 1 wherein one of said ~~verifiably random~~ inputs is chosen to be of a canonical form, whereby a predetermined relationship between said inputs is difficult to maintain.

13. (previously presented) A method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of:

providing a pair of inputs, each representative of at least one coordinate of a pair of elliptic curve points, to said arithmetic unit;

performing elliptic curve operations to obtain an output representative of at least one coordinate of a scalar multiple of an elliptic curve point;

passing said output through a one way function to obtain a bit string for use as a random number; and

utilising said random number in the cryptographic operation.

14. (currently amended) [[A]] The method according to claim 13 wherein said one way function is a hash function.

15. (currently amended) An elliptic curve random number generator comprising a first ~~pair of~~ input[[s]], ~~each of said inputs being~~ representative of at least one coordinate of a first ~~pair of~~ elliptic curve point[[s]] a second input representative of a coordinate of a second elliptic curve point; an arithmetic unit to perform elliptic curve operations on said first input and said second input[[s]]; and an output to receive the results of said elliptic operations, said output representing a random number for use in a cryptographic operation, at least one of said inputs having been obtained in a manner to ensure that one point of said first point and said second point would not have been chosen as a known multiple of the other point of said first point and said second point ~~being verifiably random~~.

16. (currently amended) [[An]] The elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function.

17. (currently amended) [[An]] The elliptic curve random number generator according to claim 16 wherein said one way function is a hash function.

18. (currently amended) [[An]] The elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function.

19. (cancelled)

20. (currently amended) [[A]] The method according to claim 5 wherein said secret value is derived from a coordinate of said other scalar multiple.

21. (currently amended) [[A]] The method according to claim 20 wherein the $\bar{x}$ coordinate of said other scalar multiple is used to change said secret value.

22. (currently amended) [[An]] The elliptic curve random number generator according to claim 15 wherein said arithmetic unit operates on said inputs to obtain a scalar multiple of a coordinate of a point represented by said one input.

23. (currently amended) [[An]] The elliptic curve random number generator according to claim 22 [[23]] wherein said arithmetic unit computes a coordinate of a scalar multiple of each of said points represented by said inputs

24. (currently amended) [[An]] The elliptic curve random number generator according to claim 23 wherein said coordinate of said scalar multiple of said point represented by said one input is operated on by said arithmetic unit and utilised as said output.

25. (currently amended) [[An]] The elliptic curve random number generator according to claim 24 wherein said arithmetic unit includes a register to maintain a secret value and a value derived from said coordinate of said scalar multiple of the point represented by said other input is stored in said register to provide said secret value.

26. (currently amended) [[An]] The elliptic curve random number generator according to claim 25 wherein said arithmetic unit utilises said secret value and said one input to obtain said coordinate of said scalar multiple of said point represented by said one input.

27. (currently amended) [[An]] The elliptic curve random number generator according to claim 26 wherein said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and truncates said coordinate to provide said output.

28. (currently amended) [[An]] The elliptic curve random number generator according to claim 26 wherein said arithmetic unit includes a one way function and said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and applies said one way function to said coordinate of said scalar multiple to obtain said output.

29. (currently amended) [[An]] The elliptic curve random number generator according to claim 28 wherein said arithmetic unit truncates said coordinate of said scalar multiple prior to applying said one way function.

30. (cancelled)

31. (cancelled)

32. (cancelled)

33. (cancelled)

34. (cancelled)

35. (cancelled)

36. (cancelled)

37. (new) The method according to claim 2 wherein both of said inputs are obtained from outputs of respective hash functions.

38. (new) The method according to claim 37 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

39. (new) The method according to claim 38 wherein one of said scalar multiples of said points is used to derive said random number.

40. (new) The method according to claim 39 wherein said random number is derived by converting a coordinate of said one of said scalar multiples of said points to an integer and truncating the resultant value for use as said random number.

41. (new) The method according to claim 40 wherein said coordinate is the x coordinate.

42. (new) The method according to claim 39 wherein the other of said scalar multiples of said points is used to change said secret value for subsequent use.

43. (new) The method according to claim 42 wherein a coordinate of said other of said scalar multiples of said points is converted to an integer and used as a secret value.

44. (new) The method according to claim 43 wherein said coordinate is the x coordinate.

45. (new) The elliptic curve random number generator of claim 16 wherein each of said inputs includes a hash function.

46. (new) The elliptic curve random number generator of claim 16 including a secret value said secret value and said arithmetic processor uses said secret value to compute scalar multiples of said points represented by said inputs.

47. (new) The ECRNG according to claim 45 wherein one of said scalar multiples of said points is used to derive said random number.

48. (new) The ECRNG according to claim 47 wherein said arithmetic processor convers a coordinate of said one of said scalar multiples of said points to an integer and truncates the resultant value, and outputs said truncated value for use as said random number.

49. (new) The ECRNG according to claim 48 wherein said coordinate is the x coordinate.

50. (new) The ERNG according to claim 47 wherein the other of said scalar multiples of said points is used to change said secret value for subsequent use.

51. (new) The method according to claim 50 wherein a coordinate of said other of said scalar multiples of said points is converted to an integer and used as a secret value.

52. (new) The method according to claim 51 wherein said coordinate is the x coordinate.

REMARKS

The Applicant's thank the Examiner for his examination of the above application and for the comments in the Office Action dated August 23, 2010.

Claim 1 has been amended to clarify the language used in that claim without changing the scope thereof. The amendment to claim 1 does not necessitate a further search and places the application in condition for allowance.

Corresponding amendments have been made to claim 15.

New claims 37 – 52 are submitted that depend upon either claim 1 (method) or claim 15 (apparatus). As these claims depend either directly or indirectly upon claim 1 or claim 15, it is believed that no further search is required in respect to these added claims.

The amendment to the dependency of claim 23 has been corrected and the Examiner is thanked for her helpful suggestion in this regard.

The Examiner rejected claim 1 under 35 U.S.C. 102 (b) on the basis of a paper to Lee. Lee discloses a random number generator, but does not disclose features recited within claim 1. As such, Lee cannot anticipate claim 1 or the claims dependent thereon.

Claim 1 is directed to a method of operating an elliptic curve random number generator and requires obtaining a pair of inputs and operating on those inputs with an arithmetic unit to perform elliptic curve operations on those inputs.

The reference to Lee does not disclose a pair of inputs. It will be noted that one arrow in Lee indicates that it is used in the first cycle only, that us to provide the Seed k_1. Subsequent cycles use only the input labeled k_{n+1}. Accordingly, Lee does not disclose the use of a pair of inputs or performing elliptic curve operations on the inputs.

For this reason alone, Lee cannot anticipate claim 1.

Moreover, claim 1 requires each input be representative of a coordinate of an elliptic curve

point. Lee is silent as to the nature of the value k_{n+1} and does not disclose or suggest that it is representative of a coordinate of an elliptic curve point. Accordingly, Lee fails to disclose the feature recited in claim 1 requiring the inputs to be representative of coordinates of elliptic curve points.

Claim 1 has also been amended to recite the relationship between the inputs, namely that one of the pair of points would not have been chosen as a known multiple of the other of the pair of points. This language can be found at paragraph 32 of the specification.

As Lee does not have a pair of inputs, there is no disclosure of this feature and it cannot be suggested by the teachings of Lee.

Again, therefore, Lee cannot be considered to anticipate claim 1 due to the emission of this feature.

In view of the above distinctions, it is believed that Lee does not anticipate claim 1 under the provisions of 35 U.S.C. 102 (b).

Similarly, claim 12, that depends upon claim 1, cannot be considered to be anticipated in that claim 1 is not anticipated.

Corresponding amendments have been made to claim 15, the apparatus claim directed to the elliptic curve random number generator, and for the reasons noted above, it is believed that Lee cannot anticipate claim 15. Similarly, claims 22 to 24, that depend upon claim 15, cannot be considered anticipated.

The Examiner has rejected claims 2 – 4, 6, 13 – 14, 16 – 18 and 25 – 26 under 35 U.S.C. 103 (a) as being unpatentable over Lee in view of the reference to DeBellis. The portions of DeBellis relied on by the Examiner do not reference the use of hash functions and do not disclose the provision of a pair of inputs arranged in the manner recited in claim 1. As such, the combination of DeBellis and Lee do not disclose the features recited in claim 1, and by inference, the claims dependent on claim 1. A fundamental starting point of the KSR analysis is to find each element claimed in the combination of art. The combination relied on by the Examiner fails to provide each element claimed and therefore the combination cannot render claims 2 through 4 and 6 obvious.

Similarly, claim 13 recites the provision of a pair of inputs and the use of a one-way function on the output. This combination of features is not taught in Lee and DeBellis and, accordingly, claim 13 and the claims dependent thereon cannot be considered obvious in view of that combination.

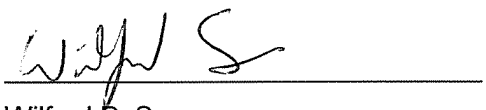
The claims dependent upon claim 15 likewise do not teach the combination of features recited in claim 15 and therefore cannot render the dependent claims obvious.

The Examiner has relied upon the tertiary reference of Gallant to teach the features recited in claims 5, 7 – 9 and 27 – 29. However, as noted above, the primary reference of Lee fails to teach the features recited in the claims upon which these claims depend and neither Gallant nor DeBellis nor Lee teach those features. As such, it is believed that the combination relied on by the Examiner fails to meet the threshold in KSR test and cannot render those claims obvious.

The Examiner relies upon a fourth reference to show the feature of claim 10, namely U.S. publication no. 2005/0251680 to Brown. Again, the failure of Lee to recite the features recited in claim 1 and the absence of those features from any of the supplementary references, including Brown, supports the finding of non-obviousness.

Further consideration of the application, entry of these amendments and allowance of the application is respectively requested.

Respectfully submitted,



Wilfred P. So
Agent for Applicant
Registration No. 65,981

Date: October 22, 2010

BLAKE, CASSELS & GRAYDON LLP
199 Bay Street
Suite 2800, Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: 416-863-2425
SOW/JRO/lxi

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	Wilfred P. So/Judith Martin
Attorney Docket Number:	67539/622

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	1202	8	52	416
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**416**

Electronic Acknowledgement Receipt

EFS ID:	8685162
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	91704
Filer:	Wilfred P. So/Judith Martin
Filer Authorized By:	Wilfred P. So
Attorney Docket Number:	67539/622
Receipt Date:	22-OCT-2010
Filing Date:	23-JAN-2006
Time Stamp:	16:04:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$416
RAM confirmation Number	2514
Deposit Account	022553
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		35404-US-PAT_OA_Response.pdf	593634 5d6fac2f894de39484a39173f2788123daf2a193	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment After Final	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	10

Warnings:

Information:

2	Fee Worksheet (PTO-875)	fee-info.pdf	30358 87f5b6c8ab1f4b61d5231ed74f44085d7fb8e370	no	2

Warnings:

Information:

Total Files Size (in bytes):	623992

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/336,814	Filing Date 01/23/2006	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	10/22/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 44	Minus	** 36	= 8	X $ =		OR	X $52=	416
	Independent (37 CFR 1.16(h))	* 3	Minus	***5	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**416**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/FRANCES Y. FIELDS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/336,814**

Applicant: **BROWN, Daniel R.L.; VANSTONE, Scott A.**

Filed: **January 23, 2006**

Title: **Elliptic Curve Random Number Generation**

Art Unit: **2431**

Examiner: **LAKHIA, Viral S.**

Docket No.: **67539/00622**

Mail Stop AF
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE

Sir:

In response to the Office Action dated August 23, 2010 the Applicant's wish to amend the application in the following manner.

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Remarks: begin on page 7 of this paper.

DO NOT ENTER: /V.L./ 11/01/2010

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

91704 7590 11/04/2010

Blake, Cassels & Graydon LLP
199 BAY STREET , SUITE 2800
COMMERCE COURT WEST
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
LAKHIA, VIRAL S	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
11/04/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

rimpatent@blakes.com
brett.slaney@blakes.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 11/336,814	**Applicant(s)** BROWN ET AL.	
	Examiner VIRAL S. LAKHIA	**Art Unit** 2431	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 22 October 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☒ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-18 and 20-29*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Viral S Lakhia/
Examiner, Art Unit 2431

/Syed Zia/
Primary Examiner, Art Unit 2431

Continuation of 3. NOTE: Claims 1-29 and 37 - 52 have been amended raising new issues requiring further consideration and/or search.

Further, Applicant argues that refernce of Lee does not teach "use of pair of inputs or performing elliptical curve operations on the inputs". Examiner does not find the argument persuasive.

Examiner does not find argument persuasive because Lee defines use of inputs to generate elliptical curve, for one of the ordinary skills in the art, examiner assumes that input for elliptical curve consists of point on an elliptical curve over a defined field elements which is described in Lee - page 239 - 241.

Applicant futher argues that Lee does not teach, "inputs to be representative of the coordiantes of elliptical curve points", examiner does not find argument persuasive.

Examiner does not find argument persuasive because, Lee pages 239 - 241 describes point P on an elliptical curve over finite fields, which reads on claim limitation since points represent inputs (as explained above) and inputs over finite fields represent coordinates of ellipical curve points.

Further claim 1 amendments of ".. second input representative being obtained without known multiple of the other pair of points .. " requires further consideration and search.

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/336,814
Filing Date	January 23, 2006
First Named Inventor	BROWN, Daniel R.L.
Art Unit	2431
Examiner Name	LAKHIA, Viral S.
Attorney Docket Number	57539/00622

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☑ Enclosed

      i. ☑ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. ☑ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 02-2553 .

      i. ☑ RCE fee required under 37 CFR 1.17(e)

      ii. ☐ Extension of time fee (37 CFR 1.136 and 1.17)

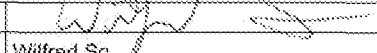
      iii. ☐ Other _____

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature		Date	February 23, 2011
Name (Print/Type)	Willfred So	Registration No.	65,981

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/22 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARMENT OF COMMERCE

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) **FY 2009** *(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)*	Docket Number (Optional) 67539/00622
Application Number 11/336,814	Filed January 23, 2006
For ELLIPTIC CURVE RANDOM NUMBER GENERATION	
Art Unit 2431	Examiner LAKHIA, Viral S.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$130	$65	$
☐	Two months (37 CFR 1.17(a)(2))	$490	$245	$
☑	Three months (37 CFR 1.17(a)(3))	$1110	$555	$ 1110.00
☐	Four months (37 CFR 1.17(a)(4))	$1730	$865	$
☐	Five months (37 CFR 1.17(a)(5))	$2350	$1175	$

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 02-2553.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

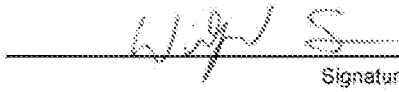
I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration Number 65,981

☐ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____



Signature

February 23, 2011
Date

Wilfred So
Typed or printed name

(416) 863-2425
Telephone Number

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☑ Total of 1 forms are submitted.

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	John Robert Scoley Orange/Judith Martin
Attorney Docket Number:	67539/622

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	1202	13	52	676
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1110	1110
Miscellaneous:				
Request for continued examination	1801	1	810	810
		Total in USD ($)		**2596**

Electronic Acknowledgement Receipt

EFS ID:	9518822
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	91704
Filer:	John Robert Scoley Orange/Judith Martin
Filer Authorized By:	John Robert Scoley Orange
Attorney Docket Number:	67539/622
Receipt Date:	23-FEB-2011
Filing Date:	23-JAN-2006
Time Stamp:	19:36:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2596
RAM confirmation Number	6983
Deposit Account	022553
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		35404-US-PAT_OA-Response.pdf	2421962 00a172af7c1d652e9b2ee8b18d374c9cb72ef46c	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment After Final	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	12

Warnings:

Information:

2	Request for Continued Examination (RCE)	35404-US-PAT_RCE.pdf	343330 104954080bc4ce916a6d95b8647332a6b3d8bbb2	no	1

Warnings:

This is not a USPTO supplied RCE SB30 form.

Information:

3	Extension of Time	35404-US-PAT_petition-ext-of-time.pdf	289496 8d60dcf7414562d3df2446918d4f6be7b9096449	no	1

Warnings:

Information:

4	Fee Worksheet (PTO-875)	fee-info.pdf	33797 2d68ea642b5ffac03248560c873e8ef37468d3b2	no	2

Warnings:

Information:

Total Files Size (in bytes):	3088585

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/336,814**

Applicant: **BROWN, Daniel R.L.; VANSTONE, Scott A.**

Filed: **January 23, 2006**

Title: **Elliptic Curve Random Number Generation**

Art Unit: **2431**

Examiner: **LAKHIA, Viral S.**

Docket No.: **67539/00622**

Mail Stop AF
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE and REQUEST FOR CONTINUED EXAMINATION

Sir:

In response to the Office Action dated August 23, 2010, and the Advisory Action dated 4 November 2010, the Applicants submit a Request for Continued Examination, a Request for a three month Extension of Time to Respond, and wish to amend the application in the following manner.

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Remarks: begin on page 8 of this paper.

REMARKS

The Applicants thank the Examiner for the examination of the above application, for the comments in the Office Action dated August 23, 2010 and explanation in the Advisory Action of November 4th 2010.

The Applicants submit herewith an Amendment, together with a Request for Continued Examination. The Advisory Action indicates that the amendments submitted in response to the Final Office Action have not been entered. Accordingly, the amendments submitted herewith are indicated as amendments to the claims pending in the application at the time of Office Action dated August 23, 2010.

Claim 1 has been amended to clarify the language used in that claim and to recite that the first input is representative of an elliptic curve point; that the second input is representative of another elliptic curve point; and that the elliptic curve points are verifiably random.

Corresponding amendments have been made to claim 15.

Claim 13 has been amended to recite that the first input is representative of an elliptic curve point; and that the second input is representative of another elliptic curve point.

New claims 37 – 66 are submitted which depend upon either claim 1 (method) or claim 15 (apparatus).

New claim 67 is submitted which is an apparatus claim corresponding to method claim 13.

The amendment to the dependency of claim 23 has been corrected and the Examiner is thanked for her helpful suggestion in this regard.

Claims 8 and 12 have been cancelled without prejudice to provide consistency with amended claim 1.

A typographical error has been corrected in claim 21.

The Examiner rejected claim 1 under 35 U.S.C. 102 (b) on the basis of a paper to Lee. Lee discloses a random number generator, but does not disclose features recited within claim 1. As

such, Lee cannot anticipate claim 1 or the claims dependent thereon.

Claim 1 is directed to a method of operating an elliptic curve random number generator and recites obtaining a first input as well as a second input and performing selected elliptic curve operations on those inputs.

The reference to Lee does not disclose a first input as well as a second input. It will be noted that one arrow in Lee indicates that it is used in the first cycle only, that is to provide the Seed k_1. Subsequent cycles use only the input labeled k_{n+1}. Accordingly, Lee does not disclose the use of a first input and a second input nor performing elliptic curve operations on the inputs.

For this reason alone, Lee cannot anticipate claim 1.

Moreover, claim 1 recites the first input is representative of an elliptic curve point, and the second input is representative of another elliptic curve point. Lee is silent as to the nature of the value k_{n+1} and does not disclose or suggest that it is representative of an elliptic curve point. Accordingly, Lee fails to disclose the feature recited in claim 1 that the first input and second inputs are representative of elliptic curve points.

Claim 1 has also been amended to recite that the points are verifiably random. As Lee does not have a pair of inputs, there is no disclosure of this feature and it cannot be suggested by the teachings of Lee.

Again, therefore, Lee cannot be considered to anticipate claim 1 due to the omission of this feature.

In view of the above distinctions, it is respectfully submitted that Lee does not anticipate claim 1 under the provisions of 35 U.S.C. 102 (b).

In the comments accompanying the Advisory Action, the Examiner suggests that because Lee defines use of inputs to generate an elliptic curve, there is an assumption that the input for the curve consists of a point on an elliptic curve. The Applicants' representative does not understand the comment made by the Examiner and requests further clarification. Lee does not describe nor suggest that the seed input k_i is representative of a point on an elliptic curve. The only constraint that is placed on k_i is that it not have a value equal to the order of P.

The value of k_{n+1} is explicitly described as $x_n + n$, where n is the current cycle number. There is no check as to whether this is representative of a point on an elliptic curve.

Therefore, the input shown in Lee to the arithmetic unit that performs the elliptic curve operation does not satisfy the recitation in the claim that it is representative of a point on an elliptic curve. Moreover, as understood by the Applicant, there is only one input to the arithmetic unit of Lee, rather than the pair recited in claim 1.

Corresponding amendments have been made to claim 15, the apparatus claim directed to the elliptic curve random number generator, and for the reasons noted above, it is believed that Lee cannot anticipate claim 15. Similarly, claims 22 to 24, and claims 59 to 64 which depend upon claim 15, cannot be considered anticipated.

The Examiner has rejected claims 2 – 4, 6, 13 – 14, 16 – 18 and 25 – 26 under 35 U.S.C. 103 (a) as being unpatentable over Lee in view of the reference to DeBellis.

Addressing firstly the rejection of claims 2-3 and 6, each of those claims recites that at least one of the inputs is derived from a hash function. As noted above, Lee does not disclose a pair of inputs as recited in claim 1, on which claim 2 depends, nor does Lee disclose the use of a hash function on at least one input as recited in claim 12. Whilst DeBellis references a hash function 230 on a single external input 226, it does not disclose a pair of inputs arranged in the manner recited in claim 1, with at least one of those inputs being derived from an output of a hash function, nor does it disclose that the input derived from the hash function is representative of an elliptic curve point. DeBellis places no constraints on the output of the hash function 230.

As such, the combination of Lee and DeBellis do not disclose the features recited in claim 1, and by inference, claims 2-3 and 6 that depend on claim 1. A fundamental starting point of the KSR analysis is to find each element claimed in the combination of art. The combination relied on by the Examiner fails to provide each element claimed and therefore the combination cannot render claims 2-3 and 6 obvious.

Claim 4 depends on claim 1 and recites that the secret value is used to compute scalar multiples of said points used as inputs. As discussed above, neither Lee nor DeBellis disclose a pair of inputs, each input representative of an elliptic curve point. As such, for the reasons discussed above, the combination of Lee and DeBellis cannot render claim 4 obvious.

Claim 15 similarly recites a first input representative of an elliptic curve point and a second input representative of another elliptic curve point, each of said points being verifiably random. As discussed above, this combination is not found in Lee or in DeBellis. Accordingly, whilst DeBellis references a hash function 230 on a single external input 226, it does not disclose the pair of inputs arranged in the manner recited in claim 15. As such, the combination of Lee and DeBellis does not disclose each and every feature recited in claim 15, nor, by inference, claims 16 - 18 which depend on claim 15.

Claims 25-26 depend upon claim 15 and accordingly recite a first input representative of an elliptic curve point and a second input representative of another elliptic curve point, each of said points being verifiably random. As discussed above, this combination is not found in Lee or in DeBellis, and, for the reasons discussed above, the combination of Lee and DeBellis does not render those claims obvious.

Claim 13 recites obtaining a first input representative of an elliptic curve point and obtaining a second input representative of another elliptic curve point. As discussed above, neither Lee nor DeBellis teach a first input representative of an elliptic curve point and a second input representative of another elliptic curve point. Claim 13 also recites passing the output obtained from performing elliptic curve operations on the inputs through a one way function. Lee does not disclose the use of a one way function on an output and neither does DeBellis. This combination of features is not taught in Lee and DeBellis and, accordingly, claim 13 and the claims dependent thereon cannot be considered obvious in view of that combination.

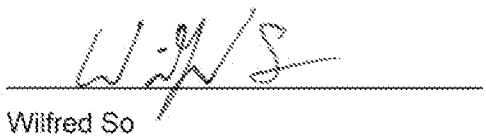
The Examiner has relied upon the tertiary reference of Gallant to teach the features recited in claims 5, 7 – 9 and 27 – 29. However, as noted above, the primary reference of Lee fails to teach the features recited in the claims upon which these claims depend and neither Gallant nor DeBellis teach those features. As such, it is believed that the combination relied on by the Examiner fails to meet the threshold in KSR test and cannot render those claims obvious.

The Examiner relies upon a fourth reference to show the feature of claim 10, namely U.S. publication no. 2005/0251680 to Brown. Again, the failure of Lee to recite the features recited in claim 1 and the absence of those features from any of the supplementary references, including Brown, supports the finding of non-obviousness.

Further consideration of the application, entry of these amendments and allowance of the

application are respectively requested.

Respectfully submitted,



Wilfred So
Agent for Applicant
Registration No. 65,981

Date: FEBRUARY 23, 2011

BLAKE, CASSELS & GRAYDON LLP
199 Bay Street
Suite 2800, Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: 416-863-2425
JRO/lxi

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/336,814	01/23/2006	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	02/23/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 57	Minus	** 44	= 13	X $ =		OR	X $52=	676
	Independent (37 CFR 1.16(h))	* 4	Minus	***5	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**676**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/STEFANIE BRYCE/

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/336,814**

Applicant: **BROWN, Daniel R.L.; VANSTONE, Scott A.**

Filed: **January 23, 2006**

Title: **Elliptic Curve Random Number Generation**

Art Unit: **2431**

Examiner: **LAKHIA, Viral S.**

Docket No.: **67539/00622**

U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL AMENDMENT

Sir:

Further to the Response filed February 23, 2011, in response to the Office Action dated August 23, 2010, and the Advisory Action dated 4 November 2010, the Applicants wish to amend the application in the following manner.

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Remarks: begin on page 8 of this paper.

REMARKS

Further to the Response, Request for Continued Examination and Petition for Extension of Time filed February 23, 2011, the Applicants have hereby corrected a typographical error in claim 13.

Further consideration of the application, entry of this amendment and allowance of the application are respectively requested.

Respectfully submitted,

Wilfred So
Agent for Applicant
Registration No. 65,981

Date: February 24, 2011

BLAKE, CASSELS & GRAYDON LLP
199 Bay Street
Suite 2800, Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: 416-863-2425
JRO/lxl

22083312.1

Electronic Acknowledgement Receipt

EFS ID:	9528219
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	91704
Filer:	John Robert Scoley Orange/Judith Martin
Filer Authorized By:	John Robert Scoley Orange
Attorney Docket Number:	67539/622
Receipt Date:	24-FEB-2011
Filing Date:	23-JAN-2006
Time Stamp:	17:35:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		35404-US-PAT_supplemental_amendment.pdf	1493165 ee173fe6783da784066e260034626a878ef58a64	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Supplemental Response or Supplemental Amendment	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	8
Warnings:			
Information:			
	Total Files Size (in bytes):	1493165	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/336,814	Filing Date 01/23/2006	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	02/24/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 57	Minus	** 57	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***4	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/BRUCE HARRISON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of:

   ~~providing~~ obtaining a ~~pair of inputs~~ first input ~~to said arithmetic unit, with each input~~ representative of ~~at least one coordinate of~~ an elliptic curve point,

   obtaining a second input representative of another elliptic curve point,

   each ~~and with at least one~~ of said points ~~inputs~~ being verifiably random;

   providing said first input and said second input as inputs to said arithmetic unit;

   performing selected elliptic curve operations on said inputs ~~to~~ and ~~obtain~~ obtaining an output; and

   utilising said output as a random number in the cryptographic operation.

2. (currently amended) A The method according to claim 1 wherein ~~said~~ at least one ~~input~~ of said inputs is ~~obtained~~ derived from an output of a hash function.

3. (currently amended) A The method according to claim 2 wherein the other of said inputs is utilized as an input to said hash function.

4. (currently amended) A The method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

5. (currently amended) A The method according to claim 4 wherein one of said scalar multiples is used to derive said random number and the other of said scalar multiples is used to change said secret value for subsequent use.

6. (currently amended) A The method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input.

7. (currently amended) A The method according to claim 6 wherein another coordinate of said point is obtained from said one coordinate for inclusion as said one input.

8. (cancelled).

9. (currently amended) A The method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and truncating said coordinate to a bit string for use as said random number.

10. (currently amended) A The method according to claim 9 wherein said one coordinate is truncated in the order of one half the length of a representation of an elliptic curve point representation.

11. (currently amended) A The method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and hashing said one coordinate to provide a bit string for use as said random number.

12. (cancelled).

13. (currently amended) A method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of:

providing obtaining a first input pair of inputs, each representative of at least one coordinate of a pair of an elliptic curve point points, to said arithmetic unit;

obtaining a second input representative of another elliptic curve point;

performing elliptic curve operations on said inputs to obtain an output representative of at least one coordinate of a sca3lar multiple of an elliptic curve point;

passing said output through a one way function to obtain a bit string for use as a random number; and

utilising said random number in the cryptographic operation.

14. (currently amended) A The method according to claim 13 wherein said one way function is a hash function.

15. (currently amended) An elliptic curve random number generator comprising a first input pair of inputs, each of said inputs being representative of at least one coordinate of a pair of an elliptic curve point points; a second input representative of another elliptic curve point, each of said points being verifiably random; an arithmetic unit to perform elliptic curve operations on said inputs; and an output to receive the results of said elliptic curve operations, said

output representing a random number for use in a cryptographic operation~~, at least one of said inputs being verifiably random~~.

16. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function.

17. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 16 wherein said one way function is a hash function.

18. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function.

19. (cancelled)

20. (currently amended) ~~An~~ The method according to claim 5 wherein said secret value is derived from a coordinate of said other scalar multiple.

21. (currently amended) ~~An~~ The method according to claim 20 wherein ~~the~~ $[[\bar{x}]]$ an x coordinate of said other scalar multiple is used to change said secret value.

22. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 15 wherein said arithmetic unit operates on said inputs to obtain a scalar multiple of a coordinate of a point represented by said one input.

23. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 22 ~~23~~ wherein said arithmetic unit computes a coordinate of a scalar multiple of each of said points represented by said inputs.

24. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 23 wherein said coordinate of said scalar multiple of said point represented by said one input is operated on by said arithmetic unit and utilised as said output.

25. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 24 wherein said arithmetic unit includes a register to maintain a secret value and a value derived from said coordinate of said scalar multiple of the point represented by said other input is stored in said register to provide said secret value.

26. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 25 wherein said arithmetic unit utilises said secret value and said one input to obtain said coordinate of said scalar multiple of said point represented by said one input.

27. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 26 wherein said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and truncates said coordinate to provide said output.

28. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 26 wherein said arithmetic unit includes a one way function and said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and applies said one way function to said coordinate of said scalar multiple to obtain said output.

29. (currently amended) ~~An~~ The elliptic curve random number generator according to claim 28 wherein said arithmetic unit truncates said coordinate of said scalar multiple prior to applying said one way function.

30. (cancelled)

31. (cancelled)

32. (cancelled)

33. (cancelled)

34. (cancelled)

35. (cancelled)

36. (cancelled)

37. (new) The method according to claim 2 wherein both of said inputs are derived from outputs of respective hash functions.

38. (new) The method according to claim 37 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

39. (new) The method according to claim 38 wherein one of said scalar multiples of said points is used to derive said random number.

40. (new) The method according to claim 39 wherein said random number is derived by converting a coordinate of said one of said scalar multiples of said points to an integer and truncating the resultant value for use as said random number.

41. (new) The method according to claim 40 wherein said coordinate is an x coordinate.

42. (new) The method according to claim 39 wherein the other of said scalar multiples of said points is used to change said secret value for subsequent use.

43. (new) The method according to claim 42 wherein a coordinate of said other of said scalar multiples of said points is converted to an integer and used as a secret value.

44. (new) The method according to claim 43 wherein said coordinate is an x coordinate.

45. (new) The elliptic curve random number generator of claim 16 wherein each of said inputs includes a hash function.

46. (new) The elliptic curve random number generator of claim 16 including a secret value, and said arithmetic processor uses said secret value to compute scalar multiples of said points represented by said inputs.

47. (new) The elliptic curve random number generator according to claim 45 wherein one of said scalar multiples of said points is used to derive said random number.

48. (new) The elliptic curve random number generator according to claim 47 wherein said arithmetic processor converts a coordinate of said one of said scalar multiples of said points to an integer and truncates the resultant value, and outputs said truncated value for use as said random number.

49. (new) The elliptic curve random number generator according to claim 48 wherein said coordinate is an x coordinate.

50. (new) The elliptic curve random number generator according to claim 47 wherein the other of said scalar multiples of said points is used to change said secret value for subsequent use.

51. (new) The method according to claim 50 wherein a coordinate of said other of said scalar multiples of said points is converted to an integer and used as a secret value.

52. (new) The method according to claim 51 wherein said coordinate is an x coordinate.

53. (new) The method according to claim 1 wherein said first input is representative of a co-ordinate of an elliptic curve point.

54. (new) The method according to claim 53 wherein said first input is representative of an x coordinate of said elliptic curve point.

55. (new) The method according to claim 1 wherein said second input is representative of a coordinate of said other elliptic curve point.

56. (new) The method according to claim 55 wherein said second input is representative of an x coordinate of said other elliptic curve point.

57. (new) The method according to claim 1 wherein said first input is an elliptic curve point.

58. (new) The method according to claim 1 wherein said second input is said other elliptic curve point.

59. (new) The elliptic curve random number generator according to claim 15 wherein said first input is representative of a co-ordinate of an elliptic curve point.

60. (new) The elliptic curve random number generator according to claim 59 wherein said first input is representative of an x coordinate of said elliptic curve point.

61. (new) The elliptic curve random number generator according to claim 15 wherein said second input is representative of a coordinate of said other elliptic curve point.

62. (new) The elliptic curve random number generator according to claim 61 wherein said second input is representative of an x coordinate of said other elliptic curve point.

63. (new) The elliptic curve random number generator according to claim 15 wherein said first input is an elliptic curve point.

64. (new) The elliptic curve random number generator according to claim 15 wherein said second input is said other elliptic curve point.

65. (new) The elliptic curve random number generator according to claim 15 wherein said elliptic curve points are on the same elliptic curve.

66. (new) The method of claim 1 wherein said elliptic curve points are on the same elliptic curve.

67. (new) An elliptic curve random number generator comprising a first input representative of an elliptic curve point; a second input representative of another elliptic curve point; an arithmetic unit to perform elliptic curve operations on said inputs; and an output to receive the results of said elliptic operations, and a one way function to receive said output and produce a bit string for use as a random number.

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (previously presented) A method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of:

   obtaining a first input representative of an elliptic curve point,

   obtaining a second input representative of another elliptic curve point,

   each of said points being verifiably random;

   providing said first input and said second input as inputs to said arithmetic unit;

   performing selected elliptic curve operations on said inputs and obtaining an output; and

   utilising said output as a random number in the cryptographic operation.

2. (previously presented) The method according to claim 1 wherein at least one of said inputs is derived from an output of a hash function.

3. (previously presented) The method according to claim 2 wherein the other of said inputs is utilized as an input to said hash function.

4. (previously presented) The method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

5. (previously presented) The method according to claim 4 wherein one of said scalar multiples is used to derive said random number and the other of said scalar multiples is used to change said secret value for subsequent use.

6. (previously presented) The method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input.

7. (previously presented) The method according to claim 6 wherein another coordinate of said point is obtained from said one coordinate for inclusion as said one input.

8. (cancelled).

9. (previously presented) The method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by

said scalar multiple and truncating said coordinate to a bit string for use as said random number.

10. (previously presented) The method according to claim 9 wherein said one coordinate is truncated in the order of one half the length of a representation of an elliptic curve point representation.

11. (previously presented) The method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and hashing said one coordinate to provide a bit string for use as said random number.

12. (cancelled).

13. (currently amended) A method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation, said method comprising the steps of:

obtaining a first input representative of an elliptic curve point;

obtaining a second input representative of another elliptic curve point;

performing elliptic curve operations on said inputs to obtain an output representative of a ~~sca3lar~~ scalar multiple of an elliptic curve point;

passing said output through a one way function to obtain a bit string for use as a random number; and

utilising said random number in the cryptographic operation.

14. (previously presented) The method according to claim 13 wherein said one way function is a hash function.

15. (previously presented) An elliptic curve random number generator comprising a first input representative of an elliptic curve point; a second input representative of another elliptic curve point, each of said points being verifiably random; an arithmetic unit to perform elliptic curve operations on said inputs; and an output to receive the results of said elliptic curve operations, said output representing a random number for use in a cryptographic operation.

16. (previously presented) The elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function.

17. (previously presented) The elliptic curve random number generator according to claim 16 wherein said one way function is a hash function.

18. (previously presented) The elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function.

19. (cancelled)

20. (previously presented) The method according to claim 5 wherein said secret value is derived from a coordinate of said other scalar multiple.

21. (previously presented) The method according to claim 20 wherein an x coordinate of said other scalar multiple is used to change said secret value.

22. (previously presented) The elliptic curve random number generator according to claim 15 wherein said arithmetic unit operates on said inputs to obtain a scalar multiple of a coordinate of a point represented by said one input.

23. (previously presented) The elliptic curve random number generator according to claim 22 ~~23~~ wherein said arithmetic unit computes a coordinate of a scalar multiple of each of said points represented by said inputs.

24. (previously presented) The elliptic curve random number generator according to claim 23 wherein said coordinate of said scalar multiple of said point represented by said one input is operated on by said arithmetic unit and utilised as said output.

25. (previously presented) The elliptic curve random number generator according to claim 24 wherein said arithmetic unit includes a register to maintain a secret value and a value derived from said coordinate of said scalar multiple of the point represented by said other input is stored in said register to provide said secret value.

26. (previously presented) The elliptic curve random number generator according to claim 25 wherein said arithmetic unit utilises said secret value and said one input to obtain said coordinate of said scalar multiple of said point represented by said one input.

27. (previously presented) The elliptic curve random number generator according to claim 26 wherein said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and truncates said coordinate to provide said output.

28. (previously presented) The elliptic curve random number generator according to claim 26 wherein said arithmetic unit includes a one way function and said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and applies said one way function to said coordinate of said scalar multiple to obtain said output.

29. (previously presented) The elliptic curve random number generator according to claim 28 wherein said arithmetic unit truncates said coordinate of said scalar multiple prior to applying said one way function.

30. (cancelled)

31. (cancelled)

32. (cancelled)

33. (cancelled)

34. (cancelled)

35. (cancelled)

36. (cancelled)

37. (previously presented) The method according to claim 2 wherein both of said inputs are derived from outputs of respective hash functions.

38. (previously presented) The method according to claim 37 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

39. (previously presented) The method according to claim 38 wherein one of said scalar multiples of said points is used to derive said random number.

40. (previously presented) The method according to claim 39 wherein said random number is derived by converting a coordinate of said one of said scalar multiples of said points to an integer and truncating the resultant value for use as said random number.

41. (previously presented) The method according to claim 40 wherein said coordinate is an x coordinate.

42. (previously presented) The method according to claim 39 wherein the other of said scalar multiples of said points is used to change said secret value for subsequent use.

43. (previously presented) The method according to claim 42 wherein a coordinate of said other of said scalar multiples of said points is converted to an integer and used as a secret value.

44. (previously presented) The method according to claim 43 wherein said coordinate is an x coordinate.

45. (previously presented) The elliptic curve random number generator of claim 16 wherein each of said inputs includes a hash function.

46. (previously presented) The elliptic curve random number generator of claim 16 including a secret value, and said arithmetic processor uses said secret value to compute scalar multiples of said points represented by said inputs.

47. (previously presented) The elliptic curve random number generator according to claim 45 wherein one of said scalar multiples of said points is used to derive said random number.

48. (previously presented) The elliptic curve random number generator according to claim 47 wherein said arithmetic processor converts a coordinate of said one of said scalar multiples of said points to an integer and truncates the resultant value, and outputs said truncated value for use as said random number.

49. (previously presented) The elliptic curve random number generator according to claim 48 wherein said coordinate is an x coordinate.

50. (previously presented) The elliptic curve random number generator according to claim 47 wherein the other of said scalar multiples of said points is used to change said secret value for subsequent use.

51. (previously presented) The method according to claim 50 wherein a coordinate of said other of said scalar multiples of said points is converted to an integer and used as a secret value.

52. (previously presented) The method according to claim 51 wherein said coordinate is an x coordinate.

53. (previously presented) The method according to claim 1 wherein said first input is representative of a co-ordinate of an elliptic curve point.

54. (previously presented) The method according to claim 53 wherein said first input is representative of an x coordinate of said elliptic curve point.

55. (previously presented) The method according to claim 1 wherein said second input is representative of a coordinate of said other elliptic curve point.

56. (previously presented) The method according to claim 55 wherein said second input is representative of an x coordinate of said other elliptic curve point.

57. (previously presented) The method according to claim 1 wherein said first input is an elliptic curve point.

58. (previously presented) The method according to claim 1 wherein said second input is said other elliptic curve point.

59. (previously presented) The elliptic curve random number generator according to claim 15 wherein said first input is representative of a co-ordinate of an elliptic curve point.

60. (previously presented) The elliptic curve random number generator according to claim 59 wherein said first input is representative of an x coordinate of said elliptic curve point.

61. (previously presented) The elliptic curve random number generator according to claim 15 wherein said second input is representative of a coordinate of said other elliptic curve point.

62. (previously presented) The elliptic curve random number generator according to claim 61 wherein said second input is representative of an x coordinate of said other elliptic curve point.

63. (previously presented) The elliptic curve random number generator according to claim 15 wherein said first input is an elliptic curve point.

64. (previously presented) The elliptic curve random number generator according to claim 15 wherein said second input is said other elliptic curve point.

65. (previously presented) The elliptic curve random number generator according to claim 15 wherein said elliptic curve points are on the same elliptic curve.

66. (previously presented) The method of claim 1 wherein said elliptic curve points are on the same elliptic curve.

67. (previously presented) An elliptic curve random number generator comprising a first input representative of an elliptic curve point; a second input representative of another elliptic curve point; an arithmetic unit to perform elliptic curve operations on said inputs; and an output to receive the results of said elliptic operations, and a one way function to receive said output and produce a bit string for use as a random number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

91704 7590 04/15/2011

Blake, Cassels & Graydon LLP
199 BAY STREET , SUITE 2800
COMMERCE COURT WEST
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
LAKHIA, VIRAL S	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/15/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

rimpatent@blakes.com
brett.slaney@blakes.com
portfolioprosecution@rim.com

Office Action Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL S. LAKHIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 February 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-11,13-18,20-29 and 37-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-11,13-18,20-29 and 37-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 2/24/2011.

Response to Amendment

Claims 1 – 7, 9 – 11, 13 - 18, 20—29, 37 - 67 are examined.

Cancelled claims - 8, 12, 19, 30 – 36.

Continued Examination under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/24/2011 has been entered.

Response to Arguments

Applicant's arguments filed 2/24/2011 with respect to claims 1 – 18, 20—29, 37 – 67 have been considered have been considered and are persuasive. However the applicant's arguments are moot in view of new ground(s) of rejection.

Examiner would like to point out that there are two different set of claims submitted on 2/24/2011. As it might be an error, examiner has examined the claim set of 1 – 7, 9 – 11, 13 - 18, 20—29, 37 – 67.

For the purpose of this office action, examiner would further like to point out that, as applicant's argument regarding with respect to Claim 1, it's unclear what Applicant's intended metes and bounds of the claim are, since the claim appears to cover anything and everything that does not prohibit "... obtaining first and second pair of inputs of an elliptical curve point to ensure that one point would not have been chosen as a known multiple ..", as a core principle of elliptical curve where y2 = x3 + ax + b there is a fundamental principle where points x and y are related through a elliptical equation although one of the points can be random on the elliptical curve the scalar multiple or known multiple is shared between any two points on elliptical curve. As the applicant has amended the claims with two inputs where the said inputs are not to share a known multiple of others is against the fundamental principle of elliptical curve since the two points will share a common equation relating the two points on the curve. Although para 0037 describes the limitation, it does not describe on how the limitation of two random points as input without having common multiple will be achieved. Examiner would like to request for clear description of the point as mentioned above.

Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims, for example independent claim 1 is amended, yet distinct description of "separate" components on how the components are

different is not described in the specification. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The examiner has addressed the newly added claim limitations in the rejection of the claims below.

Any objections or rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 – 12, 15 - 18, 20—29, 37 - 67 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, with respect to Claim 1, it's unclear what Applicant's intended metes and bounds of the claim are, since the claim appears to cover anything and everything that does not prohibit "... obtaining first and second pair of inputs of an elliptical curve point to ensure that one point would not have been chosen as a known multiple .." from occurring. The Examiner notes that usage of claim language such as "obtaining" requires mathematical steps pertaining to choice of elliptical curve within a particular finite field such that points selected to generate random number belong the specific elliptical curve, as such the mathematical step of obtaining the two input is missing in the claim language. The Examiner therefore suggests selecting two inputs selection which is tied to a specific

elliptical curve. Thus, claim 1 is indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 15 is rejected under a similar rationale.

The dependent claims included in the statement of rejection but not specifically addressed in the body of the rejection have inherited the deficiencies of their parent claim and have not resolved the deficiencies. Therefore, they are rejected based on the same rationale as applied to their parent claims above.

Further examiner would like to request distinct description of ".. performing selected elliptical curve operations or mathematical functions to obtain an output... “for example calculation of escrow key e in fig 8 or Fig 4 – generate and truncate the random number this distinct description of "mathematical functions” will clarify the boundary of claim 1.

Claims 2 and 3 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, with respect to Claims 2 and 3 are contradicting in matter, it’s unclear what Applicant’s intended boundary of claimed limitations are, for example, claim 1 covers two inputs of elliptical curve to generate random number, claim 2 covers one of the input obtained from a hash function, and claim 3 covers one of the said inputs as an input to hash function. The claim tree of claims 1, 2, and 3 in summary covers, two inputs required to generate a random number yet claims 2 and 3 are claiming derivation of hash from one of the input, yet derivation of hash is ambiguous to examiner since in claim 2 the input is obtained from

an output of hash function and claim 3, the input is utilized as an input to hashed function. The Examiner therefore suggests clarifying the clear state of two inputs for generating random number and clear definition of input and output of hash function related to one of the input value. Further in view of broad interpretation of “hash function”, the relation of “hash function” to elliptical curve calculation and random number generation should be clearly described or “hash function" can exist in overall system without relation to ECC and random number generation. Thus, the claim is indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Appropriate actions are required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 – 14, 20—21, 37 – 44, 51-58, 66 recite a “... method of operating an elliptical curve random number generator ... compute a random number generator ... to said arithmetic unit .. " under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of *In Re Bilski* 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps and therefore do not qualify as a statutory process. Since the step of computing the random

number by two inputs on behalf of system or user could be done in paper or by mental step.

Claims 15-18, 22-29, 45-50, 59-65, 67 and other dependent claims recite, " .. ECRNG (elliptical curve random number generator) which calculates random curve points as input to produce secure random number", however this step covers software per say, which is non-statutory subject matter as explained further. It is a not clear in specification or independent claims if ECRNG is software or hardware or combination of both. Therefore in broad view of independent claims examiner presumes the claims are software per say. Consequently only software based elliptical curve calculation system for producing secure random number seed is non – statutory.

The dependent claims included in the statement of rejection but not specifically addressed in the body of the rejection have inherited the deficiencies of their parent claim and have not resolved the deficiencies. Therefore, they are rejected based on the same rationale as applied to their parent claims above.

Claim Rejections - 35 USC § 102

The following is a quotation of 35 U.S.C. 102(e) which forms the basis for all obviousness rejections set forth in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 – 4, 6, 13 – 17, 37 – 39, 45 - 47 are rejected under 35 U.S.C. 102(e) as being U.S. Publication 2006/0129800 to Lauter et al. (hereinafter known as "Lauter").

As per claim 1 Lauter teaches, a method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to: compute a random number for use in a cryptographic operation *(Lauter – Fig 1, 2, 3 and 4 – element 310 para 0030 – 0031 where generation of respective secret random number r between random points on elliptical curve covers limitation)*, said method comprising the steps of:

obtaining a first input representative of an elliptic curve point *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033)*,

obtaining a second input representative of another elliptic curve point *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033 – Examiner would like to point that two points or multiple points on elliptical curve is well known in the art at the time of invention)*,

each of said points being verifiably random *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033)*;

providing said first input and said second input as input to said arithmetic unit *(Lauter – Fig 1 and 3 – para 0029 – 0033)*;

performing selected elliptic curve operations on said inputs, and obtaining an output *(Lauter –Fig 1, 2, 3 and 4 – para 0029 – 0033)*; and

utilizing said output as a random number in the cryptographic operation *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033)*.

Further examiner presumes for the purpose of this office action that cassels - tate pairings in Fig 1, para 0012 - similar to Weils pairing reads on multiple points (p,q) of the elliptical curve over a finite field with different properties like multiplicative and divisive properties over the finite field as known in the art at the time of invention. Additionally, Lauter and other cited reference have an inherent and well known functionality of scalar multiplier of various points on ECC, x-coordinate value of points on ECC over finite fields, secret value in accordance with scalar multiplier are well known in the art and within the domain of cited references.

As per claim 2 Lauter teaches, the method according to claim 1 wherein said at least one of said inputs is derived from an output of a hash function *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055 - Fig 3 – element 314 where hash of M, h(M) is computed covers the limitation, Fig 4 – element 414)*.

As per claim 3 Lauter teaches, the method according to claim 2 wherein the other of said inputs is utilized as an input to said hash function *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055 – Fig 3 – element 314 where hash of M, h(M) is computed covers the limitation, Fig 4 – element 414)*.

As per claim 4 Lauter teaches, the method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs *(Lauter – Fig 1 and 3 – para 0029 – 0033)*.

As per claim 6 Lauter teaches, the method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055 , Fig 4 – element 414)*.

As per claim 13 Lauter teaches, a method of operating an elliptic curve random number generator including an arithmetic unit to perform elliptic curve operations to compute a random number for use in a cryptographic operation *(Lauter – Fig 1 and 3 – para 0029 – 0033)*, said method comprising the steps of:

obtaining a first input pair of inputs, each representative of an elliptic curve points, to said arithmetic unit *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055)*;

obtaining a second input representative of another elliptic curve point *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055)*;

performing elliptic curve operations on said inputs to obtain an output representative of coordinate of a scalar multiple of an elliptic curve point *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055)*;

passing said output through a one way function to obtain a bit string for use as a random number *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055*; and

utilizing said random number in the cryptographic operation *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055)*.

As per claim 14 Lauter teaches the method according to claim 13 wherein said one way function is a hash function *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 – 0055, Fig 4 – element 414)*.

As per claim 15 Lauter teaches an elliptic curve random number generator comprising a first input pair representative of at least of an elliptic curve points *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 - 0055)*;

a second input representative of another elliptic curve point, each of said points being verifiably random *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 - 0055)*;

an arithmetic unit to perform elliptic curve operations on said inputs *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 - 0055)*;

and an output to receive the results of said elliptic curve operations *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 - 0055)*,

said output representing a random number for use in a cryptographic operation *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 - 0055)*.

As per claim 16 Lauter teaches the elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function *(Lauter – Fig 1, 2 and 3 – para 0029 – 0033 and 0053 – 0055 – Fig 4 – element 414)*.

As per claim 17 Lauter teaches the elliptic curve random number generator according to claim 16 wherein said one way function is a hash function *(Lauter – Fig 1,2 and 3 – para 0029 – 0033 and 0053 – 00, 55, Fig 4 – element 414)*.

As per claim 37 Lauter teaches the method according to claim 2 wherein both of said inputs are derived from outputs of respective hash functions *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033 and 0053 – 0055 – Fig 4 – element 414).*

As per claim 38 Lauter teaches the method according to claim 37 wherein said random number generator has a secret value and said secret value is 'used to compute scalar multiples of said points represented by said inputs *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033 and 0053 – 0055).*

As per claim 39 Lauter teaches the method according to claim 38 wherein one of said scalar multiples of said points is used to derive said random number *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033 and 0053 – 0055).*

As per claim 67 Lauter teaches an elliptic curve random number generator comprising

a first input representative of an elliptic curve point *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033 and 0053 – 0055)*;

a second input representative of another elliptic curve point *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033 and 0053 – 0055)*;

an arithmetic unit to perform elliptic curve operations on said inputs *(Lauter – Fig 1, 2, 3 and 4 para 0029 – 0033 and 0053 – 0055)*;

and an output to receive the results of said elliptic operations *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033 and 0053 – 0055)*,

and a one way function to receive said output and produce a bit string for use as a random number *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033 and 0053 – 0055)*.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5, 7, 9, 27 – 29, 40 - 67 are rejected under 35 U.S.C. 103(a) as being U.S. Publication 2006/0129800 to Lauter et al. (hereinafter known as "Lauter") and in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant").

As per claim 5 Lauter teaches, the method according to claim 4 wherein one of said scalar multiples is used to derive said random number *(Lauter – Fig 1 and 3 – para*

0029 – 0033) and the other of said scalar multiples is used to change said secret value for subsequent use.

Lauter does not teach however Gallant teaches, wherein one of said scalar multiples is used to derive said random number *(Gallant para 0054 – 0055).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter by accelerating multiplication of an elliptical curve point by a scalar over a finite field. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

As per claim 7 combination of Lauter – Gallant teaches, the method of claim 6.

Lauter does not teach, however Gallant teaches wherein another coordinate of said point is obtained from said one coordinate for inclusion as said one input *(Gallant Fig 2 and 3 para 0039 – 0044).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter by accelerating multiplication of an elliptical curve point by a scalar over a finite field. This would have been obvious because the ordinary

person skilled in the art at the time of invention would have been motivated to create an efficient operation of accelerating multiplication of an elliptical curve point.

As per claim 9 combination of Lauter – Gallant, the method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by, said scalar multiple *(Lauter – Fig 1 and 3 – para 0029 – 0033 and 0053 - 0055)* and truncating said Coordinate to a bit string for use as said random number.

Lauter does not teach however Gallant teaches, truncating said coordinate to a bit string for use as said random number.

However Gallant teaches truncating said coordinate to a bit string for use as said random number *(Gallant – para 0054 and 0068).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of combination of Lauter by decreasing the bit-length to use as random number. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of random number generation system.

As per claim 27 combination of Lauter – Gallant teaches, an elliptic curve random number generator wherein said arithmetic unit combines said secret value and

said one input to generate said coordinate of said scalar multiple *(Lauter Fig 1, 2 and 3 para 0039 – 0044 and para 0029 – 0033 and 0053 - 0055).*

Gallant teaches truncating said coordinate to provide said output *(Gallant – para 0054 and 0068).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter by decreasing the bit-length to use as random number. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of random number generation system.

As per claim 28 combination of Lauter – Gallant teaches, an elliptic curve random number generator according to claim 26 wherein said arithmetic unit includes a one way function and said arithmetic unit combines said secret value and said one input to generate said coordinate of said scalar multiple and applies said one way function to said coordinate of said scalar multiple to obtain said output *(Lauter Fig 1, 2 and 3 para 0039 – 0044 and para 0029 – 0033 and 0053 - 0055).*

As per claim 29 combination of Lauter – Gallant teaches, an elliptic curve random number generator.

Gallant teaches wherein said arithmetic unit truncates said coordinate of said scalar multiple prior to applying said one way function.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of combination of Lauter by decreasing the bit-length to use as random number. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of random number generation system.

As per claim 40 combination of Lauter – Gallant teaches, the method according to claim 39. wherein said random number is derived by converting a coordinate of said one of said scalar multiples of said points to an integer *(Lauter Fig 1, 2 and 3 para 0039 – 0044 and para 0029 – 0033 and 0053 - 0055).*

Lauter does not teach however Gallant teaches, truncating said coordinate to a bit string for use as said random number *(Gallant – para 0054 and 0068).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter by decreasing the bit-length to use as random number. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of random number generation system.

As per claim 41 combination of Lauter – Gallant teaches, the method according to claim 40 wherein said coordinate is an x coordinate *(Lauter Fig 1, 2 and 3 para 0039*

– 0044 and para 0029 – 0033 and 0053 – 0055, further x – coordinate value within ECC is inherent function of Elliptical curve cryptography).

As per claim 42,

Claim 42 is a claim of a method for said scalar multiples of said points is used to change said secret value for subsequent use in accordance with method of claim 5.

As per claim 43,

Claim 43 is a claim of a method for a coordinate of said other of: said scalar multiples of said points is converted to an integer and used as a secret value in accordance with method of claim 20 *(where value being an integer is an inherent function of cited ECC with random number generator and signature verification).*

As per claim 44,

Claim 44 is a claim of a method for a coordinate of said other of: said coordinate is an x coordinate in accordance with method of claim 41.

As per claim 45,

Claim 45 is a claim of an elliptic curve random number, generator of claim 16 wherein each of said inputs includes a hash function in accordance with method of claim 2.

As per claim 46,

Claim 46 is a claim of a method for elliptic curve random number generator of claim 16 including a secret value, and said arithmetic processor uses said secret value to compute scalar multiples of said points represented by said inputs in accordance with method of claim 38.

As per claim 47,

Claim 47 is a claim of a elliptic curve random number generator according to claim 45 wherein one of said scalar multiples of said points is used to derive said random number in accordance with method of claim 39.

As per claim 48,

Claim 48 is a claim of the elliptic curve random number ,generator according to claim 47 wherein said arithmetic processor converts a coordinate of said one of said scalar multiples of said points to an integer and truncates the resultant value, and outputs said truncated value for use as said random number, in accordance with method of claim 40.

As per claim 49,

Claim 49 is a claim of the elliptic curve random number generator according to claim 48 wherein said coordinate is an x coordinate in accordance with method of claim 40.

As per claim 50,

Claim 50 is a claim of the elliptic curve random number generator according to claim 47 wherein the other of said scalar multiples of said points is used to change said secret value for subsequent use in accordance with method of claim 40.

As per claim 51,

Claim 50 is a claim of the method according to a coordinate of said other of said scalar multiples of said points is converted to an integer and used as a secret value in accordance with method of claim 40.

As per claim 52,

Claim 52 is a claim of the method according to claim 51 wherein said coordinate is an x coordinate in accordance with method of claim 44.

As per claim 53,

Claim 53 is a claim of the method according to claim 1 wherein said first input is representative of a coordinate of an elliptic curve point in accordance with method of claim 44.

As per claim 54,

Claim 54 is a claim of the method according to claim 53 wherein said first input is representative of an x coordinate of said elliptic curve point in accordance with method of claim 8 and 40 and further that x-coordinate input value is an inherent property of ECC in cited reference.

As per claim 55,

Claim 55 is a claim of the method according to claim 1 wherein said second input is representative of a coordinate of said other elliptic curve point in accordance with method of claim 44.

As per claim 56,

Claim 56 is a claim of the method according to wherein said second input is representative of an x coordinate of said other elliptic curve point in accordance with method of claim 8 and 40 and further that x-coordinate input value is an inherent property of ECC in cited references.

As per claim 57,

Claim 57 is a claim of the method according to claim 1 wherein said first input is an elliptic curve point in accordance with method of claim 44.

As per claim 58,

Claim 58 is a claim of the method according to claim 1 wherein said second input is said other elliptic curve point in accordance with method of claim 44.

As per claim 59,

Claim 59 is a claim of the elliptic curve random number generator according to claim 15 wherein said first input is representative of a co-ordinate of an elliptic curve point in accordance with method of claim 44.

As per claim 60,

Claim 60 is a claim of the elliptic curve random number .generator according to claim 59 wherein said first input is representative of an x coordinate of said elliptic curve point in

accordance with method of claim 8 and 40 and further that x-coordinate input value is an inherent property of ECC in cited reference.

As per claim 61,

Claim 61 is a claim of the elliptic curve random number ,generator according to claim15 wherein said second input is representative of a coordinate of said other elliptic curve point in accordance with method of claim 44.

As per claim 62,

Claim 62 is a claim of the elliptic curve random number ,generator according to claim 61 wherein said second input is representative of an x coordinate of said other elliptic curve point in accordance with method of claim 8 and 40 and further that x-coordinate input value is an inherent property of ECC in cited reference.

As per claim 63,

Claim 63 is a claim of the elliptic curve random number ,generator according to claim 15 wherein said first input is an elliptic curve point in accordance with method of claim 44.

As per claim 64,

Claim 64 is a claim of the elliptic curve random number generator according to claim 15 wherein said second input is said other elliptic curve point in accordance with method of claim 44.

As per claim 65,

Claim 65 is a claim of the elliptic curve random number generator according to claim 15 wherein said elliptic curve points are on the same elliptic curve in accordance with method of claim 44.

As per claim 66,

Claim 66 is a claim of the method of claim 1 wherein said elliptic curve points are on the same elliptic curve in accordance with method of claim 44.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Publication 2006/0129800 to Lauter et al. (hereinafter known as "Lauter") and in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant") and further in view of U.S. Publication 2005/0251680 to Brown et al. (hereinafter "Brown").

As per claim 10 Lauter – Gallant teach a method wherein said one coordinate is truncated.

Lauter – Gallant do not teach, however Brown teaches wherein the order of one half the length of a representation of an elliptic curve point representation *(Brown para 0204)*.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Brown in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter - Gallant by calculation reducing abscissa value of x and

y – coordinate. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create an efficient operation of accelerating multiplication of an elliptical curve point.

Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Publication 2006/0129800 to Lauter et al. (hereinafter known as "Lauter") and in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant") and further in view of U.S. Patent 6,044,388 to DeBellis et al. (hereinafter "DeBellis").

As per claim 11 Lauter and Gallant teach a method wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple *(Gallant para 0054 – 0055 and as explained in claim 5).*

Lauter and Gallant do not teach hashing said one coordinate to provide a bit string for use as said random number.

However DeBellis teaches hashing said one coordinate to provide a bit string for use as said random number *(DeBellis Fig 1 and 2 col 7 – lines 30 - 40).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of DeBellis in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter and Gallant by hashing point coordinate of an elliptical curve point. This would have been obvious because the ordinary person skilled in the

art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

Claims 20 - 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Publication 2006/0129800 to Lauter et al. (hereinafter known as "Lauter") and in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant") and further in view of U.S. Patent 6,738,478 to Vanstone et al. (hereinafter "Vanstone").

As per claim 20 Lauter – Gallant teach a method according to claim 5. Lauter – Gallant does not teach wherein said secret value is derived from a coordinate of said other scalar multiple.

However Vanstone teaches where said secret value is derived from a coordinate of said other scalar multiple (Vanstone Fig 2 - col 3 – lines 30 – 42).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Vanstone in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter – Gallant by establishing an algorithm where scalar (k) is a private vector or secret value. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to minimizing the risk of successful timing attack by constantly changing value of scalar multiple and private key operations.

As per claim 21 Lauter – Gallant teach elliptical curve random number generation. Lauter and Gallant do not teach a method wherein the x coordinates of said other scalar multiple is used to change said secret value.

However Vanstone teaches wherein the x coordinates of said other scalar multiple is used to change said secret value *(Vanstone Fig 2, col 3 – lines 42 – 67).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Vanstone in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter – Gallant by incorporating Montgomery method to derive x – coordinate of an ordered pair to change secret value. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to initialize a unique method to generate unique power signatures by involving multiple operations by changing scalar – secret value.

As per claim 22 combination of Lauter – Gallant – Vanstone teaches, the elliptic curve random number generator, according :to claim 15 wherein said arithmetic unit operates on said inputs to obtain a scalar multiple of a coordinate of a point represented by said one input *(Lauter Fig 1, 2 and 3 para 0039 – 0044 and para 0029 – 0033 and 0053 – 0055 and Fig 4).*

As per claim 23 combination of Lauter – Gallant – Vanstone teaches, 23. (currently amended) A~ The elliptic curve random number generator according to claim 2_22 2~3 wherein said arithmetic unit computes a coordinate of a scalar multiple of

each of said points represented by said inputs *(Lauter Fig 1, 2 and 3 para 0039 – 0044 and para 0029 – 0033 and 0053 – 0055 and Fig 4).*

As per claim 24 combination of Lauter – Gallant – Vanstone teaches, the elliptic curve random number generator according to claim 23 wherein said coordinate of said scalar multiple of said point represented by, said one input is operated on by said arithmetic unit and utilized as said output *(Lauter Fig 1, 2 and 3 para 0039 – 0044 and para 0029 – 0033 and 0053 – 0055 and Fig 4).*

As per claim 25 combination of Lauter – Gallant – Vanstone teaches, the elliptic curve random number generator according to claim 24 wherein said arithmetic unit includes a register to maintain a secret value and a value derived from said coordinate of said scalar multiple of the point represented by said other input is stored in said register to provide said secret value *(Lauter Fig 1, 2 and 3 para 0039 – 0044 and para 0029 – 0033 and 0053 – 0055 and Fig 4).*

As per claim 26 combination of Lauter – Gallant – Vanstone teaches, the elliptic curve random number generator according to claim 25 wherein said arithmetic unit utilizes said secret value and said one input to obtain said coordinate of said scalar multiple of said point represented by said one input *(Lauter Fig 1, 2 and 3 para 0039 – 0044 and para 0029 – 0033 and 0053 – 0055 and Fig 4).*

Examiner's Notes

Examiner has cited particular paragraphs and/or columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested of the applicant, in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viral Lakhia whose telephone number is (571) 270 - 3363. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Viral S Lakhia/

Examiner, Art Unit 2431

/NATHAN FLYNN/

Supervisory Patent Examiner, Art Unit 2468

Notice of References Cited	Application/Control No. 11/336,814	Applicant(s)/Patent Under Reexamination BROWN ET AL.	
	Examiner VIRAL S. LAKHIA	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0129800	06-2006	Lauter et al.	713/151
*	B	US-7,680,270	03-2010	Srungaram, Gopala Krishna Murthy	380/30
*	C	US-2005/0036609	02-2005	Eisentraeger et al.	380/030
*	D	US-7,062,043	06-2006	Solinas, Jerome A.	380/30
*	E	US-6,424,712	07-2002	Vanstone et al.	380/28
*	F	US-7,062,044	06-2006	Solinas, Jerome A.	380/30
*	G	US-7,013,047	03-2006	Schmidt et al.	382/199
*	H	US-6,263,081	07-2001	Miyaji et al.	380/28
*	I	US-6,882,958	04-2005	Schmidt et al.	702/179
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	Art Unit
	VIRAL LAKHIA	4144

SEARCHED

Class	Subclass	Date	Examiner
380	28-30	6/17/09	V.L.
380	44-47	6/17/09	V.L.
380	277-286	6/17/09	V.L.
713	Search 713 with key word search of elliptic curve number generator	6/17/09	V.L.
726	Search 726 with key word search of elliptic curve number generator	6/17/09	V.L.
380	28-30	4.5.2011	V.L.

SEARCH NOTES

Search Notes	Date	Examiner
Key words and combination : elliptic curve number generator (creator, producer, intiator), message, digest, hash, random	7/17/09	V.L.
Get assistance with Fast and Focused Search department for the case	7/17/09	V.L
Get assistance from Peter Poltriak for claim interpretation and understanding of invention	7/17/09	V.L
Search Google Patents, NPL and wikipedia for elliptic curve technology	7/17/09	V.L
Update East with key word search	7/15/2010	V.L.
Update East with key word search.	4.6.2011	V.L.
Search INventor name for double patent issues.	4.6.2011	V.L.

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/V. S. L./ Examiner.Art Unit 2431	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	4144

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011				
	1	✓		÷		✓				
	2	✓		÷		✓				
	3	✓		÷		✓				
	4	✓		÷	✓	✓				
	5	✓		÷	✓	✓				
	6	✓		÷	✓	✓				
	7	✓		÷	✓	✓				
	8	✓		÷	✓	-				
	9	✓		÷	✓	✓				
	10	✓		÷	✓	✓				
	11	✓		÷	✓	✓				
	12	✓		÷	✓	-				
	13	✓		÷	✓	✓				
	14	✓		÷	✓	✓				
	15	✓		÷	✓	✓				
	16	✓		÷	✓	✓				
	17	✓		÷	✓	✓				
	18	✓		÷	✓	✓				
	19		✓	÷	-	-				
	20			÷	✓	✓				
	21			÷	✓	✓				
	22			÷	✓	✓				
	23			÷	✓	✓				
	24			÷	✓	✓				
	25			÷	✓	✓				
	26			÷	✓	✓				
	27			÷	✓	✓				
	28			÷	✓	✓				
	29			÷	✓	✓				
	30			÷	-	-				
	31			÷	-	-				
	32			÷	-	-				
	33			÷	-	-				
	34			÷	-	-				
	35			÷	-	-				
	36			÷	-	-				

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	4144

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011				
	37					✓				
	38					✓				
	39					✓				
	40					✓				
	41					✓				
	42					✓				
	43					✓				
	44					✓				
	45					✓				
	46					✓				
	47					✓				
	48					✓				
	49					✓				
	50					✓				
	51					✓				
	52					✓				
	53					✓				
	54					✓				
	55					✓				
	56					✓				
	57					✓				
	58					✓				
	59					✓				
	60					✓				
	61					✓				
	62					✓				
	63					✓				
	64					✓				
	65					✓				
	66					✓				
	67					✓				

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L11	0	7 and 10	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	AND	ON	2011/04/07 10:58
L10	4	(first second input pair$2 multiple random cryptographic elliptic curve).clm.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	AND	ON	2011/04/07 10:58
L9	13	7 and 8	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	AND	ON	2011/04/07 10:57
L8	901	(first second input pair$2 multiple random cryptographic elliptic curve)	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	AND	ON	2011/04/07 10:57
L7	691	(DANIEL NEAR2 BROWN).IN.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/07 10:56
L5	5	(random with generato $4) with ("oneway" one with way) same ("ECC" elliptical near3 curve)	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/07 08:00
L4	864	(random with generato $4) with ("oneway" one with way)	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/07 07:59
L1	0	(random near2 genearto $4) with (one near2 way)	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/07 07:58
S45	11	(two) with (point$2) with (random with generat$4) same (ECC elliptical curve) and (scalar) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/06 22:37
S44	5	(scott near3 vanstone$2) and (elliptical near2 curve) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/06 07:44

S43	8	(scott near3 vanstone$2) and (elliptical near2 curve)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/06 07:44
S42	409	(scott near3 vanstone$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/06 07:43
S41	2	"20070189527"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 13:30
S40	3	"11336814"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 13:03
S39	2	"7062043".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 13:03
S38	5	(two) with (point$2) with (random with generat$4) and (ECC elliptical curve) and (escrow hash$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:45
S37	2	"7103772".pn.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:45
S36	5	(two) with (point$2) with (random with generat$4) and (ECC elliptical curve) and (escrow hash$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:43
S35	0	(two) with (point$2) with (random with generat$4) same (ECC elliptical curve) and (escrow hash $3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:43

S34	0	(two) with (point$2) with (random with generat$4) same (ECC elliptical curve) same (hash$4) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:42
S33	20	(two) with (point$2) with (random with generat$4) same (ECC elliptical curve) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:41
S32	214	(point$2) with (random with generat$4) same (ECC elliptical curve) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:41
S31	370	(point$2) with (random with generat$4) same (ECC elliptical curve)	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:41
S30	2	"7853013".pn.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:36
S29	1	((two dual many plural) with (input$2 point$2)) with (random with generat $4) and (escrow seed) and ("ECC" (elliptical with curve)) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:35
S28	2	"7680270".pn.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:22
S27	7	(pseudo with random with number) and (signature $2) and (siemens).as.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:08
S26	23	(pseudo with random with number) and (signature $2) and (siemens)	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:08
S25	112	(pseudo with random with number) and (siemens)	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:07
S24	2	"20040102242"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 10:54

S23	1	((two dual many plural) with (input$2 point$2)) with (random with generat $4) and (hash$3) and ("ECC" (elliptical with curve)) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 10:24
S22	0	((two dual many plural) with (input$2 point$2)) with (random with generat $4) same (hash$3) and ("ECC" (elliptical with curve)) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 10:23
S20	26	((two dual many plural) with (input$2 point$2)) with (random with generat $4) and ("ECC" (elliptical with curve)) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 10:23
S19	770	((two dual many plural) with (input$2 point$2)) and (random with generat $4) and ("ECC" (elliptical with curve)) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 10:23
S18	6501	((two dual many plural) with (input$2 point$2)) and ("ECC" (elliptical with curve)) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 10:22
S17	12	(random with number with generator) same ((two dual many plural) with (input$2 point$2)) and ("ECC" (elliptical with curve)) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 09:29
S15	19	(random with number with generator) same ((two dual many plural) with (input$2 point$2)) and ("ECC" (elliptical with curve))	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 09:26
S14	938	(random with number with generator) same ((two dual many plural) with (input$2 point$2))	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 09:25

S13	983	(random with number with generator) same ((two dual many plural) with (input$2 point$2))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 09:25
S12	1	((elliptical with curve with random with number with generator) ("ECRNG")) same ((two dual many plural) with (input$2 point $2))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 09:24
S11	12	(elliptical with curve with random with number with generator) ("ECRNG") same ((two dual many plural) with (input$2 point $2))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 09:24
S10	12	(elliptical with curve with random with number with generator) ("ECRNG")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 09:23
S9	11	(elliptical with curve with random with number with generator)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 09:23

EAST Search History (Interference)

<This search history is empty>

4/7/2011 10:58:47 AM
C:\Documents and Settings\vlakhia\My Documents\EAST\Workspaces\11336814.i..wsp

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 94149

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 94149

OR

☐ Firm or Individual Name	Fish & Richardson P.C.		
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

Certicom Corp.
5520 Explorer Drive, 4th Floor
Mississauga, Ontario L4W 5L1, CANADA

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	[signature]	Date	1/24/11
Name	Brian Bidulka	Telephone	(519) 888-7465
Title	Director & President		

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Legal OK
JLHas per [illegible]
RM OK

Electronic Acknowledgement Receipt

EFS ID:	10244690
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	91704
Filer:	Terry J. Stalford/Paige Nordell
Filer Authorized By:	Terry J. Stalford
Attorney Docket Number:	67539/622
Receipt Date:	06-JUN-2011
Filing Date:	23-JAN-2006
Time Stamp:	20:03:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		29717-0048001POA.pdf	1405417 4b8e15b1ad02d413a47d5c666b9d69ebb25579d7	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Assignee showing of ownership per 37 CFR 3.73(b).	1	1
	Power of Attorney	2	2
Warnings:			
Information:			
	Total Files Size (in bytes):	1405417	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Certicom Corp.

Application No./Patent No.: 11/336,814 Filed/Issue Date: January 23, 2006

Entitled: ELLIPTIC CURVE RANDOM NUMBER GENERATION

Certicom Corp., a corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title and interest in
(The extent (by percentage) of its ownership interest is _____%); or

3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

in the patent application/patent identified above by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 017559, Frame 0263 on May 1, 2006.

OR

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy *(i.e.,* a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Terry J. Stalford/	June 6, 2011
Signature	Date
Terry J. Stalford, Reg. No. 39,522	Appointed Practitioner
Printed or Typed Name	Title

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622

CONFIRMATION NO. 1834

94149
Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

POA ACCEPTANCE LETTER

OC000000048200792

Date Mailed: 06/16/2011

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/06/2011.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/mteklemichael/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622

CONFIRMATION NO. 1834

POWER OF ATTORNEY NOTICE

91704
Blake, Cassels & Graydon LLP
199 BAY STREET , SUITE 4000
COMMERCE COURT WEST
TORONTO, ON M5L 1A9
CANADA

OC00000048200747

Date Mailed: 06/16/2011

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/06/2011.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/mteklemichael/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

94149 7590 08/03/2011

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER	
LAKHIA, VIRAL S	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
08/03/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Interview Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *VIRAL LAKHIA*.

(2) *SYED ZIA*.

(3) *MICHAEL HENRY*.

(4) _____.

Date of Interview: *26 July 2011*.

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *1*.

Identification of prior art discussed: *Yes*.

Agreement with respect to the claims f)☐ was reached. g)☒ was not reached. h)☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *Applicants representative explained the background of the invention. The applicant's representative further discussed Fig 7 and clarification of 112 issue with specification and highlighting the benefit of invention. Applicant's representative will submit written response after consultation with the applicant(s)*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/Viral S Lakhia/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R.L. Brown et al.	Art Unit	: 2431
Serial No.	: 11/336,814	Examiner	: Viral S. Lakhia
Filed	: January 23, 2006	Conf. No.	: 1834
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT IN REPLY TO ACTION OF APRIL 15, 2011

Please amend the above-identified application as follows:

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: August 15, 2011

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-67. (Canceled)

68. (New) A computer-implemented method comprising:

obtaining a first input value that represents a first elliptic curve point;

evaluating a hash function based on said first input value, wherein evaluating said hash function generates a hash value;

deriving from said hash value a second input value that represents a second elliptic curve point;

accessing a secret value stored in a register of an arithmetic unit;

generating an output value based on combining said secret value with said second input value;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating an updated secret value based on combining said secret value with said first input value; and

storing said updated secret value in said register.

69. (New) The method of claim 68, wherein said first input value and said second input value represent two different elliptic curve points on the same elliptic curve.

70. (New) The method of claim 68, wherein deriving said second input value includes verifying that said hash value corresponds to a valid coordinate on an elliptic curve, wherein said second elliptic curve point includes said valid coordinate.

71. (New) The method of claim 70, wherein deriving said second input value further includes obtaining a second coordinate for said second elliptic curve point.

72. (New) The method of claim 68, wherein combining said secret value with said second input value comprises generating a scalar multiple of said second elliptic curve point, and combining said secret value with said first input value comprises generating a scalar multiple of said first elliptic curve point.

73. (New) The method of claim 72, wherein generating said output value includes:
selecting a coordinate from said scalar multiple of said second elliptic curve point; and
truncating said coordinate to a bit string.

74. (New) The method of claim 73, wherein truncating said coordinate comprises truncating said coordinate to one half of a length of an elliptic curve point representation.

75. (New) The method of claim 72, wherein generating said output value includes:
selecting a coordinate from said scalar multiple of said second elliptic curve point; and
hashing said coordinate to a bit string.

76. (New) The method of claim 72, wherein generating said updated secret value includes deriving said updated secret value from a coordinate of said scalar multiple of said first elliptic curve point.

77. (New) The method of claim 76, wherein said coordinate of said scalar multiple of said first elliptic curve point comprises an x coordinate.

78. (New) The method of claim 68, wherein obtaining said first input value comprises deriving said first input value from an initial hash value.

79. (New) The method of claim 68, wherein said first input value represents an x coordinate of said first elliptic curve point.

80. (New) The method of claim 68, wherein said second input value represents an x coordinate of said second elliptic curve point.

81. (New) The method of claim 68, wherein said first input represents two coordinates of said first elliptic curve point.

82. (New) The method of claim 68, wherein said second input represents two coordinates of said second elliptic curve point.

83. (New) A computer-implemented method comprising:

obtaining a first input value that represents a first elliptic curve point;

obtaining a second input value that represents a second elliptic curve point;

generating a scalar multiple of said first elliptic curve point based on a secret value and said first input value;

generating an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generating an updated secret value based on said scalar multiple of said first elliptic curve point; and

storing said updated secret value.

84. (New) The method of claim 83, wherein said one-way function includes a hash function.

85. (New) A random number generator system comprising:

an input module operable to:

obtain a first input value that represents a first elliptic curve point;

generate a hash value based on said first input value; and

derive from said hash value a second input value that represents a second elliptic curve point;

a register operable to store a secret value; and

an arithmetic unit operable to:

access said first input value, said second input value, and said secret value;

generate an output value based on said secret value and said second input value;

provide, to a cryptographic module, said output value as a random number in accordance with a specified level of security;

generate an updated secret value based on said secret value and said first input value; and

store said updated secret value in said register.

86. (New) The random number generator system of claim 85, wherein generating said hash value comprises evaluating a hash function based on said first input value.

87. (New) The random number generator system of claim 86, wherein said input module includes a hash function module operable to generate the hash value.

88. (New) The random number generator system of claim 85, wherein said arithmetic unit is operable to generate said output value by generating a coordinate of a scalar multiple of said second elliptic curve point.

89. (New) The random number generator system of claim 88, wherein said arithmetic unit is operable to generate said coordinate of said scalar multiple of said second elliptic curve point based on said secret value and said second input value.

90. (New) The random number generator system of claim 89, wherein said arithmetic unit is operable to generate said updated secret value by generating a coordinate of a scalar multiple of said first elliptic curve point.

91. (New) The random number generator system of claim 90, wherein said arithmetic unit is operable to generate said coordinate of said scalar multiple of said first elliptic curve point based on said secret value and said first input value.

92. (New) The random number generator system of claim 91, wherein said arithmetic unit is operable to generate said updated secret value by converting said coordinate of said scalar multiple of said first elliptic curve point to an integer.

93. (New) The random number generator system of claim 91, wherein said arithmetic unit is operable to generate said output value by:

converting said coordinate of said scalar multiple of said second elliptic curve point to an integer; and

truncating said integer.

94. (New) The random number generator system of claim 93, wherein converting said coordinate includes converting an x coordinate.

95. (New) The random number generator system of claim 88, wherein said arithmetic unit is operable to generate said output value by applying a one-way function to said coordinate of said scalar multiple of said second elliptic curve point.

96. (New) The random number generator system of claim 95, wherein said arithmetic unit is operable to generate said output value by truncating said coordinate of said scalar multiple of said second elliptic curve point prior to applying said one-way function.

97. (New) The random number generator system of claim 85, wherein said first input value represents an x coordinate of said first elliptic curve point.

98. (New) The random number generator system of claim 85, wherein said second input value represents an x coordinate of said second elliptic curve point.

99. (New) The random number generator system of claim 85, wherein said first input value represents two coordinates of said first elliptic curve point.

100. (New) The random number generator system of claim 85, wherein said second input value represents two coordinates of said second elliptic curve point.

101. (New) The random number generator system of claim 85, wherein said first input value and said second input value represent elliptic curve points on the same elliptic curve.

102. (New) A random number generator system comprising:

an input module operable to:

obtain a first input value that represents a first elliptic curve point;

obtain a second input value that represents a second elliptic curve point;

a register operable to store a secret value; and

an arithmetic unit operable to:

access said first input value, said second input value, and said secret value;

generate a scalar multiple of said second elliptic curve point based on said secret value and said second input value;

generate an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

provide, to a cryptographic module, said output value as a random number in accordance with a specified level of security;

generate a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generate an updated secret value based on said scalar multiple of said first elliptic curve point; and

store said updated secret value in said register.

103. (New) The random number generator system of claim 102, wherein said first input value and said second input value represent two different elliptic curve points on the same elliptic curve.

REMARKS

Claims 1-7, 9-11, 13-18, 20-29, and 37-67 were pending in the non-final Office Action dated April 15, 2011 ("the Office Action"). Claims 1-7, 9-11, 13-18, 20-29, and 37-67 were rejected in the Office Action. In the present amendment, claims 1-67 are canceled, and new claims 68-103 are added. Accordingly, claims 68-103 are currently pending in the Application. Claims 68, 83, 85, and 102 are independent claims. Applicants submit that no new matter has been added to the Application by the amendments to the claims. Applicants respectfully request reconsideration of the application in accordance with the following remarks.

Examiner Interview Summary

Applicants note and appreciate the courtesy of the Examiner interview conducted by telephone on July 26, 2011. Examiner Viral Lakhia, Supervisory Patent Examiner Syed Zia, and Applicants' representative Michael Henry participated in the interview. The interview included a discussion of the rejections under 35 U.S.C. § 112 and a discussion of claim 1. Applicants' representative noted that the Office Action appears to reject claim 1 on the basis of language that is not recited in claim 1. The Office indicated that these rejections would be withdrawn if an appropriate response is filed. The Office also suggested that cancelling the prior claims and presenting new claims would be appropriate. Applicants' representative agreed to provide a written response, and the Office agreed to conduct a subsequent interview after the written response has been filed. No further agreement was reached.

Claim Rejections Under 35 U.S.C. § 112

Claims 1-12, 15-18, 20-29, 37-67 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The rejections are respectfully traversed. Moreover, claims 1-67 are currently cancelled, and Applicants respectfully submit that all currently pending claims are in compliance with 35 U.S.C. § 112.

Claim Rejections Under 35 U.S.C. § 101

Claims 1-7, 9-11, 13-18, 20-29, and 37-67 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The rejections are respectfully traversed. Moreover, claims 1-67 are currently canceled, and Applicants respectfully submit that all currently pending claims are in compliance with 35 U.S.C. § 101.

Claim Rejections Under 35 USC § 102

Claims 1-4, 6, 13-17, 37-39, 45-47 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2006/0129800 to Lauter (*Lauter*). The rejections are respectfully traversed because the cited references have not been shown to disclose or suggest the features recited in the claims. Moreover, claims 1-67 are currently canceled, and *Lauter* has not been shown to disclose or suggest the features recited in the currently pending claims.

For example, independent claim 68 recites

> obtaining a first input value that represents a first elliptic curve point;
> evaluating a hash function based on said first input value, wherein evaluating said hash function generates a hash value;
> deriving from said hash value a second input value that represents a second elliptic curve point;
> accessing a secret value stored in a register of an arithmetic unit;
> generating an output value based on combining said secret value with said second input value;
> using said output value as a random number to achieve a specified level of security in a cryptographic operation;
> generating an updated secret value based on combining said secret value with said first input value; and
> storing said updated secret value in said register.

Lauter has not been shown to disclose or suggest at least these features. The Office Action at page 8 cites paragraphs 29-33 of *Lauter*. The cited portion of *Lauter* refers to "two random points, *P* and *P'*," and later refers to a "secret random number, r." *Lauter*, ¶¶ 30-31. *Lauter* has not been shown to disclose or suggest generating an output value and an updated secret value

based on a secret value combined with two elliptic curve points, using the output value as a random number to achieve a specified level of security in a cryptographic operation, and storing the updated secret value in a register. Nor has *Lauter* been shown to disclose or suggest one of the elliptic curve points is derived from a hash value that is based on the other elliptic curve point.

As such, *Lauter* has not been shown to disclose or suggest features of claim 68. Accordingly, it is submitted that claim 68 and its dependent claims are allowable. Independent claim 85 includes features that are analogous one or more of the features of claim 68 discussed above. Accordingly, it is submitted that claim 85 and its dependent claims are allowable at least for analogous reasons.

Moreover, independent claim 83 recites

> obtaining a first input value that represents a first elliptic curve point;
> obtaining a second input value that represents a second elliptic curve point;
> generating a scalar multiple of said first elliptic curve point based on a secret value and said first input value;
> generating an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;
> using said output value as a random number to achieve a specified level of security in a cryptographic operation;
> generating a scalar multiple of said first elliptic curve point based on said secret value and said first input value;
> generating an updated secret value based on said scalar multiple of said first elliptic curve point; and
> storing said updated secret value.

Lauter has not been shown to disclose or suggest at least these features. The Office Action at page 10 cites paragraphs 29-33 and 53-55 of *Lauter*. The cited portion of *Lauter* refers to "two random points, *P* and *P'*," and later refers to a "secret random number, r." *Lauter*, ¶¶ 30-31. *Lauter* has not been shown to disclose or suggest generating scalar multiples of two elliptic curve points based on a secret value, generating an output value and an updated secret value based on the scalar multiples, and using the output value as a random number to achieve a specified level of security in a cryptographic operation. Nor has *Lauter* been shown to disclose or suggest the output value is generated by evaluating a one-way function based on one of the scalar multiples.

As such, *Lauter* has not been shown to disclose or suggest features of claim 83. Accordingly, it is submitted that claim 83 and its dependent claim are allowable. Independent claim 102 includes features that are analogous one or more of the features of claim 83 discussed above. Accordingly, it is submitted that claim 102 and its dependent claim are allowable at least for analogous reasons.

Claim Rejections Under 35 U.S.C. § 103

Claims 5, 7, 9, 27-29, 40-67 are rejected under 35 U.S.C. § 103 as being unpatentable over *Lauter* and in view of U.S. Patent Application Publication No. 2002/0044649 to Gallant et al. (*Gallant*). Claim 10 is rejected under 35 U.S.C. § 103 as being unpatentable over *Lauter*, in view of *Gallant* and further in view of U.S. Patent Application Publication No. 2005/0251680 to Brown et al. (*Brown*). Claim 11 is rejected under 35 U.S.C. § 103 as being unpatentable over *Lauter*, in view of *Gallant* and further in view of U.S. Patent No. 6,044,338 to DeBellis et al. (*DeBellis*). Claim 20-26 are rejected under 35 U.S.C. § 103 as being unpatentable over *Lauter*, in view of *Gallant* and further in view of U.S. Patent No. 6,738,478 to Vanstone et al. (*Vanstone*).

The rejections are respectfully traversed because none of the secondary references (*Gallant*, *Brown*, *DeBellis*, *Vanstone*) have been applied to address the deficiencies of *Lauter* described above. Moreover, claims 1-67 are currently canceled, and the cited references have not been shown to disclose or suggest the features recited in the current claims.

CONCLUSION

Any circumstance in which the Applicants have (a) addressed certain comments of the examiner does not mean that the Applicants concede other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the Applicants concede any of the examiner's positions with respect to that claim or other claims.

If the present application is not allowed and/or if one or more of the rejections is maintained, Applicant hereby requests a telephone conference with the Examiner and further request that the Examiner contact the undersigned agent to schedule the telephone conference.

This Amendment is being filed with a Petition for One-Month Extension of Time and the associated fees. No additional fees are believed to be due. However, the Commissioner is hereby authorized to charge any necessary fees or credit any overpayments to deposit account 06-1050, referencing the attorney docket number shown above.

Respectfully submitted,

Date: August 15, 2011

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone:
Facsimile: (877) 769-7945

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R.L. Brown, et al.	Art Unit	: 2431
Serial No.	: 11/336,814	Examiner	: Viral S. Lakhia
Filed	: January 23, 2006	Conf. No.	: 1834
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR ONE-MONTH EXTENSION OF TIME UNDER 37 C.F.R. §1.136

Please extend the period for response to the action dated April 15, 2011, for one month to and including August 15, 2011.

The fees in the amount of $130 are being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account authorization. Please apply any necessary charges or credits to Deposit Account 06-1050, referencing the above attorney docket number.

Respectfully submitted,

Date: August 15, 2011

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

90536441.doc

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: August 15, 2011.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R.L. Brown, et al.	Art Unit	: 2431
Serial No.	: 11/336,814	Examiner	: Viral S. Lakhia
Filed	: January 23, 2006	Conf. No.	: 1834
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR ONE-MONTH EXTENSION OF TIME UNDER 37 C.F.R. §1.136

Please extend the period for response to the action dated April 15, 2011, for one month to and including August 15, 2011.

The fees in the amount of $130 are being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account authorization. Please apply any necessary charges or credits to Deposit Account 06-1050, referencing the above attorney docket number.

Respectfully submitted,

Date: August 15, 2011

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

90536441.doc

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: August 15, 2011.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11336814
	Filing Date	2006-01-23
	First Named Inventor	Daniel R.L. Brown
	Art Unit	2431
	Examiner Name	Viral S. Lakhia
	Attorney Docket Number	29717-0048001

	1	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on March 10, 2010; 4 pages.	☐
	2	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on July 22, 2010; 4 pages.	☐
	3	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on June 15, 2011; 4 pages.	☐
	4	International Search Report and Written Opinion of the International Searching Authority issued in International Application No. PCT/CA2006/000065 on May 1, 2006; 11 pages.	☐
	5	International Preliminary Report on Patentability issued in International Application No. PCT/CA2006/000065 on August 2, 2007; 8 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Henry/	Date (YYYY-MM-DD)	2011-08-15
Name/Print	Michael K. Henry	Registration Number	59516

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING TRANSMITTAL OF COPY OF INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (CHAPTER I OF THE PATENT COOPERATION TREATY)
(PCT Rule 44bis.1(c))

To:

ORANGE, John R.S.
Blake, Cassels & Graydon Llp
199 Bay Street
Box 25, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Date of mailing *(day/month/year)*	
02 August 2007 (02.08.2007)	
Applicant's or agent's file reference 67539/00623	**IMPORTANT NOTICE**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/CA2006/000065	23 January 2006 (23.01.2006)	21 January 2005 (21.01.2005)

Applicant
CERTICOM CORP. et al

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Athina Nickitas-Etienne

e-mail: pt04.pct@wipo.int

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 67539/00623	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/CA2006/000065	International filing date *(day/month/year)* 23 January 2006 (23.01.2006)	Priority date *(day/month/year)* 21 January 2005 (21.01.2005)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant CERTICOM CORP.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☒	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 24 July 2007 (24.07.2007)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Athina Nickitas-Etienne e-mail: pt04.pct@wipo.int

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
BLAKE, CASSELS & GRAYDON LLP
Box 25, Commerce Court West
199 Bay Street
TORONTO, Ontario
Canada, M5L 1A9

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)* 1 May 2006 (01-05-2006)

Applicant's or agent's file reference
67539/00623

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/CA2006/000065	23 January 2006 (23-01-2006)	21 January 2005 (21-01-2005)

International Patent Classification (IPC) or both national classification and IPC
IPC: ***G06F 7/58*** (2006.01) , ***H04L 9/28*** (2006.01)

Applicant
CERTICOM CORP. ET AL

1. This opinion contains indications relating to the following items :

- [X] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [X] Box No. V Reasoned statement under Rule 43*bis*.1(a)(I) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [X] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**
If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/CA	Date of completion of this opinion	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	10 April 2006 (10.04.06)	Reid Mulligan (819) 934-7566

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   [X] the international application in the language in which it was filed

   [ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of :

   a. type of material

      [ ] a sequence listing

      [ ] table(s) related to the sequence listing

   b. format of material

      [ ] on paper

      [ ] in electronic form

   c. time of filing/furnishing

      [ ] contained in the international application as filed.

      [ ] filed together with the international application in electronic form

      [ ] furnished subsequently to this Authority for the purposes of search.

3 [ ] In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statement that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments :

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(I) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1 to 19	YES
	Claims	none	NO
Inventive step (IS)	Claims	5 to 11	YES
	Claims	1 to 4 and 12 to 19	NO
Industrial applicability (IA)	Claims	1 to 19	YES
	Claims	none	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: "Elliptic Curve Random Number Generation" (Lee et al.) 19 August 2001 (19.08.01)
D2: "A Pseudo-Random Bit Generator Based On Elliptic Logarithms" (Kaliski) 1987
D3: US 2004/0102242 (Poelmann) 27 May 2004 (27.05.04)
D4: US 6,044,388 (Debellis et al.) 28 March 2000 (28.03.00)
D5: US 6,243,467 (Reiter et al.) 5 June 2001 (5.06.01)

Article 33 (2) PCT - Novelty

1) When taken alone, none of documents D1, D2, D3, D4 or D5 disclose features of independent claims 1, 13, 15, and 19. More specifically, none of the following features are disclosed: a method of computing a random number with a pair of inputs to an elliptic curve random number generator with one such input being verifiably random; a method of computing a random number with a pair of inputs with each representing a point on a elliptic curve to an elliptic curve random number generator and an output passing through a one-way function; a elliptic curve random number generator having a pair of inputs, one being a coordinate of an elliptic curve point and one input being verifiably random; and, establishing an escrow key, 'e', with an administrator for generating a random number through an elliptic curve random number generator.

Therefore, the subject matter of claims 1 to 19 is novel under **Article 33(2) PCT** in view of D1, D2, D3, D4 or D5.

Article 33(3) PCT - Inventive Step

2) Independent claims 1, 12, and 15 are obvious in view of D1 or D2 and D3. Both D1 and D2 discuss a random number generator based on an elliptic curve and since it is based on an elliptic curve, they require two coordinates in order to compute the logarithm and produce a random number. D3 describes a method of establishing a verifiable random number. This verifiably random number can be utilized in any type of process, like the input of a random number generator, to show that the random number was computed correctly (par. 9).

(continued on Supplemental Box 1, see page 5)

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted :

1. The reference "a network 42" found on page 9, line 25 does not comply with **Rule 11.13 (l) PCT**. Reference signs not mentioned in the description shall not appear in the drawings, and vice versa.

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of: **Box V**

Additionally, the fact that the verifiably random input is in canonical form does not differentiate over the prior art since this is based on personal preference of a skilled worker which would not affect the end result if the inputs where of another form and therefore, would be obvious to someone skilled in the art.

Therefore, the subject matter of claims 1, 12, and 15 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D3.

3) Dependent claims 2, 3, 16, 17, and 18 are obvious in view of D1 or D2 and D3 and D4. D4 describes a pseudo-random number generator in a cryptographic module comprising a time dependent value with a secret value with the results passing through a one-way hash function (abstract). Therefore, the use of a hash function would be obvious to someone skilled in the art since the role of a hash function is to transform the data into a fix sized string, in order, to mask the original data.

Therefore, the subject matter of claims 2, 3, 16, 17, and 18 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D3 and D4.

4) The dependent claim 4 is obvious in view of D1 or D2 and D3 and D5. D5 describes a method to securely generate and verify a digital signature based on a discrete logarithm and on an elliptic curve. D5 discloses that scalar multiplication is a dominate operation in elliptic curve cryptography and an integer k for use in the scalar multiplication (col. 4, lines 61-67 and col. 5, lines 1-11). Thus, the addition of a secret value, like integer k, for use as a scalar multiple would be an obvious computation in view of the prior art.

Therefore, the subject matter of claim 4 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D3 and D5.

5) Claims 13 and 14 are obvious in view of D1 or D2 and D4 and D5. As mentioned above, the use of scalar multiples and the inclusion of a one-way hash function at the output of the random number generator is an obvious embodiment since both are well known for use in elliptic curve cryptography or random number generators. Thus, fail to provide an inventive step and would be well known to a skilled technician in the art.

Therefore, the subject matter of claims 13 and 14 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D4 and D5.

6) Independent claim 19 is obvious in view of D1 or D2 and D5. Claim 19 describes an escrow key, 'e', for use in the scalar multiplication of Q such that P=eQ for generating a random number from an elliptic curve random number generator. Subsequently, in D1 and D5, where Q = kP to compute the value of Q integer k is needed. Therefore, the inclusion of an escrow key, 'e', does not add an inventive step since the integer would need to be provided and the fact that a third party possesses this key does not add an inventive step since the third party only keeps this key in secret from outside parties. Thus, having a third party safeguard the key would be obvious to someone skilled in the art.

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of: **Supplement Box 1**

Therefore, the subject matter of claim 19 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D5.

7) Dependent claims 5 to 11 involve an inventive step in view of D1, D2, D3, D4 or D5. None of the documents alone or in combination teach a method of computing a random number where one scalar multiple is used to derive a random number and changes the secret value for subsequent use, validating the output of a hash function of an elliptic curve point for use as an input, the random number is derived from a scalar multiple and selecting a coordinate and truncating or hashing a coordinate to a bit string for use as a random number.

Therefore, the subject matter of claims 5 to 11 does involve an inventive step under **Article 33(3) PCT** in view of D1, D2, D3, D4 or D5.

Article 33(4) PCT - Industrial Applicability

8) Claims 1 to 19 are considered to be industrial applicable as per **Article 33(4) PCT**.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
BLAKE, CASSELS & GRAYDON LLP
Box 25, Commerce Court West
199 Bay Street
TORONTO, Ontario
Canada, M5L 1A9

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 1 May 2006 (01-05-2006)
Applicant's or agent's file reference 67539/00623	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/CA2006/000065	International filing date *(day/month/year)* 23 January 2006 (23-01-2006)

Applicant
CERTICOM CORP. ET AL

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19 :
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46) :

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that :

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for the international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Authorized officer Lucille Leonard (819) 953-1737

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 67539/00623	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below
International application No. **PCT/CA2006/000065**	International filing date *(day/month/year)* 23 January 2006 (23-01-2006)	(Earliest)Priority date *(day/month/year)* 21 January 2005 (21-01-2005)
Applicant CERTICOM CORP. ET AL		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of:

      [X] the international application in the language in which it was filed

      [ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

   b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I

2. [ ] **Certain claims were found unsearchable** (see Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No. III)

4. With regard to the **title**,

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established by this Authority to read as follows :

5. With regard to the **abstract**,

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

   a. the figure of the **drawings** to be published with the abstract is Figure No. 1

      [X] as suggested by the applicant

      [ ] as selected by this Authority, because the applicant failed to suggest a figure

      [ ] as selected by this Authority, because this figure better characterizes the invention

   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2006/000065

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G06F 7/58*** (2006.01) , ***H04L 9/28*** (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: *G06F 7/00* (2006.01); *G06F 7/58* (2006.01); *H04L 9/28* (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Databases used: Canadian Patent Database; USPTO West (full-text patent database, pre-grant publication, EPO/JPO abstracts); Esp@cenet; and, IEEE Xplore.
Search words used: elliptic curve, random number generator, cryptography, scalar multiple(s), verifiably random, escrow key, truncate, and hash function.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Categor	Citation of document, with indication, where appropriate, of the	Relevant to claim No.
Y	Lee et al., "Elliptic Curve Random Number Generation" *Electrical and Electronic Technology, 2001. Tencon. Proceedings of IEEE Region 10 International Conference on 19-22 August 2001.* Volume 1, pages 239 to 241. entire document	1-4, 12-19
Y	Kaliski, B S., "A Pseudo-Random Bit Generator Based On Elliptic Logarithms". *Advances in Cryptology, CRYPTO 1986.* Volume 263, pages 84 to 103, 1987. entire document	1-4, 12-19
Y	US 2004/0102242 (Poelmann) 27 May 2004 (27.05.04) abstract; paragraph 9	1-4, 12, 15-18

[X] Further documents are listed in the continuation of [X] See patent family annex.

* Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 April 2006 (10-04-2006)	1 May 2006 (01-05-2006)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Authorized officer Reid Mulligan (819) 934-7566

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the	Relevant to claim No.
Y	US 6,044,388 (Debellis et al.) 28 May 2000 (28.05.2000) abstract; column 5, lines 1-8	2, 3, 13, 14, 16-18
Y	US 6,243,467 (Reiter et al.) 5 June 2001 (5.06.2001) column 4, lines 61-67 and column 5, lines 1-11	4, 19

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US 2004/0102242	27-05-2004	AU 2003288680 A1 WO 2004046911 A2	15-06-2004 03-06-2004
US 6,044,388	28-03-2000	NONE	
US 6,243,467	05-06-2001	NONE	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
BLAKE, CASSELS & GRAYDON LLP
Box 25, Commerce Court West
199 Bay Street
TORONTO, Ontario
Canada, M5L 1A9

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	1 May 2006 (01-05-2006)
Applicant's or agent's file reference 67539/00623	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/CA2006/000065	23 January 2006 (23-01-2006)	21 January 2005 (21-01-2005)

International Patent Classification (IPC) or both national classification and IPC
IPC: ***G06F 7/58*** (2006.01) , ***H04L 9/28*** (2006.01)

Applicant
CERTICOM CORP. ET AL

1. This opinion contains indications relating to the following items :

[X]	Box No. I	Basis of the opinion
[ ]	Box No. II	Priority
[ ]	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
[ ]	Box No. IV	Lack of unity of invention
[X]	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(I) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
[ ]	Box No. VI	Certain documents cited
[X]	Box No. VII	Certain defects in the international application
[ ]	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**
If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/CA	Date of completion of this opinion	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	10 April 2006 (10.04.06)	Reid Mulligan (819) 934-7566

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   [**X**] the international application in the language in which it was filed

   [ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of :

   a. type of material

      [ ] a sequence listing

      [ ] table(s) related to the sequence listing

   b. format of material

      [ ] on paper

      [ ] in electronic form

   c. time of filing/furnishing

      [ ] contained in the international application as filed.

      [ ] filed together with the international application in electronic form

      [ ] furnished subsequently to this Authority for the purposes of search.

3 [ ] In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statement that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments :

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(I) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1 to 19	YES
	Claims	none	NO
Inventive step (IS)	Claims	5 to 11	YES
	Claims	1 to 4 and 12 to 19	NO
Industrial applicability (IA)	Claims	1 to 19	YES
	Claims	none	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: "Elliptic Curve Random Number Generation" (Lee et al.) 19 August 2001 (19.08.01)
D2: "A Pseudo-Random Bit Generator Based On Elliptic Logarithms" (Kaliski) 1987
D3: US 2004/0102242 (Poelmann) 27 May 2004 (27.05.04)
D4: US 6,044,388 (Debellis et al.) 28 March 2000 (28.03.00)
D5: US 6,243,467 (Reiter et al.) 5 June 2001 (5.06.01)

Article 33 (2) PCT - Novelty

1) When taken alone, none of documents D1, D2, D3, D4 or D5 disclose features of independent claims 1, 13, 15, and 19. More specifically, none of the following features are disclosed: a method of computing a random number with a pair of inputs to an elliptic curve random number generator with one such input being verifiably random; a method of computing a random number with a pair of inputs with each representing a point on a elliptic curve to an elliptic curve random number generator and an output passing through a one-way function; a elliptic curve random number generator having a pair of inputs, one being a coordinate of an elliptic curve point and one input being verifiably random; and, establishing an escrow key, 'e', with an administrator for generating a random number through an elliptic curve random number generator.

Therefore, the subject matter of claims 1 to 19 is novel under **Article 33(2) PCT** in view of D1, D2, D3, D4 or D5.

Article 33(3) PCT - Inventive Step

2) Independent claims 1, 12, and 15 are obvious in view of D1 or D2 and D3. Both D1 and D2 discuss a random number generator based on an elliptic curve and since it is based on an elliptic curve, they require two coordinates in order to compute the logarithm and produce a random number. D3 describes a method of establishing a verifiable random number. This verifiably random number can be utilized in any type of process, like the input of a random number generator, to show that the random number was computed correctly (par. 9).

(continued on Supplemental Box 1, see page 5)

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted :

1. The reference "a network 42" found on page 9, line 25 does not comply with **Rule 11.13 (l) PCT**. Reference signs not mentioned in the description shall not appear in the drawings, and vice versa.

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of: **Box V**

Additionally, the fact that the verifiably random input is in canonical form does not differentiate over the prior art since this is based on personal preference of a skilled worker which would not affect the end result if the inputs where of another form and therefore, would be obvious to someone skilled in the art.

Therefore, the subject matter of claims 1, 12, and 15 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D3.

3) Dependent claims 2, 3, 16, 17, and 18 are obvious in view of D1 or D2 and D3 and D4. D4 describes a pseudo-random number generator in a cryptographic module comprising a time dependent value with a secret value with the results passing through a one-way hash function (abstract). Therefore, the use of a hash function would be obvious to someone skilled in the art since the role of a hash function is to transform the data into a fix sized string, in order, to mask the original data.

Therefore, the subject matter of claims 2, 3, 16, 17, and 18 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D3 and D4.

4) The dependent claim 4 is obvious in view of D1 or D2 and D3 and D5. D5 describes a method to securely generate and verify a digital signature based on a discrete logarithm and on an elliptic curve. D5 discloses that scalar multiplication is a dominate operation in elliptic curve cryptography and an integer k for use in the scalar multiplication (col. 4, lines 61-67 and col. 5, lines 1-11). Thus, the addition of a secret value, like integer k, for use as a scalar multiple would be an obvious computation in view of the prior art.

Therefore, the subject matter of claim 4 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D3 and D5.

5) Claims 13 and 14 are obvious in view of D1 or D2 and D4 and D5. As mentioned above, the use of scalar multiples and the inclusion of a one-way hash function at the output of the random number generator is an obvious embodiment since both are well known for use in elliptic curve cryptography or random number generators. Thus, fail to provide an inventive step and would be well known to a skilled technician in the art.

Therefore, the subject matter of claims 13 and 14 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D4 and D5.

6) Independent claim 19 is obvious in view of D1 or D2 and D5. Claim 19 describes an escrow key, 'e', for use in the scalar multiplication of Q such that P=eQ for generating a random number from an elliptic curve random number generator. Subsequently, in D1 and D5, where Q = kP to compute the value of Q integer k is needed. Therefore, the inclusion of an escrow key, 'e', does not add an inventive step since the integer would need to be provided and the fact that a third party possesses this key does not add an inventive step since the third party only keeps this key in secret from outside parties. Thus, having a third party safeguard the key would be obvious to someone skilled in the art.

(continued on Supplemental Box 2, see page 6)

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of: **Supplement Box 1**

Therefore, the subject matter of claim 19 does not involve an inventive step under **Article 33(3) PCT** in view of D1 or D2 and D5.

7) Dependent claims 5 to 11 involve an inventive step in view of D1, D2, D3, D4 or D5. None of the documents alone or in combination teach a method of computing a random number where one scalar multiple is used to derive a random number and changes the secret value for subsequent use, validating the output of a hash function of an elliptic curve point for use as an input, the random number is derived from a scalar multiple and selecting a coordinate and truncating or hashing a coordinate to a bit string for use as a random number.

Therefore, the subject matter of claims 5 to 11 does involve an inventive step under **Article 33(3) PCT** in view of D1, D2, D3, D4 or D5.

Article 33(4) PCT - Industrial Applicability

8) Claims 1 to 19 are considered to be industrial applicable as per **Article 33(4) PCT**.

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	Michael K. Henry/Susan Johnson
Attorney Docket Number:	67539/622

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	130	130

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**310**

Electronic Acknowledgement Receipt

EFS ID:	10736791
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Susan Johnson
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	67539/622
Receipt Date:	15-AUG-2011
Filing Date:	23-JAN-2006
Time Stamp:	15:03:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$310
RAM confirmation Number	1426
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		29717-0048001_ResponseToOfficeAction.pdf	122401 cd98d62182ee01f3ce0b15b5986eadc33faf096f	yes	12

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	12

Warnings:

Information:

2	Extension of Time	29717-0048001_ExtensionOfTime.pdf	65686 cf5eec04cbe4cfcbcd1f913c57df3b5ebaf32426	no	1

Warnings:

Information:

3	Information Disclosure Statement (IDS) Form (SB08)	29717-0048001_InformationDisclosureSB08.pdf	31596 d42589b22f2f4824c1ae349eb645626610ac1935	no	4

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

4	Non Patent Literature	EPOAJuly2010.pdf	125147 b8305c932e5087bb1737d6c9b926ccfe9e89623d	no	4

Warnings:

Information:

5	Non Patent Literature	EPOAJune2011.pdf	102139 d283d1dd55529db9267da307cfc82d393faaa660	no	4

Warnings:

Information:

6	Non Patent Literature	EPOAMar2010.pdf	159956 e1e5d61bb9a475550a9671de235eb3f4f09ea967	no	4

Warnings:

Information:

7	Non Patent Literature	WO1IPRP.pdf	346825 c9637d8d9b031766db0cf70001b5dd6aa944f45b	no	8

Warnings:

Information:

8	Non Patent Literature	WO1ISRWrittenOpinion.pdf	527190 d909bddceeab9730fdbc6bd09bb96f6c5fe3f161	no	11
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	31813 538ebc7c1704e574c0683a34df93889b56527c14	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1512753	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/336,814	01/23/2006	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
FOR	NUMBER FILED	NUMBER EXTRA					
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT	08/15/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 36	Minus	** 57	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DIANE JOHNSON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit	: 2431
Serial No.	: 11/336,814	Examiner	: Viral S. Lakhia
Filed	: January 23, 2006	Conf. No.	: 1834
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL AMENDMENT
IN REPLY TO THE OFFICE ACTION OF APRIL 15, 2011

Please amend the above-identified application as follows:

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: September 23, 2011.

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-67. (Canceled)

68. (Currently Amended) A computer-implemented method comprising:

obtaining a first input value that represents a first elliptic curve point;

evaluating a hash function based on said first input value, wherein evaluating said hash function generates a hash value;

deriving from said hash value a second input value that represents a second elliptic curve point;

accessing an initial secret value stored in a register of an arithmetic unit;

generating, by a processor, an output value based on a scalar multiple of said second elliptic curve point, the scalar multiple of said second elliptic curve point obtained by combining said secret value with said second input value;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating, by the processor, an updated secret value based on a scalar multiple of said first elliptic curve point, the scalar multiple of said first elliptic curve point obtained by combining said initial secret value with said first input value; and

storing said updated secret value in said register.

69. (Previously Presented) The method of claim 68, wherein said first input value and said second input value represent two different elliptic curve points on the same elliptic curve.

70. (Previously Presented) The method of claim 68, wherein deriving said second input value includes verifying that said hash value corresponds to a valid coordinate on an elliptic curve, wherein said second elliptic curve point includes said valid coordinate.

71. (Previously Presented) The method of claim 70, wherein deriving said second input value further includes obtaining a second coordinate for said second elliptic curve point.

72. (Canceled)

73. (Currently Amended) The method of claim 68 [[72]], wherein generating said output value includes:

selecting a coordinate from said scalar multiple of said second elliptic curve point; and

truncating said coordinate to a bit string.

74. (Previously Presented) The method of claim 73, wherein truncating said coordinate comprises truncating said coordinate to one half of a length of an elliptic curve point representation.

75. (Currently Amended) The method of claim 68 [[72]], wherein generating said output value includes:

selecting a coordinate from said scalar multiple of said second elliptic curve point; and

hashing said coordinate to a bit string.

76. (Currently Amended) The method of claim 68 [[72]], wherein generating said updated secret value includes deriving said updated secret value from a coordinate of said scalar multiple of said first elliptic curve point.

77. (Previously Presented) The method of claim 76, wherein said coordinate of said scalar multiple of said first elliptic curve point comprises an x coordinate.

78. (Previously Presented) The method of claim 68, wherein obtaining said first input value comprises deriving said first input value from an initial hash value.

79. (Previously Presented) The method of claim 68, wherein said first input value represents an x coordinate of said first elliptic curve point.

80. (Previously Presented) The method of claim 68, wherein said second input value represents an x coordinate of said second elliptic curve point.

81. (Previously Presented) The method of claim 68, wherein said first input represents two coordinates of said first elliptic curve point.

82. (Previously Presented) The method of claim 68, wherein said second input represents two coordinates of said second elliptic curve point.

83. (Previously Presented) A computer-implemented method comprising:

obtaining a first input value that represents a first elliptic curve point;

obtaining a second input value that represents a second elliptic curve point;

generating a scalar multiple of said first elliptic curve point based on a secret value and said first input value;

generating an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generating an updated secret value based on said scalar multiple of said first elliptic curve point; and

storing said updated secret value.

84. (Previously Presented) The method of claim 83, wherein said one-way function includes a hash function.

85. (Previously Presented) A random number generator system comprising:

an input module operable to:

obtain a first input value that represents a first elliptic curve point;

generate a hash value based on said first input value; and

derive from said hash value a second input value that represents a second elliptic

curve point;

a register operable to store a secret value; and

an arithmetic unit operable to:

access said first input value, said second input value, and said secret value;

generate an output value based on said secret value and said second input value;

provide, to a cryptographic module, said output value as a random number in accordance with a specified level of security;

generate an updated secret value based on said secret value and said first input value; and

store said updated secret value in said register.

86. (Previously Presented) The random number generator system of claim 85, wherein generating said hash value comprises evaluating a hash function based on said first input value.

87. (Previously Presented) The random number generator system of claim 86, wherein said input module includes a hash function module operable to generate the hash value.

88. (Previously Presented) The random number generator system of claim 85, wherein said arithmetic unit is operable to generate said output value by generating a coordinate of a scalar multiple of said second elliptic curve point.

89. (Previously Presented) The random number generator system of claim 88, wherein said arithmetic unit is operable to generate said coordinate of said scalar multiple of said second elliptic curve point based on said secret value and said second input value.

90. (Previously Presented) The random number generator system of claim 89, wherein said arithmetic unit is operable to generate said updated secret value by generating a coordinate of a scalar multiple of said first elliptic curve point.

91. (Previously Presented) The random number generator system of claim 90, wherein said arithmetic unit is operable to generate said coordinate of said scalar multiple of said first elliptic curve point based on said secret value and said first input value.

92. (Previously Presented) The random number generator system of claim 91, wherein said arithmetic unit is operable to generate said updated secret value by converting said coordinate of said scalar multiple of said first elliptic curve point to an integer.

93. (Previously Presented) The random number generator system of claim 91, wherein said arithmetic unit is operable to generate said output value by:

converting said coordinate of said scalar multiple of said second elliptic curve point to an integer; and

truncating said integer.

94. (Previously Presented) The random number generator system of claim 93, wherein converting said coordinate includes converting an x coordinate.

95. (Previously Presented) The random number generator system of claim 88, wherein said arithmetic unit is operable to generate said output value by applying a one-way function to said coordinate of said scalar multiple of said second elliptic curve point.

96. (Previously Presented) The random number generator system of claim 95, wherein said arithmetic unit is operable to generate said output value by truncating said coordinate of said scalar multiple of said second elliptic curve point prior to applying said one-way function.

97. (Previously Presented) The random number generator system of claim 85, wherein said first input value represents an x coordinate of said first elliptic curve point.

98. (Previously Presented) The random number generator system of claim 85, wherein said second input value represents an x coordinate of said second elliptic curve point.

99. (Previously Presented) The random number generator system of claim 85, wherein said first input value represents two coordinates of said first elliptic curve point.

100. (Previously Presented) The random number generator system of claim 85, wherein said second input value represents two coordinates of said second elliptic curve point.

101. (Previously Presented) The random number generator system of claim 85, wherein said first input value and said second input value represent elliptic curve points on the same elliptic curve.

102. (Previously Presented) A random number generator system comprising:

an input module operable to:

obtain a first input value that represents a first elliptic curve point;

obtain a second input value that represents a second elliptic curve point;

a register operable to store a secret value; and

an arithmetic unit operable to:

access said first input value, said second input value, and said secret value;

generate a scalar multiple of said second elliptic curve point based on said secret value and said second input value;

generate an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

provide, to a cryptographic module, said output value as a random number in accordance with a specified level of security;

generate a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generate an updated secret value based on said scalar multiple of said first elliptic curve point; and

store said updated secret value in said register.

103. (Previously Presented) The random number generator system of claim 102, wherein said first input value and said second input value represent two different elliptic curve points on the same elliptic curve.

104. (New) The method of claim 68, wherein the first input value comprises a verifiably random first input value.

105. (New) The method of claim 104, wherein the second input value comprises a verifiably random second input value.

106. (New) The method of claim 83, wherein the first input value comprises a verifiably random first input value.

107. (New) The method of claim 106, wherein the second input value comprises a verifiably random second input value.

108. (New) The random number generator system of claim 85, wherein the first input value comprises a verifiably random first input value.

109. (New) The random number generator system of claim 108, wherein the second input value comprises a verifiably random second input value.

110. (New) The random number generator system of claim 102, wherein the first input value comprises a verifiably random first input value.

111. (New) The random number generator system of claim 110, wherein the second input value comprises a verifiably random second input value.

REMARKS

Claims 1-7, 9-11, 13-18, 20-29, and 37-67 were pending in the non-final Office Action dated April 15, 2011. Claims 1-67 were canceled and claims 68-103 were added by the Amendment dated August 15, 2011. Claims 68, 73, 75, and 76 are currently amended. Claim 72 is currently canceled. New claims 104-111 are currenlty added. Accordingly, claims 68-71 and 73-111 are now pending in the Application. Claims 68, 83, 85, and 102 are independent claims. Applicants submit that no new matter has been added to the Application by the amendments to the claims. Applicants respectfully request reconsideration of the application in accordance with the following remarks.

Examiner Interview Summary

Applicants note and appreciate the courtesy of the Examiner interview conducted by telephone on September 16, 2011. Examiner Viral Lakhia and Applicants' representative Michael Henry participated in the interview. The interview included a discussion of the Amendment filed on August 15, 2011. The Examiner suggested additional amendments to claim 68 that would place the application in condition for allowance. Applicants' representative agreed to notify the Examiner of whether the Examiner's suggested amendments would be acceptable. No further agreement was reached during the Examiner interview.

The Application Is In Condition for Allowance

The undersigned attempted to contact Examiner Lakhia by phone on September 21, 22, and 23, 2011 to notify him that a Supplemental Amendment would be filed to adopt the amendments that were suggested by the Examiner during the Examiner interview of September 16, 2011. This Supplemental Amendment is being filed with the amendments suggested by the Examiner and accordingly is believed to place the case in condition for allowance. Accordingly, allowance of the present application is respectfully requested.

Request for Examiner Interview

If the present application is not allowed and/or if one or more of the rejections is maintained, Applicants hereby request a telephone conference with the Examiner and further request that the Examiner contact the undersigned agent to schedule the telephone conference.

CONCLUSION

Any circumstance in which the Applicants have (a) addressed certain comments of the examiner does not mean that the Applicants concede other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the Applicants concede any of the examiner's positions with respect to that claim or other claims.

Fees in the amount of $416 are currently being paid for addition of eight dependent claims in excess of twenty total claims. No additional fees are believed to be due. However, the Commissioner is hereby authorized to charge any necessary fees or credit any overpayments to deposit account 06-1050, referencing the attorney docket number shown above.

Respectfully submitted,

Date: September 23, 2011

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Vanstone
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001/35404-US-PA

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
1	1	2003-507761	JP		2003-02-25	Siemens Aktiengesellschaft		☒

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11336814
	Filing Date	2006-01-23
	First Named Inventor	Vanstone
	Art Unit	2431
	Examiner Name	Viral S. Lakhia
	Attorney Docket Number	29717-0048001/35404-US-PA

	1	ANS X9.62-2005; "Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA)"; November 16, 2005; 163 pages.	☐
	2	ANSI X9.82; "Part 3 - Draft" October 2003; 175 pages.	☐
	3	ANS X9.82; "Part 3 - Draft"; June 2004; 189 pages.	☐
	4	Barker, Elaine and John Kelsey; "Recommendation for Random Number Generation Using Deterministic Random Bit Generators"; NIST Special Publication 800-90; National Institute of Standards and Technology; December 2005; 130 pages.	☐
	5	Barker, Elaine and John Kelsey; "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)"; NIST Special Publication 800-90; National Institute of Standards and Technology; March 2007; 133 pages.	☐
	6	Blum, Manuel and Silvio Micali; "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits"; SIAM Journal on Computing; Vol. 13, No. 4; November 1984; pp. 850-864.	☐
	7	Brown, Daniel R.L.; "Conjecture Security of the ANSI-NIST Elliptic Curve RNG"; Cryptology ePrint Archive; Report 2006/117; March 29, 2006; 14 pages. Retrieved from the internet <http://eprint.iacr.org>.	☐
	8	El Mahassni, Edwin and Igor Shparlinksi; "On the Uniformity of Distribution of Congruential Generators over Elliptic Curves"; Sequences and Their Applications: Proceedings of SETA '01; 2002' pp. 257-264.	☐
	9	Goldreich, Oded; "Foundations of Cryptography Basic Tools'; Cambridge University Press; 2001; pages 30-183.	☐
	10	Gjoesteen, Kristian; "Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005"; March 16, 2006; 8 pages.	☐
	11	Guerel, Nicolas; "Extracting Bits from Coordinates of a Point of an Elliptic Curve"; Cryptology ePrint Archive; Report 2005/324; 2005; 9 pages. Retrieved from the internet <http://eprint.iacr.org>	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11336814
	Filing Date	2006-01-23
	First Named Inventor	Vanstone
	Art Unit	2431
	Examiner Name	Viral S. Lakhia
	Attorney Docket Number	29717-0048001/35404-US-PA

	12	Luby, Michael; "Pseudorandomness and Cryptographic Applications"; Princeton University Press; 1996; pp. 70-78.	☐
	13		☐
	14		☐
	15		☐
	16		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Vanstone
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001/35404-US-PA

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Henry/	Date (YYYY-MM-DD)	2011-09-23
Name/Print	Michael K. Henry	Registration Number	59516

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. Februar 2001 (22.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/13218 A1

(51) Internationale Patentklassifikation[7]: G06F 7/58, H04L 9/32 // G06F 7/72

(21) Internationales Aktenzeichen: PCT/DE00/02776

(22) Internationales Anmeldedatum:
16. August 2000 (16.08.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 39 059.2 18. August 1999 (18.08.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HESS, Erwin** [DE/DE]; Gottfried-Keller-Strasse 36, D-85521 Ottobrunn (DE). **SERF, Pascale** [DE/DE]; Max-Löw-Strasse 61, D-85579 Neubiberg (DE).

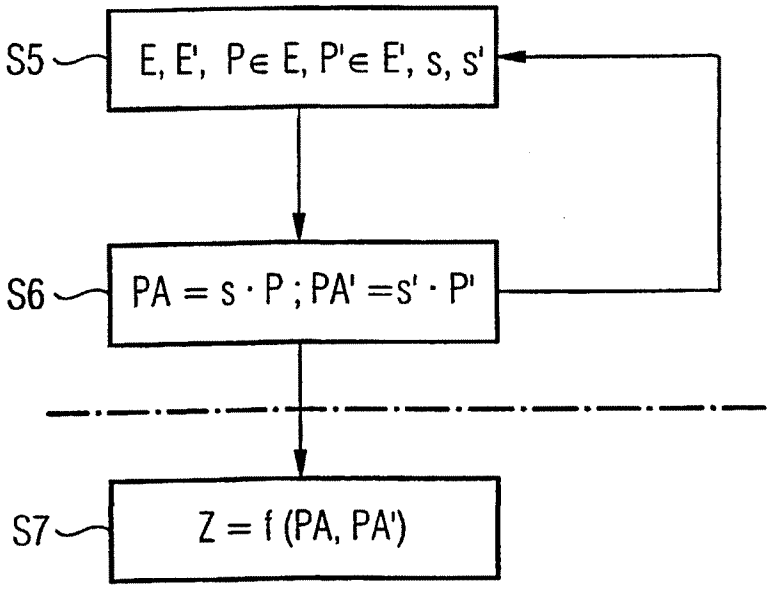
(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, D-80506 München (DE).

(81) Bestimmungsstaaten *(national)*: CA, JP, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR GENERATING PSEUDO RANDOM NUMBERS AND METHOD FOR ELECTRONIC SIGNATURES

(54) Bezeichnung: VERFAHREN ZUM ERZEUGEN VON PSEUDOZUFALLSZAHLEN UND VERFAHREN FÜR ELEKTRONISCHE SIGNATUR



(57) Abstract: The invention relates to a method for generating pseudo random numbers and a method for electronic signatures. According to the inventive method for generating pseudo random numbers, points are determined on at least two different elliptical curves. A pseudo random number is produced respectively by linking the points. The linking of points of different elliptical curves to generate a pseudo random number makes it impossible to deduce the individual elliptical curves on the basis of the pseudo random numbers. The cryptographic security of the inventive method is thus tremendously increased because the computation of discrete logarithms is made impossible.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Erzeugen von Pseudozufallszahlen, sowie ein Verfahren für elektronische Signatur. Bei dem erfindungsgemäßen Verfahren zum Erzeugen von Pseudozufallszahlen werden Punkte auf zumindest zwei verschiedenen elliptischen Kurven bestimmt, und durch Verknüpfen der Punkte wird jeweils eine Pseudozufallszahl erzeugt. Das Verknüpfen der Punkte von unterschiedlichen elliptischen Kurven zu einer Pseudozufallszahl macht Rückschlüsse aus den so erzeugten Pseudozufallszahlen auf die einzelnen elliptischen Kurven unmöglich, wodurch die kryptographische Sicherheit des erfindungsgemäßen Verfahrens erheblich erhöht wird, weil die Berechnung diskreter Logarithmen unmöglich gemacht wird.

WO 01/13218 A1

Cited Reference 3

(19)日本国特許庁（ＪＰ）　(12)**公表特許公報**（Ａ）　(11)特許出願公表番号
特表2003－507761
（P2003－507761A）
(43)公表日　平成15年２月25日(2003.2.25)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０９Ｃ	1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ	５Ｊ１０４
Ｇ０６Ｆ	7/58		Ｇ０６Ｆ　7/58	Ａ	
Ｈ０４Ｌ	9/30		Ｈ０４Ｌ　9/00	６７５Ｂ	
	9/32			６６３Ｚ	

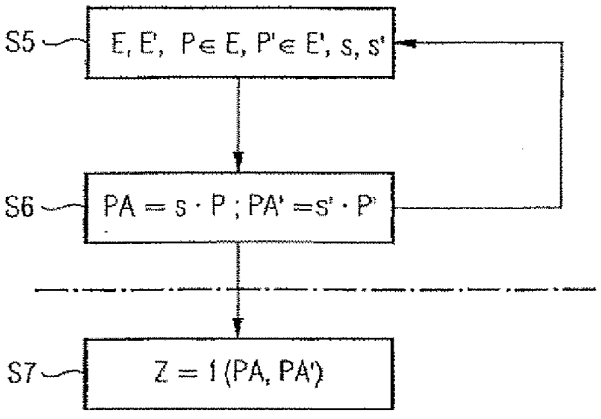
審査請求　未請求　予備審査請求　有　（全 19 頁）

(21)出願番号　特願2001－517250(P2001－517250)
(86)(22)出願日　平成12年８月16日(2000.8.16)
(85)翻訳文提出日　平成14年２月15日(2002.2.15)
(86)国際出願番号　ＰＣＴ／ＤＥ００／０２７７６
(87)国際公開番号　ＷＯ０１／０１３２１８
(87)国際公開日　平成13年２月22日(2001.2.22)
(31)優先権主張番号　１９９　３９　０５９．２
(32)優先日　平成11年８月18日(1999.8.18)
(33)優先権主張国　ドイツ（ＤＥ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＪＰ，ＵＳ

(71)出願人　シーメンス　アクチエンゲゼルシヤフト
Ｓｉｅｍｅｎｓ　Ａｋｔｉｅｎｇｅｓｅｌｌｓｃｈａｆｔ
ドイツ連邦共和国　Ｄ－80333　ミュンヘン　ヴィッテルスバッハープラッツ　２
(72)発明者　エルヴィン　ヘス
ドイツ連邦共和国　オットーブルン　ゴットフリート－ケラー－シュトラーセ　36
(72)発明者　パスカーレ　ゼルフ
ドイツ連邦共和国　ミュンヘン　ヴィルヘルムー－ヘイーシュトラーセ　16
(74)代理人　弁理士　矢野　敏雄　（外４名）
Ｆターム(参考)　5J104 AA09 JA25 JA29 LA06 NA16

(54)【発明の名称】　擬似乱数の形成方法および電子署名方法

(57)【要約】
本発明は擬似乱数を形成する方法および電子署名方法に関する。本発明の擬似乱数の形成方法では、少なくとも２つの点を少なくとも２つの異なる楕円曲線上で求め、当該の点を結合することにより擬似乱数を形成する。異なる楕円曲線の点を１つの擬似乱数として結合することにより、形成された擬似乱数から個々の楕円曲線を推論することは不可能である。これにより本発明の方法による暗号化手段のセキュリティは著しく高められる。なぜなら離散的対数の計算が不可能となるからである。



【特許請求の範囲】

【請求項１】　少なくとも２つの点（Ｐ，Ｐ’）を有限体（ＧＦ）上の少なくとも２つの異なる楕円曲線（Ｅ，Ｅ’）から求め、該少なくとも２つの点（Ｐ，Ｐ’）を結合することにより擬似乱数を形成する、
ことを特徴とする擬似乱数の形成方法。

【請求項２】　擬似乱数を形成するために１組の点（Ｐ，Ｐ’）を求め、個々の組を求める際に当該のそれぞれ２つの楕円曲線（Ｅ，Ｅ’）を用いる、請求項１記載の方法。

【請求項３】　２つの楕円曲線（Ｅ，Ｅ’）は相互に同種である、請求項２記載の方法。

【請求項４】　第１の組の点（Ｐ，Ｐ’）を２つのスタート値（ｓ，ｓ’）に依存して求める、請求項１から３までのいずれか１項記載の方法。

【請求項５】　スタート値（ｓ，ｓ’）を予め定められた規則にしたがって変化させることにより別の組の点（Ｐ，Ｐ’）を求める、請求項４記載の方法。

【請求項６】　楕円曲線および／または点（Ｐ，Ｐ’）を予め定められた規則にしたがって変化させることにより別の組の点（Ｐ，Ｐ’）を求める、請求項１から４までのいずれか１項記載の方法。

【請求項７】　乱数を求めるために２つの点（Ｐ，Ｐ’）の座標を相互に結合する、請求項１から６までのいずれか１項記載の方法。

【請求項８】　２つの点（Ｐ，Ｐ’）のｘ座標を相互に結合し、その際に２つの楕円曲線（Ｅ，Ｅ’）を同種である、請求項１から７までのいずれか１項記載の方法。

【請求項９】　有限体ＧＦ（ｐ）上の楕円曲線（Ｅ，Ｅ’）の点群（Ｅ（ＧＦ（ｐ）），Ｅ’（ＧＦ（ｐ））は少なくとも2^{100}、有利には少なくとも2^{130}の群の次数（ｑ，ｑ’）を有する、請求項１から４までのいずれか１項記載の方法。

【請求項１０】　楕円曲線は有限体ＧＦ（ｐ）上に定義されており、ここでｐは３よりも大きい素数である、請求項１から９までのいずれか１項記載の方法。

【請求項１１】　乱数に基づく鍵を形成する楕円曲線ベースの電子署名方法において、請求項１から１０までのいずれか１項記載の乱数の形成方法により乱数を求める、

ことを特徴とする楕円曲線ベースの電子署名方法。

【請求項１２】　請求項１１記載の楕円曲線ベースの電子署名方法を実施する装置において、

有限体（ＧＦ（ｐ））上の楕円曲線（Ｅ，Ｅ’）の点群内で乗法を行う装置と、署名装置と、請求項１から９までのいずれか１項記載の擬似乱数の形成方法により擬似乱数を形成する装置とを有しており、

前記署名装置および前記擬似乱数を形成する装置は前記乗法を行う装置を使用する、

ことを特徴とする楕円曲線ベースの電子署名方法を実施する装置。

【発明の詳細な説明】

【０００１】

本発明は擬似乱数の形成方法および電子署名方法に関する。

【０００２】

乱数はメッセージを暗号化したりメッセージに署名したりするための暗号技術で必要とされるものである。文献 Otto Leiberich, "Vom diplomatischen Code zur Falltuerfunktion", Jun.1999, 26頁～34頁にはドイツ連邦共和国における暗号技術の発展について記載されている。ここにはかつて使用されていた記号列プロセスが説明されており、このプロセスでは内部構造を有さないきわめて長い記号シーケンス、いわゆるキャラクタワームまたはキャラクタストリームが記号ごとに暗号化すべき平文のメッセージへ付加されていた。文字が存在する場合、これらはまずａ＝０，ｂ＝１，．．．．，ｚ＝２５という所定のスキーマにしたがって数字へ変換される。２５より大きな数は生じないので、モジュロ２６での加法が行われる。コンピュータ時代になるとテクストは２進数へ変換され、０および１がモジュロ２で加法されるようになった。受信機は受信された秘密文からキャラクタストリームを（モジュロ２６またはモジュロ２で）減算し、これにより平文を得る。

【０００３】

キャラクタストリームは乱数発生器を用いて形成される。乱数発生器は以前には特定の管、いわゆるサイラトロンの高周波数の電圧変動を基礎としていたが、後に放射性崩壊現象を基礎とするようになった。

【０００４】

ただしキャラクタストリームをそれぞれ送受信機間でパラレルに確実に伝送しなければならないので、このプロセスでは大きな流量で確実にデータ伝送することが必要となる。

【０００５】

したがって擬似乱数を形成する手法、いわゆる擬似乱数発生器が開発され、鍵に依存してほぼ任意の長さの擬似乱数列を形成できるようになった。これによれば上述の符号化法でも通信相手との間の唯一の鍵のみを秘密に伝達すればよいの

で、そのつど完全なキャラクタストリームを伝達する手法よりも格段に簡単に扱うことができる。

【０００６】

こんにちの公開ネットワーク、例えばインターネットに対して、はじめて相互に通信しようとする２者が暗号化されたメッセージを送信できるプロセスが開発されている。このプロセスはいわゆる非対称鍵プロセスであり、公開鍵法とも称され、受信者に対していわゆる公開鍵を公開する。

【０００７】

この種の周知の手法の１つにいわゆるＲＳＡ法があり、ここでは鍵の各成分、いわゆる鍵モジュールは２つの大きな素数の積である。メッセージの送信者は鍵モジュールすなわち積のみを知っており、所定の数学的関数にしたがってメッセージを暗号化する。ただしメッセージを復号化するには積の知識のみでは不充分であり、２つの素数が必要である。これらの素数および相応の逆関数により、鍵を形成した正当な受信者のみにしか暗号化されたメッセージを復号化できない。

【０００８】

鍵モジュールをその約数つまり２つの素数へ分解することは、モジュールが大きければ通常の計算コストでは事実上不可能である。Johannes Buchmann, "Faktorisierung grosser Zahlen", Spektrum der Wissenschaft, Sep.1996 80頁～88頁には、大きな数の素因数分解の問題が詳細に説明されており、１２９桁の数を分解する際のコストが示されている。この数はコンピュータを使用した６００人のボランティアにより個々の素数へ分解されている。

【０００９】

ＲＳＡ法の欠点はメッセージの暗号化にきわめて時間がかかることである。なぜなら充分なセキュリティを保証するには非常に大きな数（２進で約１０００桁または１０進で約３００桁）を使用しなければならないからである。このように大きな数と別の同様に大きな次数の数とを相乗しなければならないので、伝送すべきデータの暗号化は充分に迅速には行えない。したがってＲＳＡ法は、本来の暗号化を行う従来のプロセスに対して秘密保持を要する鍵の暗号化伝送の目的のみに使用される。

【００１０】

ＲＳＡ法に代えて、楕円曲線に基づくプロセスが開発されている。暗号技術では有限体上の楕円曲線のみを扱う。有限体上の楕円曲線は加法および乗法で定義される点群を形成しており、この加法および乗法は通常の加法および乗法と計算規則以外の共通性を有さない。有限体上の楕円曲線での乗法は一方向性関数であり、反転（いわゆる離散的対数計算）が通常のケースでは計算技術的に実行不能である。これに対して通常の乗法はきわめて簡単かつ迅速に行うことができる。この事実は受信者が乱数ｔを選択し、当該の乱数ｔおよび楕円曲線でのｔとの乗法に基づいてカーブポイントＴを求めることにより楕円曲線ベースの暗号化プロセスで利用される。カーブポイントＴは鍵として公開されており、これに対して乱数ｔは受信者にとっては秘密に保持される。送信者はカーブポイントＴを用いてメッセージを暗号化し、これはカーブポイントＴに基づく乱数ｔを知っている受信者のみにしか復号化できない。

【００１１】

楕円曲線ベースのこの種のプロセスはＲＳＡプロセスと同程度のセキュリティに対して格段に僅かな計算能力しか要しない。このプロセスはマイクロコンピュータ、例えばチップカード内に組み込まれる。シーメンス社は商標ＳＬＥ４４ＣＲ８０Ｓのチップカードを扱っており、このカードには楕円曲線ベースの署名プロセスが組み込まれている。

【００１２】

受信者に公開する公開鍵と相応の秘密鍵とを形成する際にも乱数が必要となる。

【００１３】

したがって本発明の課題は、楕円曲線ベースで擬似乱数を形成する簡単かつ迅速な方法を提供し、質の高い大量の乱数を形成できるようにすることである。

【００１４】

この課題は本発明の請求項１記載の特徴を有する方法により解決される。

【００１５】

さらに本発明の課題は、楕円曲線ベースでの電子署名方法およびその装置を提

供し、周知の楕円曲線ベースの電子署名方法および電子署名装置よりもメモリスペースが少なく、小さな計算装置（例えばチップカード）に組み込めるようにすることである。

【００１６】

この課題は本発明の請求項１１記載の特徴を有する方法、および本発明の請求項１２記載の特徴を有する装置により解決される。

【００１７】

本発明の有利な実施形態は従属請求項に記載されている。

【００１８】

本発明の請求項１の擬似乱数の形成方法では、有限体上の少なくとも２つの異なる楕円曲線に存在する１組の点を求め、それぞれの組の点に依存して乱数を求める。

【００１９】

本発明によれば、２つの異なる楕円曲線が利用されており、擬似乱数が１組の点から導出されるが、ここでこの１組の２つの点は異なる楕円曲線上にあるので、このようにして求められた擬似乱数からカーブポイントを推論することはできない。擬似乱数の形成に唯一の楕円曲線しか使用されない場合には、離散的対数計算により擬似乱数からカーブポイントを推論しうる。これにより第３者が擬似乱数のための計算規則を求めて別の擬似乱数を予測してしまう可能性がある。このためセキュリティの大きな危険が発生するが、これは本発明を用いれば回避される。

【００２０】

電子署名に対する本発明の方法は、周知の署名プロセスと本発明の擬似乱数の形成プロセスとを組み合わせたものである。同じルーチンないし装置が署名プロセスにおいても乱数形成プロセスにおいても使用され。これにより著しくプログラムコードおよびメモリスペースを節約することができる。さらにＥＣアリスメティク（楕円曲線算法）の最適化は擬似乱数を形成する際にも署名プロセスを直接に実行する際にも有利である。楕円曲線ベースのルーチンおよび装置を２重に使用することにより、相乗効果が達成される。

【００２１】

さらに本発明により形成された擬似乱数は真の乱数発生器の乱数と異なるものではなく、比較的僅かな計算コストで形成することができる。

【００２２】

本発明を以下に図示の実施例に則して詳細に説明する。図１には概略的に実数上の楕円曲線が示されている。図２には概略的に有限体上の楕円曲線が示されている。図３には概略的に実数上の楕円曲線の２つの点が加法される様子が示されている。図４には概略的に１７個の点を備えた周期群を形成するモジュロ１３の体上の楕円曲線$y^2 = x^3 + 2x + 9$の点が示されている。図５には概略的に本発明の実施例の方法シーケンスがフローチャートで示されている。図６には概略的に本発明の擬似乱数の形成方法の基本原理がフローチャートで示されている。図７には概略的に本発明の電子署名方法を実行するプログラムの構造が示されている。

【００２３】

まず簡単に楕円曲線計算のための数学的基礎を説明する。体Ｋ上の楕円曲線は３次の式

$y^2 = x^3 + ax + b$

によって記述される曲線である。ここでａ，ｂはＫから成り、$4a^3 + 27b^2 \neq 0$である。組（ｘ、ｙ）はＫ×Ｋから成り、上述の式を満足する。また形式的な組（∞，∞）をＫ上の曲線Ｅの点と称する。

【００２４】

実数上の楕円曲線が図１に示されている。ここから楕円曲線が楕円でないことが見て取れる。

【００２５】

図２には有限体上の楕円曲線が示されている。代数の概念“体”とは有理数から既知の形式的な計算規則にしたがって加減乗除可能な“数の領域”として定義される。無限体、例えば有理数、実数、複素数と有限体とが存在する。有限体は例えばｐが素数であるモジュロｐの数の体ＧＦ（ｐ）であるか、または長さｎの２進ベクトルの体ＧＦ（2^n）である。ＧＦとは“ガロアフィールド”を表して

おり、これは有限体と同義語である。暗号技術では有限体上の楕円曲線のみが扱われる。

【００２６】

図３には実数上の楕円曲線の２つの点P_1，P_2の加法が示されており、ここから点P_3が生じている。この加法では点P_1，P_2の結合直線が形成され、楕円曲線との第３の交点が求められる。この交点はｘ軸反転され、P_1，P_2の加算の結果P_3が生じる。

【００２７】

楕円曲線上の点の加法は次式により表される。

【００２８】

$x_3 = r^2 - x_1 - x_2$

$y_3 = r(x_1 - x_3) - y_1$

$x_1 \neq x_2$のとき$r = (y_2 - y_1)/(x_2 - x_1)$

$P_1 = P_2$のとき$r = (3x_1^2 + a)/2y_1$

ここでx_i，y_iは点P_i（$i = 1, 2, 3$）の座標である。

【００２９】

これらの式は有限体上の楕円曲線についても成り立つ。

【００３０】

点の加法を反復することによりカーブポイントと整数ｋとの乗法が定義される。すなわち

$k * P = P + P + \ldots + P$（ｋ倍の和）

である。

【００３１】

カーブポイントと整数との乗法は簡単かつ迅速に実行可能であるが、これに対して反転のタスク、すなわちいわゆる離散的対数計算は一般には厖大な計算コストをかけない限り解くことはできない。これに対する準指数時間のアルゴリズムは存在しない。したがってこの点の乗法は一方向性関数であるので、いわゆる公開鍵プロセスで使用される。

【００３２】

以下に図５に示されている実施例に則して本発明による擬似乱数の形成方法を説明する。

【００３３】

体ＧＦ（ｐ）上の第１の楕円曲線Ｅは次式によって与えられる。すなわち

$(y^2)\ mod\ p = (x^3 + 6x +$

$6050679034418465473882149660454552069529384067 71)\ mod\ p$

ここで$p = 2^{160} - 47 =$

1461501637330902918203684832716283019655932542929

であり、ｐは１６０bitの素数である。

【００３４】

ＧＦ（ｐ）上の楕円曲線Ｅは群の次数として

＃Ｅ（ＧＦ（ｐ））＝７＊ｑ

を有しており、

ｑ＝208785948190128988314812461240940947434505754881

であり、ｑは１２８bitの素数である。

【００３５】

楕円曲線の群の次数は点群の要素の数であり、したがって体ＧＦ（ｐ）上の楕円曲線Ｅの定義式の解の数である。群次数の素数の最大約数が大きくなるにつれて、離散対数計算も困難となる。群次数およびその素数の最大約数の大きさは本発明の方法の品質の指標である。ここで群の次数は少なくとも2^{100} または有利には2^{130} でなければならない。

【００３６】

体ＧＦ（ｐ）上の第２の楕円曲線Ｅ’は次式により与えられる。すなわち

$(y^2)\ mod\ p = (x^3 + 3x +$

$1687563857404985474001529233182001487121493639 91)\ mod\ p$

である。

【００３７】

曲線Ｅ’は曲線Ｅに対して同種である。つまり曲線Ｅが

$y^2 = x^3 + ax + b$

の形状を有するとき、曲線Ｅ’は

$y^2 = x^3 + ac^2 x + bc^3$

の形状を有する。ここでａ，ｂ，ｃはＧＦ（ｐ）から成り、ｃはモジュロｐの平方非剰余である。この実施例ではｃについて

ｃ＝503145425704462245322517599589013227703324936803

が相当する。

【００３８】

２つの任意の曲線に代えて２つの同種の曲線を使用することにより重要な利点が得られる。ＧＦ（ｐ）上の楕円曲線Ｅ’の次数は簡単に楕円曲線Ｅの群の次数から導出できる。なぜなら２つの次数の和は２ｐ＋２であるので、式

＃Ｅ’（ＧＦ（ｐ））＝２ｐ＋２－＃Ｅ（ＧＦ（ｐ））

が成り立つからである。

【００３９】

この実施例ではＥ’の群の次数に対して

＃Ｅ’（ＧＦ（ｐ））＝２ｐ＋２－＃Ｅ（ＧＦ（ｐ））＝１１＊１９＊ｑ’

が得られ、ここで

ｑ’＝4581509834893112596249788202965452687367789347

であり、ｑ’は１５２bitの長さの素数である。

【００４０】

曲線Ｅ，Ｅ’の２つの点Ｐ，Ｐ’は例えば

Ｐ（27，1199480719563308855489368355308026541006624847440）

Ｐ’（318，767790262932904318810390534329377261151321453045）

に選定され、２つのスタート値ｓ，ｓ’は例えばｓ＝ｓ’＝２に選定される。

【００４１】

楕円曲線Ｅ，Ｅ’、点Ｐ，Ｐ’、およびスタート値ｓ，ｓ’を求めることにより、図５のステップＳ１が終了する。方法シーケンスはステップＳ２へ移行し、ここでは点Ｐ，Ｐ’とスタート値ｓ，ｓ’とが乗算される。結果はＰＡ，ＰＡ’として表される。乗法はｓ回の加法またはｓ’回の加法として図３に示されている加法にしたがって行われる。

【００４２】

点ＰＡ、ＰＡ’はランダムビットを求める規則（Vorschrift）の個所へ引き渡される（ステップＳ３）。この実施例では２つの点ＰＡ、ＰＡ’のｘ座標はＸＯＲで結合され、ｃにより除算される。

【００４３】

同種の楕円曲線Ｅ，Ｅ’では次のことが成り立つ。ＧＦ（ｐ）からの任意のｘについてｘは楕円曲線Ｅ上の異なる２点のｘ座標であるか、またはｘは楕円曲線Ｅ上の１点のｘ座標である。ｃｘは楕円曲線Ｅ’上の１点のｘ座標であるか、またはｘが楕円曲線Ｅ上の１点のｘ座標ではなくｃｘが楕円曲線Ｅ’上の２点のｘ座標である。このｘ座標がｃで除算されると、ＧＦ（ｐ）からの任意の全てのｘはｘ座標のちょうど２ｘ倍となる。つまり楕円曲線Ｅ上のｘ座標とｃで除算された楕円曲線Ｅ’上のｘ座標とが結合されると、０からｐ－１までの間の２つの任意の乱数値を結合することと等価となる。これにより導出される擬似乱数ビットは真のランダムビットとしての特性を有する。

【００４４】

ステップＳ２から点ＰＡ，ＰＡ’はステップＳ４へ引き渡される。このステップでは点Ｐ，Ｐ’は不変のままであり、ｓ，ｓ’はそれぞれ１だけ高められる。

【００４５】

ステップＳ４から方法シーケンスは再びステップＳ２へ戻る。ここで新たな点ＰＡ，ＰＡ’が形成され、別のランダムビットの計算のためにステップＳ３へ引き渡され、さらにステップＳ４へ送出される。この方法シーケンスは複数回反復可能であり、つねに新たなランダムビットを形成することができる。

【００４６】

出願人は本発明の上述の乱数形成方法により２０×１００万ランダムビットの乱数を形成し、これらのランダムビットを種々の統計的検査にかけた。検査によれば、これらの真のランダムビットに偏差は検出されなかった。

【００４７】

本発明にとって重要なのは、ステップＳ３で乱数Ｚが２つの点ＰＡ，ＰＡ’から求められ、これらが異なる楕円曲線Ｅ，Ｅ’に由来することである。これら２

つの点ＰＡ，ＰＡ’を結合することにより、形成された擬似乱数に則して点ＰＡ，ＰＡ’に基づき点Ｐ，Ｐ’を離散対数計算で求められなくなることが保証される。したがってステップＳ３の結果から点ＰＡ，ＰＡ’を形成する方法をステップＳ１、Ｓ２、Ｓ４によって推論することはできない。このことは図５の破線によって示されている。

【００４８】

本発明は図５に示されている実施例には限定されない。本発明の範囲では、例えばステップＳ３においてｘ座標の別の結合を選定することができる。例えば２つのｘ座標をモジュロｐの加法により相互に結合することができる。またはｙ座標を結合してもよい。またｘ座標およびｙ座標を結合することもできる。また本発明の範囲で点Ｐ，Ｐ’を有する固定に設定された楕円曲線Ｅ，Ｅ’に代えてＰＡ，ＰＡ’の計算後に新たな曲線E^{*}，E^{*}’、P^{*}，P^{*}’を求め、これを次の点PA^{*}，PA^{*}’の計算の際に利用することができる。値ｓ，ｓ’もそれ自体で任意に変更することができる。本発明に取って重要なのは、値ｓ，ｓ’が整数であるということのみである。これらの値は本発明の方法の開始時に例えば簡単な乱数発生器によって形成されればよく、高い要求を満足する必要はない。

【００４９】

図６には本発明の方法の基本原理が示されている。この方法はステップＳ５、Ｓ６からなるループを有しており、ここでステップＳ５では２つの曲線および２つのスタート値ｓ，ｓ’上の２つの楕円曲線Ｅ，Ｅ’、２つの点Ｐ，Ｐ’、が選定される。ステップＳ６では点Ｐ，Ｐ’とｓ，ｓ’とが乗算され、ここからＰＡ，ＰＡ’が得られる。ループＳ５、Ｓ６を反復するたびにＥ，Ｅ’、Ｐ，Ｐ’、ｓ，ｓ’のうち少なくとも１組が変更される。またこれらのうち２組、または３組全てを予め定められた規則にしたがって変更してもよい。

【００５０】

ループを反復するたびに新たな数値の組ＰＡ，ＰＡ’が形成され、方法ステップＳ７へ引き渡される。このステップでは２つの点ＰＡ，ＰＡ’がそのつど１つの擬似乱数Ｚへ結合される。

【００５１】

楕円曲線ベースのプロセスは一方向性関数として楕円曲線上での乗法を使用しているので、このプロセスを実行する装置には楕円曲線上のアリスメティクのためのルーチンおよび装置が設けられている。このプロセスはさらに秘密鍵および公開鍵を形成するための乱数を必要とする。本発明の乱数形成方法を使用することにより質の高い擬似乱数を形成して、しかもプログラムコードを小さく保つことができる。なぜなら既存のルーチンを２重に使用することができるからである。これによりリソースが著しく節約され、同時にプロセスのセキュリティが格段に向上する。

【００５２】

図７には概略的に本発明の方法を実施するプログラムの構造がブロック回路図で示されている。このプログラムは署名プロセスを実行するプログラムセクションＰ１と、有限体上の楕円曲線の乗法を行うプログラムセクションＰ２とから成っている。プログラムセクションＰ１には別のプログラムセクションＰ３から乱数が供給され、ここでプログラムセクションＰ３はさらに楕円曲線での乗法を行うプログラムセクションＰ２に依存している。プログラムセクションＰ１にはデータ入力流Ｉおよびデータ出力流Ｏが示されている。ここでデータ入力流は署名すべきメッセージであり、データ出力流は署名である。さらにプログラムセクションＰ１はデータ出力流Ｏに秘密鍵および公開鍵を出力する。プログラムセクションＰ１の関数はそれ自体周知の楕円曲線ベースの署名プロセスおよび署名装置に相応している。

【００５３】

本発明の方法は有利には計算容量の比較的小さい計算装置、例えばチップカードで使用することができる。これは相応のプログラムコードがきわめてコンパクトであり、処理すべき数の長さが同じセキュリティレベルのＲＳＡプロセスの場合と比べて格段に短いためである。ただしこのプログラムを電子読み取り可能なデータ担体上で動かすこともできる。

【図面の簡単な説明】

【図１】

実数上の楕円曲線を示す図である。

【図２】

有限体上の楕円曲線を示す図である。

【図３】

実数上の楕円曲線の２つの点が加法される様子を示す図である。

【図４】

ｍｏｄ１３の体上の楕円曲線$y^2 = x^3 + 2x + 9$の点を示す図である。

【図５】

本発明の実施例の方法シーケンスのフローチャートである。

【図６】

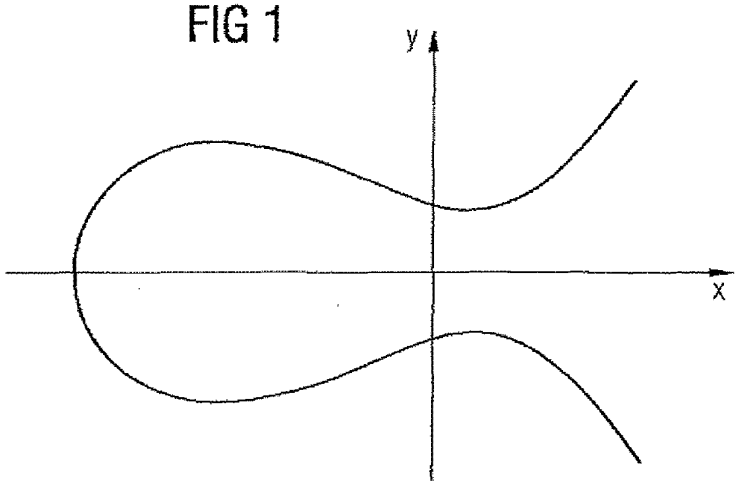
本発明の擬似乱数の形成方法の基本原理のフローチャートである。

【図７】

本発明の電子署名方法を実行するプログラムの構造を示す図である。

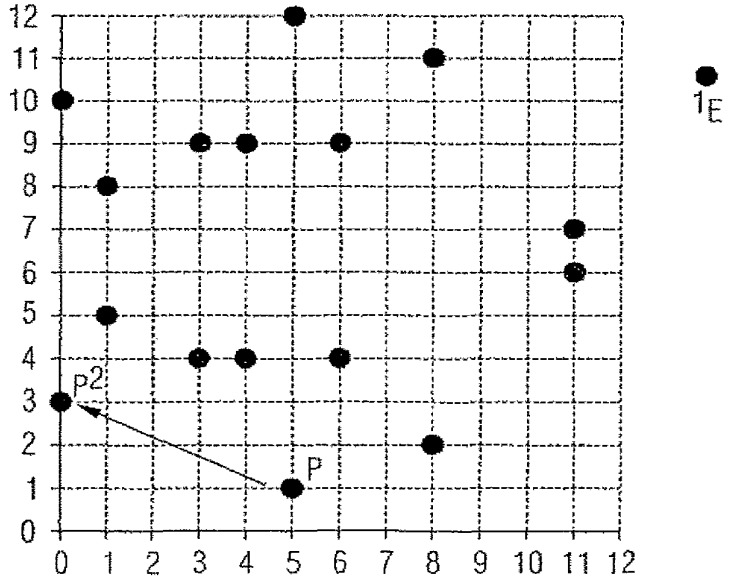
【図１】

FIG 1



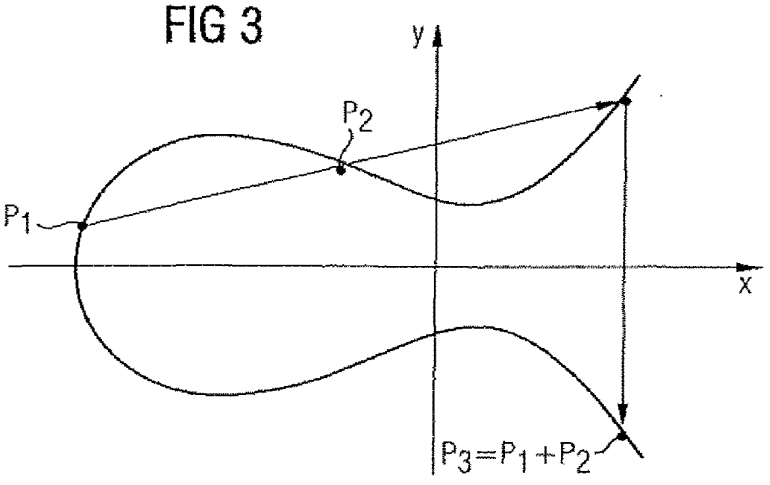
【図２】

FIG 2



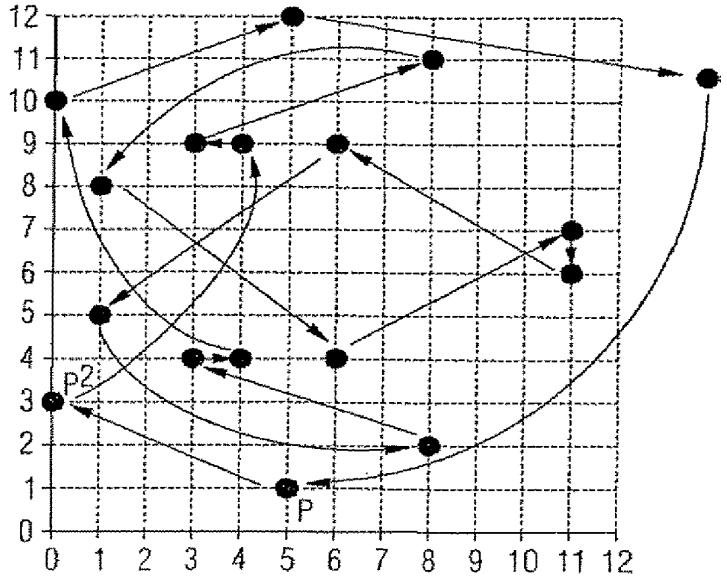
【図３】

FIG 3



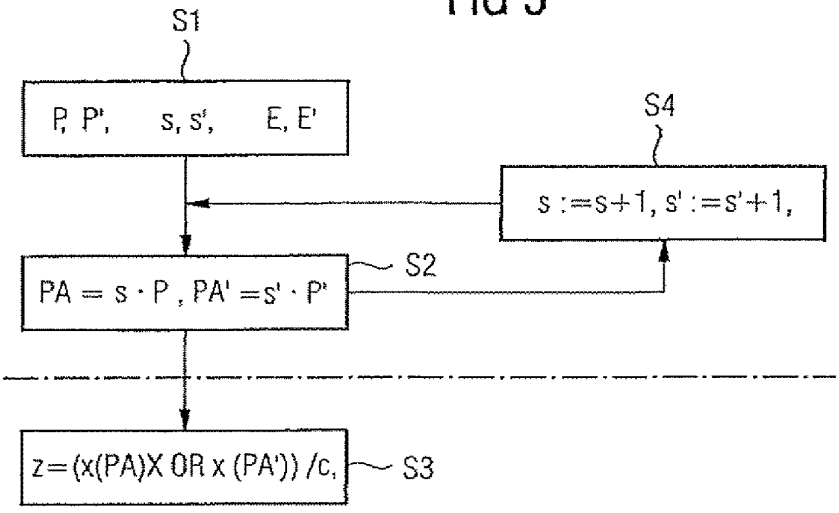
【図４】

FIG 4



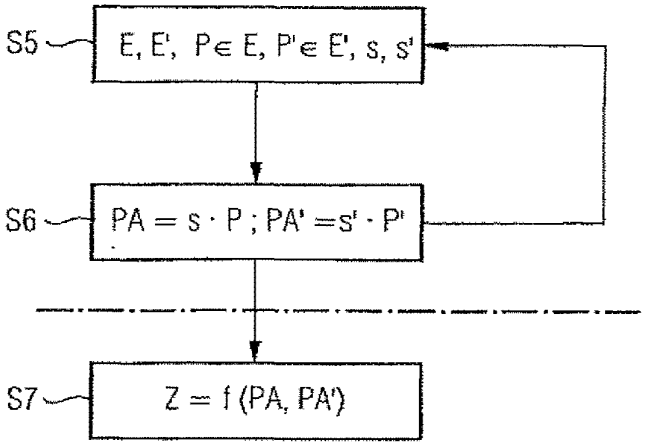
【図５】

FIG 5



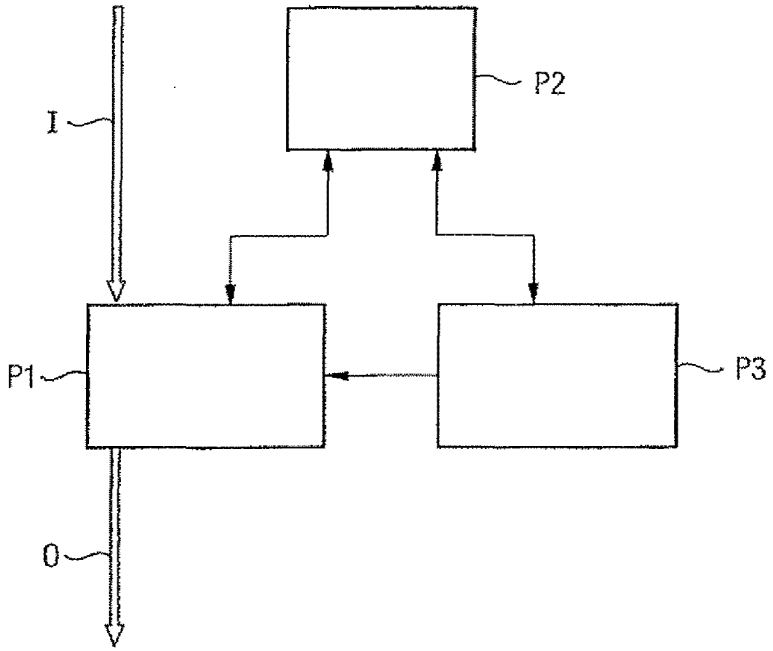
【図６】

FIG 6



【図７】

FIG 7



【国際調査報告】

INTERNATIONAL SEARCH REPORT

Intern. nal Application No
PCT/DE 00/02776

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58 H04L9/32 //G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H03K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KALISKI B S JR: "One-way permutations on elliptic curves" JOURNAL OF CRYPTOLOGY, 1991, USA, vol. 3, no. 3, pages 187-199, XP000972491 ISSN: 0933-2790 page 187, paragraph 1 page 188, paragraph 7 page 194, paragraph 2 -page 196, paragraph 1	1-12
X	KALISKI B S: "A PSEUDO-RANDOM BIT GENERATOR BASED ON ELLIPTIC LOGARITHMS" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 6, 1986, pages 84-103, XP000090665 page 98, line 20 - line 33	1-12

☐ Further documents are listed in the continuation of box C. ☐ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 December 2000	20/12/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer Verhoof, P

Form PCT/ISA/210 (second sheet) (July 1992)

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	Michael K. Henry/Paige Nordell
Attorney Docket Number:	67539/622

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	1202	8	52	416
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**596**

Electronic Acknowledgement Receipt

EFS ID:	11036990
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Paige Nordell
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	67539/622
Receipt Date:	23-SEP-2011
Filing Date:	23-JAN-2006
Time Stamp:	16:55:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$596
RAM confirmation Number	7662
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		SupplAmendment.pdf	98540 3050a91f88db80faf05c42ec477d083e9e327744	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Supplemental Response or Supplemental Amendment	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	10

Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	34459 8a22d7942d055758b07f01278639b5c35ef2ef3a	no	5
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	JP2003507761.pdf	1034866 861e43bc4c11e194e0ac660c339d7738de7f28d8	no	20
Warnings:					
Information:					
4	Non Patent Literature	ANSX9-62.pdf	6843127 bc93891bd8c6972989a2ce3e4e70219845c1e55d	no	163
Warnings:					
Information:					
5	Non Patent Literature	ANSIX9-82Part3forX9F1.pdf	780434 047f15c4c812438fc11f5b18b1041f34bf4eedce	no	175
Warnings:					
Information:					
6	Non Patent Literature	ANSX9-82-1.pdf	792418 84e71046e9def6b10c9fad68fec8055d6d51f7a7	no	189
Warnings:					
Information:					
7	Non Patent Literature	Barker-1.pdf	514700 a23991914a1b170ce09d26d6eff812777d6f28d0	no	130
Warnings:					
Information:					

8	Non Patent Literature	BarkerRevised-1.pdf	472234 c130aeb29dc35369646d4790b65fd39dd37ddaa4	no	133
Warnings:					
Information:					
9	Non Patent Literature	Blum.pdf	2715148 b5a01a7e9546857f93ce3fac02798fd39130d83f	no	15
Warnings:					
Information:					
10	Non Patent Literature	Brown.pdf	205980 34cda3d973280bfcdf39aa1f4f09653c4b13e045	no	14
Warnings:					
Information:					
11	Non Patent Literature	ELMahassni.pdf	1737373 632e3ea232b608f57630cdd1c9a6948c81451d24	no	10
Warnings:					
Information:					
12	Non Patent Literature	Documentcryptography.pdf	13654399 83d8cb2086c9884ca26bc1b70db34e5a40884695	no	162
Warnings:					
Information:					
13	Non Patent Literature	Gjoesteen.pdf	139815 50145d5a8dba45bb5d560f03724b28cd96b6b20e	no	8
Warnings:					
Information:					
14	Non Patent Literature	Guerel.pdf	126833 f9e0c9054cb6066f7efd9ca4d3d2dfef4f69443b	no	9
Warnings:					
Information:					
15	Non Patent Literature	Luby.pdf	2212140 71a0321507dcfc3fec1e8bee1564ec66fc07eaf6	no	15
Warnings:					
Information:					
16	Fee Worksheet (SB06)	fee-info.pdf	32097 223338fc055d13358c4ec5137127ea79e6314b3f	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	31394563

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/336,814	01/23/2006	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
FOR	NUMBER FILED	NUMBER EXTRA					
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 09/23/2011

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 43	Minus	** 57	= 0	X $ =		OR	X $52=	0
Independent (37 CFR 1.16(h))	* 3	Minus	***4	= 0	X $ =		OR	X $220=	0
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/MINNIE JACKSON/

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001

	1	Office Action received in Japanese Patent Application No. 2007-551522, issued on August 19, 2011, with English translation, 19 pages total.	☒
	2		☐
	3		☐
	4		☐
	5		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Henry/	Date (YYYY-MM-DD)	2011-09-29
Name/Print	Michael K. Henry	Registration Number	59516

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	11075773
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Susan Johnson
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	67539/622
Receipt Date:	29-SEP-2011
Filing Date:	23-JAN-2006
Time Stamp:	12:20:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	29717-0048001_InfoDisclosure Statement.pdf	31394 37dc7902d4788f834cab2c35b6cf5861a2c9bc45	no	4

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	JPOAandEnglishtranslation.pdf	689885 96dab82015fed90ae406e291b9d13f9308af995a	no	19
Warnings:					
Information:					
			Total Files Size (in bytes):	721279	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

94149 7590 10/20/2011

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER	
LAKHIA, VIRAL S	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
10/20/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *VIRAL LAKHIA*.

(2) *SYED ZIA*.

(3) *MICHAEL HENRY*.

(4) _____.

Date of Interview: *13 October 2011*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☒101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: _____.

Identification of prior art discussed: _____.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative and Examiner discussed the 101 issue and general background of the invention. Applicant's representative agreed to amend the claims to overcome the 101 issues and examiner agreed to conduct focused search on amended claims on 9/23/2011. .

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Viral S Lakhia/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit	: 2431
Serial No.	: 11/336,814	Examiner	: Viral S. Lakhia
Filed	: January 23, 2006	Conf. No.	: 1834
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Examiner Interview Summary

Applicants note and appreciate the courtesy of the Examiner interview conducted by telephone on October 13, 2011. Examiner Viral Lakhia, Supervisory Patent Examiner Syed Zia, and Applicants' representative Michael Henry participated in the interview. The Examiners expressed their concern that the claims in the Supplemental Amendment dated September 23, 2011 may not comply with 35 U.S.C. § 101. The Examiners further indicated that the claims appear to include subject matter that would be allowable over the art of record and noted further search would be necessary. The undersigned stated the Applicants' position that the claims in the Supplemental Amendment do comply with § 101, and Applicants would consider further amendments in order to address the Examiners' concerns and move prosecution forward. No further agreement was reached during the Examiner interview.

Respectfully submitted,

Date: November 18, 2011

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Electronic Acknowledgement Receipt

EFS ID:	11436850
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Susan Johnson
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	67539/622
Receipt Date:	18-NOV-2011
Filing Date:	23-JAN-2006
Time Stamp:	10:02:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant summary of interview with examiner	29907-0037001_ExaminerInterviewSummary.pdf	44911 b8559e10aece0eac09c79fc9f5c5b8c763420f0c	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	44911

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PLUS Search Results for S/N 11336814, Searched Tue Mar 06 10:41:40 EST 2012

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

20070189527 99
20040098436 62
5442707 71
6078667 71
6088798 71
6263081 71
6307935 71
6341349 71
7308469 71
7853012 71
7936874 71
7936874 71
20030072443 71
20040228478 71
20060285682 71
20070121933 71
20080080710 71
5271061 62
5463690 62
5581616 62
5805703 62
6049610 62
6195433 62
6285760 62
6345098 62
7023990 62
7680272 62
20040228484 62
20060126828 62
5955717 62
6611597 62
6704867 62
6738899 62
6847951 62
6876745 62
6910058 62
7127063 62
7218735 62
7512233 62
7593527 62
7680270 62
7853013 62
7869593 62
7912216 62
7936869 62
7869593 62
7912216 62
7936869 62
20030123668 62
20030152218 62

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

94149 7590 03/09/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER	
LAKHIA, VIRAL S	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/09/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *VIRAL LAKHIA*. (3)_____.

(2) *Michael Henry*. (4)_____.

Date of Interview: *05 March 2012*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☒101 ☐112 ☐102 ☐103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *68 and 83*.

Identification of prior art discussed: *No*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner and Applicant's representative discussed 101 issue to be amended in claim 83. Applicant's representative asked to issue the office action upon which they will make the appropriate changes upon confirmation with client .

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Viral S Lakhia/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *VIRAL LAKHIA*. (3)_____.

(2) *Michael Henry*. (4)_____.

Date of Interview: *05 March 2012*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☒101 ☐112 ☐102 ☐103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *68 and 83*.

Identification of prior art discussed: *No*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner and Applicant's representative discussed 101 issue to be amended in claim 83. Applicant's representative asked to issue the office action upon which they will make the appropriate changes upon confirmation with client .

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Viral S Lakhia/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

94149 7590 03/22/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER	
LAKHIA, VIRAL S	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
03/22/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 September 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *68-111* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☒ Claim(s) *68-82 and 85-111* is/are allowed.

7)☐ Claim(s) *83 and 84* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *23 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to application filed on 9/29/2011.

Claims 68 - 111 are examined.

Allowable Subject Matter

Claims 68 – 82 and 85 – 111 are allowed.

Response to Arguments

Applicant's arguments filed 9/29/2011 with respect to claims 68 – 111 have been considered and are persuasive.

Examiner would like to thank attorney Michael Henry for conversation regarding amendment and 101 issues on 3/5/2012.

Regarding claims 83 – 84 are rejected under USC 101.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 83 – 84 are moth claims that are not tied to another class of invention. These claims could be done without a mechine.

Examiner would like to request to amend the claims by adding computer / processor in the body of the claim limitation or to add storing mechanism of register for example in claim 68 and 85.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 83 - 84 are rejected under 35 U.S.C. 103(a) as being U.S. Publication 2006/0129800 to Lauter et al. (hereinafter known as "Lauter") and in view of U.S. Publication 2002/0044649 to Gallant et al. (hereinafter "Gallant").

As per claim 83 Lauter teaches, a computer-implemented method comprising:

obtaining a first input value that represents a first elliptic curve point;

obtaining a second input value that represents a second elliptic curve point;

generating a scalar multiple of said first elliptic curve point based on a secret value and said first input value;

generating an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

using said output value as a random number to achieve a specified level of security in a

cryptographic operation;

generating a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generating an updated secret value based on said scalar multiple of said first elliptic curve point; and

storing said updated secret value *(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033).*

Lauter does not teach however Gallant teaches, wherein one of said scalar multiples is used to derive said random number *(Gallant para 0054 – 0055).*

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gallant in Elliptical Curve Random Number Generation system comprising Random number generator with Elliptical Curve Cryptography system of Lauter by accelerating multiplication of an elliptical curve point by a scalar over a finite field. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to create a strong one-way function and to protect the random value.

Further examiner presumes for the purpose of this office action that cassels - tate pairings in Fig 1, para 0012 - similar to Weils pairing reads on multiple points (p,q) of the elliptical curve over a finite field with different properties like multiplicative and divisive properties over the finite field as known in the art at the time of invention. Additionally, Lauter and other cited reference have an inherent and well known functionality of scalar

multiplier of various points on ECC, x-coordinate value of points on ECC over finite fields, secret value in accordance with scalar multiplier are well known in the art and within the domain of cited references.

As per claim 84 combination of Lauter and Gallant teaches, the method of claim 83, wherein said one-way function includes a hash function (*(Lauter – Fig 1, 2, 3 and 4 – para 0029 – 0033)*.

Conclusion

Claims 83 - 84 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viral Lakhia whose telephone number is (571) 270 - 3363. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Viral S Lakhia/

Examiner, Art Unit 2431

/NATHAN FLYNN/

Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/336,814	Applicant(s)/Patent Under Reexamination BROWN ET AL.	
	Examiner VIRAL LAKHIA	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,542,568	06-2009	Ohmori et al.	380/201
*	B	US-7,480,795	01-2009	Vanstone, Scott A.	713/156
*	C	US-7,639,799	12-2009	Lauter et al.	380/30
*	D	US-7,092,979	08-2006	Shim, Jae-seong	708/250
*	E	US-2006/0285682	12-2006	Sarangarajan et al.	380/028
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	Art Unit
	VIRAL LAKHIA	4144

SEARCHED

Class	Subclass	Date	Examiner
380	28-30	6/17/09	V.L.
380	44-47	6/17/09	V.L.
380	277-286	6/17/09	V.L.
713	Search 713 with key word search of elliptic curve number generator	6/17/09	V.L.
726	Search 726 with key word search of elliptic curve number generator	6/17/09	V.L.
380	28-30	4.5.2011	V.L.
380	28/283-286		
713	171		

SEARCH NOTES

Search Notes	Date	Examiner
Key words and combination : elliptic curve number generator (creator, producer, intiator), message, digest, hash, random	7/17/09	V.L.
Get assistance with Fast and Focused Search department for the case	7/17/09	V.L
Get assistance from Peter Poltriak for claim interpretation and understanding of invention	7/17/09	V.L
Search Google Patents, NPL and wikipedia for elliptic curve technology	7/17/09	V.L
Update East with key word search	7/15/2010	V.L.
Update East with key word search.	4.6.2011	V.L.
Search INventor name for double patent issues.	4.6.2011	V.L.
Update East with key word search.	3/3/2012	v.l.
Search Google Patents, NPL and wikipedia for elliptic curve technology	3/3/2012	v.l.
Conduct plus search for independent claims	3/3/2012	v.l.
Examiner reached out to N.Flynn - T.Swann for 101 issue clarification, 101 rejection based on Todd Swan's comments.	3/5/2012	v.l.

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
380	277-286	3/3/2012	v.l.
380	28-30	3/3/2012	v.l.

/V. S. L./ Examiner.Art Unit 2431	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012			
	1	✓		÷		✓	-			
	2	✓		÷		✓	-			
	3	✓		÷		✓	-			
	4	✓		÷	✓	✓	-			
	5	✓		÷	✓	✓	-			
	6	✓		÷	✓	✓	-			
	7	✓		÷	✓	✓	-			
	8	✓		÷	✓	-	-			
	9	✓		÷	✓	✓	-			
	10	✓		÷	✓	✓	-			
	11	✓		÷	✓	✓	-			
	12	✓		÷	✓	-	-			
	13	✓		÷	✓	✓	-			
	14	✓		÷	✓	✓	-			
	15	✓		÷	✓	✓	-			
	16	✓		÷	✓	✓	-			
	17	✓		÷	✓	✓	-			
	18	✓		÷	✓	✓	-			
	19		✓	÷	-	-	-			
	20			÷	✓	✓	-			
	21			÷	✓	✓	-			
	22			÷	✓	✓	-			
	23			÷	✓	✓	-			
	24			÷	✓	✓	-			
	25			÷	✓	✓	-			
	26			÷	✓	✓	-			
	27			÷	✓	✓	-			
	28			÷	✓	✓	-			
	29			÷	✓	✓	-			
	30			÷	-	-	-			
	31			÷	-	-	-			
	32			÷	-	-	-			
	33			÷	-	-	-			
	34			÷	-	-	-			
	35			÷	-	-	-			
	36			÷	-	-	-			

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012			
	37					✓	-			
	38					✓	-			
	39					✓	-			
	40					✓	-			
	41					✓	-			
	42					✓	-			
	43					✓	-			
	44					✓	-			
	45					✓	-			
	46					✓	-			
	47					✓	-			
	48					✓	-			
	49					✓	-			
	50					✓	-			
	51					✓	-			
	52					✓	-			
	53					✓	-			
	54					✓	-			
	55					✓	-			
	56					✓	-			
	57					✓	-			
	58					✓	-			
	59					✓	-			
	60					✓	-			
	61					✓	-			
	62					✓	-			
	63					✓	-			
	64					✓	-			
	65					✓	-			
	66					✓	-			
	67					✓	-			
	68						=			
	69						=			
	70						=			
	71						=			
	72						=			

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012			
	73						=			
	74						=			
	75						=			
	76						=			
	77						=			
	78						=			
	79						=			
	80						=			
	81						=			
	82						=			
	83						✓			
	84						✓			
	85						=			
	86						=			
	87						=			
	88						=			
	89						=			
	90						=			
	91						=			
	92						=			
	93						=			
	94						=			
	95						=			
	96						=			
	97						=			
	98						=			
	99						=			
	100						=			
	101						=			
	102						=			
	103						=			
	104						=			
	105						=			
	106						=			
	107						=			
	108						=			

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012			
	109						=			
	110						=			
	111						=			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Receipt date: 09/29/2011	Application Number	11336814	11336814 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-01-23	
	First Named Inventor	Daniel R.L. Brown	
	Art Unit	2431	
	Examiner Name	Viral S. Lakhia	
	Attorney Docket Number	29717-0048001	

	1	Office Action received in Japanese Patent Application No. 2007-551522, issued on August 19, 2011, with English translation, 19 pages total.	☒
	2		☐
	3		☐
	4		☐
	5		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Viral Lakhia/	Date Considered	03/03/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Receipt date: 09/29/2011	Application Number	11336814	11336814 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-01-23	
	First Named Inventor	Daniel R.L. Brown	
	Art Unit	2431	
	Examiner Name	Viral S. Lakhia	
	Attorney Docket Number	29717-0048001	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Henry/	Date (YYYY-MM-DD)	2011-09-29
Name/Print	Michael K. Henry	Registration Number	59516

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Vanstone
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001/35404-US-PA

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
1	1	2003-507761	JP		2003-02-25	Siemens Aktiengesellschaft		☒

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Receipt date: 09/23/2011	Application Number	11336814 11336814 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-01-23
	First Named Inventor	Vanstone
	Art Unit	2431
	Examiner Name	Viral S. Lakhia
	Attorney Docket Number	29717-0048001/35404-US-PA

	1	ANS X9.62-2005; "Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA)"; November 16, 2005; 163 pages.	☐
	2	ANSI X9.82; "Part 3 - Draft" October 2003; 175 pages.	☐
	3	ANS X9.82; "Part 3 - Draft"; June 2004; 189 pages.	☐
	4	Barker, Elaine and John Kelsey; "Recommendation for Random Number Generation Using Deterministic Random Bit Generators"; NIST Special Publication 800-90; National Institute of Standards and Technology; December 2005; 130 pages.	☐
	5	Barker, Elaine and John Kelsey; "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)"; NIST Special Publication 800-90; National Institute of Standards and Technology; March 2007; 133 pages.	☐
	6	Blum, Manuel and Silvio Micali; "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits"; SIAM Journal on Computing; Vol. 13, No. 4; November 1984; pp. 850-864.	☐
	7	Brown, Daniel R.L.; "Conjecture Security of the ANSI-NIST Elliptic Curve RNG"; Cryptology ePrint Archive; Report 2006/117; March 29, 2006; 14 pages. Retrieved from the internet <http://eprint.iacr.org>.	☐
	8	El Mahassni, Edwin and Igor Shparlinksi; "On the Uniformity of Distribution of Congruential Generators over Elliptic Curves"; Sequences and Their Applications: Proceedings of SETA '01; 2002' pp. 257-264.	☐
	9	Goldreich, Oded; "Foundations of Cryptography Basic Tools'; Cambridge University Press; 2001; pages 30-183.	☐
	10	Gjoesteen, Kristian; "Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005"; March 16, 2006; 8 pages.	☐
	11	Guerel, Nicolas; "Extracting Bits from Coordinates of a Point of an Elliptic Curve"; Cryptology ePrint Archive; Report 2005/324; 2005; 9 pages. Retrieved from the internet <http://eprint.iacr.org>	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Receipt date: 09/23/2011	Application Number	11336814	11336814 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-01-23	
	First Named Inventor	Vanstone	
	Art Unit	2431	
	Examiner Name	Viral S. Lakhia	
	Attorney Docket Number	29717-0048001/35404-US-PA	

	12	Luby, Michael; "Pseudorandomness and Cryptographic Applications"; Princeton University Press; 1996; pp. 70-78.	☐
	13		☐
	14		☐
	15		☐
	16		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Viral Lakhia/	Date Considered	03/03/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Receipt date: 09/23/2011	Application Number	11336814 11336814 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-01-23
	First Named Inventor	Vanstone
	Art Unit	2431
	Examiner Name	Viral S. Lakhia
	Attorney Docket Number	29717-0048001/35404-US-PA

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Henry/	Date (YYYY-MM-DD)	2011-09-23
Name/Print	Michael K. Henry	Registration Number	59516

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S77	26	((two dual many plural) with (input$2 point$2)) with (random with generat$4) and ("ECC" (elliptical with curve)) and (number$2) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/05 07:06
S76	1	((two dual many plural) with (input$2 point$2)) with (random with generat$4) and (escrow seed) and ("ECC" (elliptical with curve)) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 12:34
S75	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) same (random with number) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/03/03 12:26
S74	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) same (random with number) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/03/03 12:25
S69	0	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) same (escrow hash$3) and @ad<"20050121" and 705/54-55.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:46
S68	3	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) same (escrow hash$3) and @ad<"20050121" and 713/155-158.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:46
S67	1	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) same (escrow hash$3) and @ad<"20050121" and 380/200-201.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:24
S66	10	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) same (escrow hash$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:21
S65	5	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) and (escrow hash$3) and @ad<"20050121" and 380/30.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:21
S64	1	(two) with (point$2) with (random with generat$4) and (ECC elliptical curve) and (escrow hash$3) and @ad<"20050121" and 380/30.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:14
S63	1	(two) with (point$2) with (random	US-PGPUB;	OR	ON	2012/03/03

		with generat$4) and (ECC elliptical curve) and (escrow hash$3) and @ad<"20050121" and 380/44.ccls.	USPAT; EPO; DERWENT; IBM_TDB			09:06
S62	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/03/03 09:05
S61	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 09:04
S60	0	((elliptical with curve) ("ecc")) same (first same second same point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 09:04
S59	0	((elliptical with curve) ("ecc")) same (first same second same hash$4) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 09:03
S58	51	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 09:02
S57	27	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3) and @ad<"20050121"	USPAT	AND	OFF	2012/03/03 09:02
S56	51	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3)	USPAT	AND	OFF	2012/03/03 09:01
S55	0	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3).clm.	USPAT	AND	OFF	2012/03/03 09:01
S54	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of secur$4 cryptograp$3).clm.	USPAT	AND	OFF	2012/03/03 09:01
S53	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of secur$4 cryptograp$3 operation).clm.	USPAT	AND	OFF	2012/03/03 08:52
S52	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of secur$4 cryptographic operation).clm.	USPAT	AND	OFF	2012/03/03 08:52
S51	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation).clm.	USPAT	AND	OFF	2012/03/03 08:52
S50	0	S45 and S49	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:51

S49	15	(Daniel with r with l with brown).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:51
S48	0	S45 and S47	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:51
S47	790	(Daniel with brown).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:50
S46	3	"11336814"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:50
S45	3	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:49

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S73	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	USPAT; UPAD	OR	OFF	2012/03/03 09:05
S72	0	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3).clm.	USPAT; UPAD	AND	OFF	2012/03/03 09:01
S71	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation).clm.	USPAT; UPAD	AND	OFF	2012/03/03 08:52
S70	1	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation)	USPAT; UPAD	AND	OFF	2012/03/03 08:51

3/5/2012 3:44:36 PM
C:\Users\vlakhia\Documents\EAST\Workspaces\11336814.i..wsp

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29717-0048001

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Receipt date: 08/15/2011	Application Number	11336814	11336814 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-01-23	
	First Named Inventor	Daniel R.L. Brown	
	Art Unit	2431	
	Examiner Name	Viral S. Lakhia	
	Attorney Docket Number	29717-0048001	

	1	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on March 10, 2010; 4 pages.	☐
	2	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on July 22, 2010; 4 pages.	☐
	3	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on June 15, 2011; 4 pages.	☐
	4	International Search Report and Written Opinion of the International Searching Authority issued in International Application No. PCT/CA2006/000065 on May 1, 2006; 11 pages.	☐
	5	International Preliminary Report on Patentability issued in International Application No. PCT/CA2006/000065 on August 2, 2007; 8 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Viral Lakhia/	Date Considered	03/03/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Receipt date: 08/15/2011	Application Number	11336814	11336814 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-01-23	
	First Named Inventor	Daniel R.L. Brown	
	Art Unit	2431	
	Examiner Name	Viral S. Lakhia	
	Attorney Docket Number	29717-0048001	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Henry/	Date (YYYY-MM-DD)	2011-08-15
Name/Print	Michael K. Henry	Registration Number	59516

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit	: 2431
Serial No.	: 11/336,814	Examiner	: Viral S. Lakhia
Filed	: January 23, 2006	Conf. No.	: 1834
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT IN REPLY TO ACTION OF MARCH 22, 2012

Please amend the above-identified application as follows:

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-67. (Canceled)

68. (Previously Presented) A computer-implemented method comprising:

obtaining a first input value that represents a first elliptic curve point;

evaluating a hash function based on said first input value, wherein evaluating said hash function generates a hash value;

deriving from said hash value a second input value that represents a second elliptic curve point;

accessing an initial secret value stored in a register of an arithmetic unit;

generating, by a processor, an output value based on a scalar multiple of said second elliptic curve point, the scalar multiple of said second elliptic curve point obtained by combining said secret value with said second input value;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating, by the processor, an updated secret value based on a scalar multiple of said first elliptic curve point, the scalar multiple of said first elliptic curve point obtained by combining said initial secret value with said first input value; and

storing said updated secret value in said register.

69. (Previously Presented) The method of claim 68, wherein said first input value and said second input value represent two different elliptic curve points on the same elliptic curve.

70. (Previously Presented) The method of claim 68, wherein deriving said second input value includes verifying that said hash value corresponds to a valid coordinate on an elliptic curve, wherein said second elliptic curve point includes said valid coordinate.

71. (Previously Presented) The method of claim 70, wherein deriving said second input value further includes obtaining a second coordinate for said second elliptic curve point.

72. (Canceled)

73. (Previously Presented) The method of claim 68, wherein generating said output value includes:

selecting a coordinate from said scalar multiple of said second elliptic curve point; and

truncating said coordinate to a bit string.

74. (Previously Presented) The method of claim 73, wherein truncating said coordinate comprises truncating said coordinate to one half of a length of an elliptic curve point representation.

75. (Previously Presented) The method of claim 68, wherein generating said output value includes:

selecting a coordinate from said scalar multiple of said second elliptic curve point; and

hashing said coordinate to a bit string.

76. (Previously Presented) The method of claim 68, wherein generating said updated secret value includes deriving said updated secret value from a coordinate of said scalar multiple of said first elliptic curve point.

77. (Previously Presented) The method of claim 76, wherein said coordinate of said scalar multiple of said first elliptic curve point comprises an x coordinate.

78. (Previously Presented) The method of claim 68, wherein obtaining said first input value comprises deriving said first input value from an initial hash value.

79. (Previously Presented) The method of claim 68, wherein said first input value represents an x coordinate of said first elliptic curve point.

80. (Previously Presented) The method of claim 68, wherein said second input value represents an x coordinate of said second elliptic curve point.

81. (Previously Presented) The method of claim 68, wherein said first input represents two coordinates of said first elliptic curve point.

82. (Previously Presented) The method of claim 68, wherein said second input represents two coordinates of said second elliptic curve point.

83. (Currently Amended) A computer-implemented method comprising:

obtaining a verifiably random first input value that represents a first elliptic curve point;

obtaining a second input value that represents a second elliptic curve point;

generating, by a processor, a scalar multiple of said second ~~first~~ elliptic curve point based on a secret value and said second ~~first~~ input value;

generating, by the processor, an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating, by the processor, a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generating, by the processor, an updated secret value based on said scalar multiple of said first elliptic curve point; and

storing said updated secret value.

84. (Previously Presented) The method of claim 83, wherein said one-way function includes a hash function.

85. (Previously Presented) A random number generator system comprising:

an input module operable to:

obtain a first input value that represents a first elliptic curve point;

generate a hash value based on said first input value; and

derive from said hash value a second input value that represents a second elliptic curve point;

a register operable to store a secret value; and

an arithmetic unit operable to:

access said first input value, said second input value, and said secret value;

generate an output value based on said secret value and said second input value;

provide, to a cryptographic module, said output value as a random number in accordance with a specified level of security;

generate an updated secret value based on said secret value and said first input value; and

store said updated secret value in said register.

86. (Previously Presented) The random number generator system of claim 85, wherein generating said hash value comprises evaluating a hash function based on said first input value.

87. (Previously Presented) The random number generator system of claim 86, wherein said input module includes a hash function module operable to generate the hash value.

88. (Previously Presented) The random number generator system of claim 85, wherein said arithmetic unit is operable to generate said output value by generating a coordinate of a scalar multiple of said second elliptic curve point.

89. (Previously Presented) The random number generator system of claim 88, wherein said arithmetic unit is operable to generate said coordinate of said scalar multiple of said second elliptic curve point based on said secret value and said second input value.

90. (Previously Presented) The random number generator system of claim 89, wherein said arithmetic unit is operable to generate said updated secret value by generating a coordinate of a scalar multiple of said first elliptic curve point.

91. (Previously Presented) The random number generator system of claim 90, wherein said arithmetic unit is operable to generate said coordinate of said scalar multiple of said first elliptic curve point based on said secret value and said first input value.

92. (Previously Presented) The random number generator system of claim 91, wherein said arithmetic unit is operable to generate said updated secret value by converting said coordinate of said scalar multiple of said first elliptic curve point to an integer.

93. (Previously Presented) The random number generator system of claim 91, wherein said arithmetic unit is operable to generate said output value by:

converting said coordinate of said scalar multiple of said second elliptic curve point to an integer; and

truncating said integer.

94. (Previously Presented) The random number generator system of claim 93, wherein converting said coordinate includes converting an x coordinate.

95. (Previously Presented) The random number generator system of claim 88, wherein said arithmetic unit is operable to generate said output value by applying a one-way function to said coordinate of said scalar multiple of said second elliptic curve point.

96. (Previously Presented) The random number generator system of claim 95, wherein said arithmetic unit is operable to generate said output value by truncating said coordinate of said scalar multiple of said second elliptic curve point prior to applying said one-way function.

97. (Previously Presented) The random number generator system of claim 85, wherein said first input value represents an x coordinate of said first elliptic curve point.

98. (Previously Presented) The random number generator system of claim 85, wherein said second input value represents an x coordinate of said second elliptic curve point.

99. (Previously Presented) The random number generator system of claim 85, wherein said first input value represents two coordinates of said first elliptic curve point.

100. (Previously Presented) The random number generator system of claim 85, wherein said second input value represents two coordinates of said second elliptic curve point.

101. (Previously Presented) The random number generator system of claim 85, wherein said first input value and said second input value represent elliptic curve points on the same elliptic curve.

102. (Previously Presented) A random number generator system comprising:

an input module operable to:

obtain a first input value that represents a first elliptic curve point;

obtain a second input value that represents a second elliptic curve point;

a register operable to store a secret value; and

an arithmetic unit operable to:

access said first input value, said second input value, and said secret value;

generate a scalar multiple of said second elliptic curve point based on said secret value and said second input value;

generate an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

provide, to a cryptographic module, said output value as a random number in accordance with a specified level of security;

generate a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generate an updated secret value based on said scalar multiple of said first elliptic curve point; and

store said updated secret value in said register.

103. (Previously Presented) The random number generator system of claim 102, wherein said first input value and said second input value represent two different elliptic curve points on the same elliptic curve.

104. (Previously Presented) The method of claim 68, wherein the first input value comprises a verifiably random first input value.

105. (Previously Presented) The method of claim 104, wherein the second input value comprises a verifiably random second input value.

106. (Canceled)

107. (Currently Amended) The method of claim 83 [[106]], wherein the second input value comprises a verifiably random second input value.

108. (Previously Presented) The random number generator system of claim 85, wherein the first input value comprises a verifiably random first input value.

109. (Previously Presented) The random number generator system of claim 108, wherein the second input value comprises a verifiably random second input value.

110. (Previously Presented) The random number generator system of claim 102, wherein the first input value comprises a verifiably random first input value.

111. (Previously Presented) The random number generator system of claim 110, wherein the second input value comprises a verifiably random second input value.

REMARKS

Claims 68-71 and 73-111 were pending in the final Office Action dated March 22, 2012, with claims 68, 83, 85, and 102 as independent claims. Claim 106 is currently canceled; claims 83 and 107 are currently amended. Accordingly, claims 68-71 and 73-105, and 107-111 are now pending. It is submitted that no new matter has been added to the Application by the amendments to the claims. Reconsideration of the application is respectfully requested.

The Application Is In Condition for Allowance

To move prosecution forward, claim 83 is currently amended as suggested by the Examiner and to incorporate the allowed subject matter of claim 106. The amendments are made solely to move prosecution forward, without conceding the merits of any of the rejections set forth in the Office Action.

Rejections Under 35 U.S.C. § 101

Claims 83 and 84 were rejected under 35 U.S.C. § 101. Although the Applicants respectfully traverse the rejections, claim 83 is currently amended as requested by the Examiner in order to move prosecution forward. Accordingly, it is respectfully requested that the rejections under 35 U.S.C. § 101 be withdrawn.

Rejections Under 35 U.S.C. § 103

Claims 83 and 84 were rejected under 35 U.S.C. § 103. The Applicants respectfully traverse the rejections because the references have not been shown to disclose or suggest the features recited in the claims. Without conceding the rejections, claim 83 is currently amended in order to move prosecution forward. In particular, the subject matter of prior claim 106 (which the Office Action indicated as allowable) has been incorporated into claim 83. Accordingly, it is respectfully requested that the rejections under 35 U.S.C. § 103 be withdrawn.

Examiner Interview Summary

An Examiner interview was conducted by telephone on March 5, 2012. Examiner Viral S. Lakhia and the Applicants' representative Michael Henry participated in the interview. The Examiner expressed his concern that the claims in the Supplemental Amendment dated September 23, 2011 may not comply with 35 U.S.C. § 101. The undersigned stated the Applicants' position that (1) the claims in the Supplemental Amendment do comply with § 101, and (2) upon receipt of an Office Action, Applicants would consider further amendments in order to address the Examiner's concerns and move prosecution forward. No further agreement was reached during the Examiner interview.

Request for Examiner Interview

If the present application is not allowed and/or if one or more of the rejections is maintained, Applicants hereby request a telephone conference with the Examiner and further request that the Examiner contact the undersigned agent to schedule the telephone conference.

CONCLUSION

Any circumstance in which the Applicants have (a) addressed certain comments of the examiner does not mean that the Applicants concede other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the Applicants concede any of the examiner's positions with respect to that claim or other claims.

No fees are believed to be due. However, the Commissioner is hereby authorized to charge any necessary fees or credit any overpayments to deposit account 06-1050, referencing the attorney docket number shown above.

Respectfully submitted,

Date: June 22, 2012

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

Electronic Acknowledgement Receipt

EFS ID:	13086191
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	Elliptic curve random number generation
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Joni MeGuire
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	67539/622
Receipt Date:	22-JUN-2012
Filing Date:	23-JAN-2006
Time Stamp:	16:32:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		299070037001AmendmentinReplytoActionofMarch222012.pdf	106184 5b9b71c24cfa5d2dac182b99b8f1d78675edfdfe	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	11
Warnings:			
Information:			
	Total Files Size (in bytes):	106184	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/336,814	01/23/2006	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
FOR	NUMBER FILED	NUMBER EXTRA					
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	06/22/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 42	Minus	** 57	= 0	X $ =		OR	X $60=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $250=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DONNA 1. SMALLS LOGAN/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

94149 7590 07/03/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER
LAKHIA, VIRAL S

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 07/03/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

TITLE OF INVENTION: ELLIPTIC CURVE RANDOM NUMBER GENERATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	10/03/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

94149 7590 07/03/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

TITLE OF INVENTION: ELLIPTIC CURVE RANDOM NUMBER GENERATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	10/03/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAKHIA, VIRAL S	2431	380-044000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

94149 7590 07/03/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER	
LAKHIA, VIRAL S	

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 07/03/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 702 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 702 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/22/2012*.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *68-71 and 73-111*.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Viral S Lakhia/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

DETAILED ACTION

Claims *68 – 71 and 73 - 105* are allowed.

REASONS FOR ALLOWANCE

The following is an examiner's statement of reasons for allowance:

Examiner finds applicant's representative's argument dated 6/22/2012 persuasive for reason of allowance. The applicant's argument are persuasive in indication of allowable subject matter: The teachings Lauter – Gallant does not teach nor suggest applicant's claim limitation element of: "Using Elliptical Cryptography to generate secure random number by hashing one of the input values, deriving from hashed input value – second input value, using secret value to generate scalar multiple and then further generating updated random number as combination of secret value, scalar multiple and hashed points on EC (elliptical curve)", as described in amended independent claim(s) on 6/22/2012.

Updated search does not teach or fairly suggest the claimed limitations.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viral Lakhia whose telephone number is (571) 270 - 3363. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Viral S Lakhia/

Examiner, Art Unit 2431

/NATHAN FLYNN/

Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/336,814	Applicant(s)/Patent Under Reexamination BROWN ET AL.	
	Examiner VIRAL LAKHIA	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,714,648	03-2004	Miyazaki et al.	380/30
*	B	US-7,639,799	12-2009	Lauter et al.	380/30
*	C	US-7,200,225	04-2007	Schroeppel, Richard	380/28
*	D	US-7,599,491	10-2009	Lambert, Robert J.	380/30
*	E	US-7,418,099	08-2008	Vanstone et al.	380/28
*	F	US-7,308,096	12-2007	Okeya et al.	380/28
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Dr RW Lichota, Verifying the correctnes of cryptographic protocols using "convince", IEEE, Dec 13 1996, Pages 119-122.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L5	2	(first input value hash$3 elliptical curve second secret value scalar multiple random number cryptogr$4 register) and @ad<"20050121"	US-PGPUB; USPAT	AND	OFF	2012/06/27 07:18
L4	0	2 and 3	US-PGPUB; USPAT	AND	OFF	2012/06/27 07:18
L3	10	(first input value hash$3 elliptical curve second secret value scalar multiple random number cryptogr$4 register)	US-PGPUB; USPAT	AND	OFF	2012/06/27 07:18
L2	34	(daniel brown scott vanstone).in.	US-PGPUB; USPAT	AND	OFF	2012/06/27 06:57
L1	3	((elliptical with curve) ("ecc")) same (value$2 point$2) same (scalar with multiple$2) and (cryptograph$4) and @ad<"20050121" and 380/28-30.ccls.	US-PGPUB; USPAT	OR	OFF	2012/06/27 06:57
S82	17	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3) and @ad<"20050121" and 380/28-30.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/06/26 23:33
S81	26	((two dual many plural) with (input$2 point$2)) with (random with generat$4) and ("ECC" (elliptical with curve)) and (number$2) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/06/26 23:23
S80	3	"11336814"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/26 23:17
S79	6	((elliptical with curve) ("ecc")) same (value$2 point$2) same (scalar with multiple$2) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT	OR	OFF	2012/06/26 22:58
S78	4	((elliptical with curve) ("ecc")) same (value$2 point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/06/26 22:57
S77	3	"11336814"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/06/26 22:56
S76	1	((two dual many plural) with (input$2 point$2)) with (random with generat$4) and (escrow seed) and	US-PGPUB; USPAT; EPO; DERWENT;	OR	ON	2012/03/03 12:34

		("ECC" (elliptical with curve)) and @ad<"20050121"	IBM_TDB			
S75	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) same (random with number) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/03/03 12:26
S74	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) same (random with number) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/03/03 12:25
S69	0	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) same (escrow hash$3) and @ad<"20050121" and 705/54-55.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:46
S68	3	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) same (escrow hash$3) and @ad<"20050121" and 713/155-158.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:46
S67	1	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) same (escrow hash$3) and @ad<"20050121" and 380/200-201.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:24
S66	10	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) same (escrow hash$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:21
S65	5	(two dual second) with (point$2) with (random with generat$4) and (ECC elliptical curve) and (escrow hash$3) and @ad<"20050121" and 380/30.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:21
S64	1	(two) with (point$2) with (random with generat$4) and (ECC elliptical curve) and (escrow hash$3) and @ad<"20050121" and 380/30.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:14
S63	1	(two) with (point$2) with (random with generat$4) and (ECC elliptical curve) and (escrow hash$3) and @ad<"20050121" and 380/44.ccls.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/03/03 09:06
S62	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/03/03 09:05
S61	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 09:04
S60	0	((elliptical with curve) ("ecc")) same (first same second same point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 09:04

S59	0	((elliptical with curve) ("ecc")) same (first same second same hash$4) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 09:03
S58	51	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3) and @ad<"20050121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 09:02
S57	27	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3) and @ad<"20050121"	USPAT	AND	OFF	2012/03/03 09:02
S56	51	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3)	USPAT	AND	OFF	2012/03/03 09:01
S55	0	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3).clm.	USPAT	AND	OFF	2012/03/03 09:01
S54	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of secur$4 cryptograp$3).clm.	USPAT	AND	OFF	2012/03/03 09:01
S53	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of secur$4 cryptograp$3 operation).clm.	USPAT	AND	OFF	2012/03/03 08:52
S52	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of secur$4 cryptographic operation).clm.	USPAT	AND	OFF	2012/03/03 08:52
S51	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation).clm.	USPAT	AND	OFF	2012/03/03 08:52
S50	0	S45 and S49	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:51
S49	15	(Daniel with r with l with brown).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:51
S48	0	S45 and S47	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:51
S47	790	(Daniel with brown).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:50
S46	3	"11336814"	US-PGPUB; USPAT; USOCR; FPRS; EPO;	AND	OFF	2012/03/03 08:50

			JPO; DERWENT; IBM_TDB			
S45	3	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/03/03 08:49

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L9	1	((two dual many plural) with (input$2 point$2)) with (random with generat$4) and (escrow seed) and ("ECC" (elliptical with curve))	USPAT; UPAD	OR	ON	2012/06/27 07:19
L8	7	((elliptical with curve) ("ecc")) same (value$2 point$2) same (scalar with multiple$2)	USPAT; UPAD	OR	OFF	2012/06/27 07:19
L7	6	((elliptical with curve) ("ecc")) same (value$2 point$2) same (scalar with multiple$2) and (cryptograph$4)	USPAT; UPAD	OR	OFF	2012/06/27 07:19
L6	3	(first input value hash$3 elliptical curve second secret value scalar multiple random number cryptogr$4 register)	USPAT; UPAD	AND	OFF	2012/06/27 07:18
S73	0	((elliptical with curve) ("ecc")) same (first and second same point$2) same (scalar with multiple) and (cryptograph$4) and @ad<"20050121"	USPAT; UPAD	OR	OFF	2012/03/03 09:05
S72	0	(first hash input value elliptic curve point secret scalar multiple second random number cryptograp$3).clm.	USPAT; UPAD	AND	OFF	2012/03/03 09:01
S71	0	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation).clm.	USPAT; UPAD	AND	OFF	2012/03/03 08:52
S70	1	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation)	USPAT; UPAD	AND	OFF	2012/03/03 08:51

6/27/2012 8:00:42 AM
C:\Users\vlakhia\Documents\EAST\Workspaces\11336814.i..wsp

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
11336814	BROWN ET AL.
Examiner	**Art Unit**
VIRAL LAKHIA	2431

ORIGINAL		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
380	44	H 0 4 L 9 / 00 (2006.01.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
380	286	28	45	46	
713	157				

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

/VIRAL LAKHIA/ Examiner.Art Unit 2431 (Assistant Examiner)	06/26/2012 (Date)	**Total Claims Allowed:** 37	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431 (Primary Examiner)	07/02/2012 (Date)	O.G. Print Claim(s) 68	O.G. Print Figure 2

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	4144

SEARCHED

Class	Subclass	Date	Examiner
380	28-30	6/17/09	V.L.
380	44-47	6/17/09	V.L.
380	277-286	6/17/09	V.L.
713	Search 713 with key word search of elliptic curve number generator	6/17/09	V.L.
726	Search 726 with key word search of elliptic curve number generator	6/17/09	V.L.
380	28-30	4.5.2011	V.L.
380	28- 30/283-286	6/27/2012	v.l.
713	171	6/27/2012	v.l.

SEARCH NOTES

Search Notes	Date	Examiner
Key words and combination : elliptic curve number generator (creator, producer, intiator), message, digest, hash, random	7/17/09	V.L.
Get assistance with Fast and Focused Search department for the case	7/17/09	V.L
Get assistance from Peter Poltriak for claim interpretation and understanding of invention	7/17/09	V.L
Search Google Patents, NPL and wikipedia for elliptic curve technology	7/17/09	V.L
Update East with key word search	7/15/2010	V.L.
Update East with key word search.	4.6.2011	V.L.
Search INventor name for double patent issues.	4.6.2011	V.L.
Update East with key word search.	3/3/2012	v.l.
Search Google Patents, NPL and wikipedia for elliptic curve technology	3/3/2012	v.l.
Conduct plus search for independent claims	3/3/2012	v.l.
Examiner reached out to N.Flynn - T.Swann for 101 issue clarification, 101 rejection based on Todd Swan's comments.	3/5/2012	v.l.
Update East with key word search.	6/26/2012	v.l.
Search Inventor name for double patent isssue.	6/26/2012	v.l.

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
380	277-286	3/3/2012	v.l.

/V. S. L./
Examiner.Art Unit 2431

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**
380	28-30	3/3/2012	v.l.
380	28-30	6/27/2012	v.l.

/V. S. L./ Examiner.Art Unit 2431	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit	: 2431
Serial No.	: 11/336,814	Examiner	: Viral S. Lakhia
Filed	: January 23, 2006	Conf. No.	: 1834
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT IN REPLY TO ACTION OF MARCH 22, 2012

Please amend the above-identified application as follows:

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012	08/14/2012		
	1	✓		÷		✓	-	-		
	2	✓		÷		✓	-	-		
	3	✓		÷		✓	-	-		
	4	✓		÷	✓	✓	-	-		
	5	✓		÷	✓	✓	-	-		
	6	✓		÷	✓	✓	-	-		
	7	✓		÷	✓	✓	-	-		
	8	✓		÷	✓	-	-	-		
	9	✓		÷	✓	✓	-	-		
	10	✓		÷	✓	✓	-	-		
	11	✓		÷	✓	✓	-	-		
	12	✓		÷	✓	-	-	-		
	13	✓		÷	✓	✓	-	-		
	14	✓		÷	✓	✓	-	-		
	15	✓		÷	✓	✓	-	-		
	16	✓		÷	✓	✓	-	-		
	17	✓		÷	✓	✓	-	-		
	18	✓		÷	✓	✓	-	-		
	19		✓	÷	-	-	-	-		
	20			÷	✓	✓	-	-		
	21			÷	✓	✓	-	-		
	22			÷	✓	✓	-	-		
	23			÷	✓	✓	-	-		
	24			÷	✓	✓	-	-		
	25			÷	✓	✓	-	-		
	26			÷	✓	✓	-	-		
	27			÷	✓	✓	-	-		
	28			÷	✓	✓	-	-		
	29			÷	✓	✓	-	-		
	30			÷	-	-	-	-		
	31			÷	-	-	-	-		
	32			÷	-	-	-	-		
	33			÷	-	-	-	-		
	34			÷	-	-	-	-		
	35			÷	-	-	-	-		
	36			÷	-	-	-	-		

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012	08/14/2012		
	37					✓	-	-		
	38					✓	-	-		
	39					✓	-	-		
	40					✓	-	-		
	41					✓	-	-		
	42					✓	-	-		
	43					✓	-	-		
	44					✓	-	-		
	45					✓	-	-		
	46					✓	-	-		
	47					✓	-	-		
	48					✓	-	-		
	49					✓	-	-		
	50					✓	-	-		
	51					✓	-	-		
	52					✓	-	-		
	53					✓	-	-		
	54					✓	-	-		
	55					✓	-	-		
	56					✓	-	-		
	57					✓	-	-		
	58					✓	-	-		
	59					✓	-	-		
	60					✓	-	-		
	61					✓	-	-		
	62					✓	-	-		
	63					✓	-	-		
	64					✓	-	-		
	65					✓	-	-		
	66					✓	-	-		
	67					✓	-	-		
	68						=	=		
	69						=	=		
	70						=	=		
	71						=	=		
	72						=	-		

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012	08/14/2012		
	73						=	=		
	74						=	=		
	75						=	=		
	76						=	=		
	77						=	=		
	78						=	=		
	79						=	=		
	80						=	=		
	81						=	=		
	82						=	=		
	83						✓	=		
	84						✓	=		
	85						=	=		
	86						=	=		
	87						=	=		
	88						=	=		
	89						=	=		
	90						=	=		
	91						=	=		
	92						=	=		
	93						=	=		
	94						=	=		
	95						=	=		
	96						=	=		
	97						=	=		
	98						=	=		
	99						=	=		
	100						=	=		
	101						=	=		
	102						=	=		
	103						=	=		
	104						=	=		
	105						=	=		
	106						=	-		
	107						=	=		
	108						=	=		

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012	08/14/2012		
	109						=	=		
	110						=	=		
	111						=	=		

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
11336814	BROWN ET AL.
Examiner	**Art Unit**
VIRAL LAKHIA	2431

ORIGINAL		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
380	44	H 0 4 L 9 / 00 (2006.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
380	286	28	45	46	
713	157				

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	68	20	85	36	101										
2	69	21	86	39	102										
3	70	22	87	40	103										
4	71	23	88	14	104										
5	73	24	89	15	105										
6	74	25	90	19	107										
7	75	26	91	37	108										
8	76	27	92	38	109										
9	77	28	93	41	110										
10	78	29	94	42	111										
11	79	30	95												
12	80	31	96												
13	81	32	97												
14	82	33	98												
17	83	34	99												
18	84	35	100												

/VIRAL LAKHIA/ Examiner.Art Unit 2431	06/26/2012	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	42	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431	07/02/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	68	2

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	67539/622	1834

94149 7590 08/29/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER	
LAKHIA, VIRAL S	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
08/29/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Supplemental Notice of Allowability	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/6/2012*.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *68-71, 73-105, and 107-111*.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Viral S Lakhia/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995. no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/336,814
Filing Date	January 23, 2006
First Named Inventor	Scott Alexander Vanstone
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29907-0037001

This is a Request for Continued Examination (RCE) under 37 CFR 1 .114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☒ Enclosed

      i. ☒ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☒ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a

   a. ☐ period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
   The Director is hereby authorized to charge the following fees any underpayment of fees or credit any overpayments to

   a. ☒ Deposit Account No. 06-1050 .

      i. ☒ RCE fee required under 37 CFR 1.17(e)

      ii ☐ Extension of time fee (37 CFR 1.136 and 1.17)

      iii ☒ Other any deficiencies

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/Michael K. Henry/	Date	September 18, 2012
Name (Print/Type)	Michael K. Henry, Ph.D.	Registration No.	59,516

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit	: 2431
Serial No.	: 11/336,814	Examiner	: Viral S. Lakhia
Filed	: January 23, 2006	Conf. No.	: 1834
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CONTINUED EXAMINATION (RCE)

Applicants respectfully request a Continued Examination (RCE) under 37 C.F.R. §1.114 of the above identified application and also request that the below amendments are entered as follows:

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-67. (Canceled)

68. (Previously Presented) A computer-implemented method comprising:

obtaining a first input value that represents a first elliptic curve point;

evaluating a hash function based on said first input value, wherein evaluating said hash function generates a hash value;

deriving from said hash value a second input value that represents a second elliptic curve point;

accessing an initial secret value stored in a register of an arithmetic unit;

generating, by a processor, an output value based on a scalar multiple of said second elliptic curve point, the scalar multiple of said second elliptic curve point obtained by combining said secret value with said second input value;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating, by the processor, an updated secret value based on a scalar multiple of said first elliptic curve point, the scalar multiple of said first elliptic curve point obtained by combining said initial secret value with said first input value; and

storing said updated secret value in said register.

69. (Previously Presented) The method of claim 68, wherein said first input value and said second input value represent two different elliptic curve points on the same elliptic curve.

70. (Previously Presented) The method of claim 68, wherein deriving said second input value includes verifying that said hash value corresponds to a valid coordinate on an elliptic curve, wherein said second elliptic curve point includes said valid coordinate.

71. (Previously Presented) The method of claim 70, wherein deriving said second input value further includes obtaining a second coordinate for said second elliptic curve point.

72. (Canceled)

73. (Previously Presented) The method of claim 68, wherein generating said output value includes:

selecting a coordinate from said scalar multiple of said second elliptic curve point; and

truncating said coordinate to a bit string.

74. (Previously Presented) The method of claim 73, wherein truncating said coordinate comprises truncating said coordinate to one half of a length of an elliptic curve point representation.

75. (Previously Presented) The method of claim 68, wherein generating said output value includes:

selecting a coordinate from said scalar multiple of said second elliptic curve point; and

hashing said coordinate to a bit string.

76. (Previously Presented) The method of claim 68, wherein generating said updated secret value includes deriving said updated secret value from a coordinate of said scalar multiple of said first elliptic curve point.

77. (Previously Presented) The method of claim 76, wherein said coordinate of said scalar multiple of said first elliptic curve point comprises an x coordinate.

78. (Previously Presented) The method of claim 68, wherein obtaining said first input value comprises deriving said first input value from an initial hash value.

79. (Previously Presented) The method of claim 68, wherein said first input value represents an x coordinate of said first elliptic curve point.

80. (Previously Presented) The method of claim 68, wherein said second input value represents an x coordinate of said second elliptic curve point.

81. (Previously Presented) The method of claim 68, wherein said first input represents two coordinates of said first elliptic curve point.

82. (Previously Presented) The method of claim 68, wherein said second input represents two coordinates of said second elliptic curve point.

83. (Previously Presented) A computer-implemented method comprising:

obtaining a verifiably random first input value that represents a first elliptic curve point;

obtaining a second input value that represents a second elliptic curve point;

generating, by a processor, a scalar multiple of said second elliptic curve point based on a secret value and said second input value;

generating, by the processor, an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating, by the processor, a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generating, by the processor, an updated secret value based on said scalar multiple of said first elliptic curve point; and

storing said updated secret value.

84. (Previously Presented) The method of claim 83, wherein said one-way function includes a hash function.

85. (Previously Presented) A random number generator system comprising:

an input module operable to:

obtain a first input value that represents a first elliptic curve point;

generate a hash value based on said first input value; and

derive from said hash value a second input value that represents a second elliptic curve point;

a register operable to store a secret value; and

an arithmetic unit operable to:

access said first input value, said second input value, and said secret value;

generate an output value based on said secret value and said second input value;

provide, to a cryptographic module, said output value as a random number in accordance with a specified level of security;

generate an updated secret value based on said secret value and said first input value; and

store said updated secret value in said register.

86. (Previously Presented) The random number generator system of claim 85, wherein generating said hash value comprises evaluating a hash function based on said first input value.

87. (Previously Presented) The random number generator system of claim 86, wherein said input module includes a hash function module operable to generate the hash value.

88. (Previously Presented) The random number generator system of claim 85, wherein said arithmetic unit is operable to generate said output value by generating a coordinate of a scalar multiple of said second elliptic curve point.

89. (Previously Presented) The random number generator system of claim 88, wherein said arithmetic unit is operable to generate said coordinate of said scalar multiple of said second elliptic curve point based on said secret value and said second input value.

90. (Previously Presented) The random number generator system of claim 89, wherein said arithmetic unit is operable to generate said updated secret value by generating a coordinate of a scalar multiple of said first elliptic curve point.

91. (Previously Presented) The random number generator system of claim 90, wherein said arithmetic unit is operable to generate said coordinate of said scalar multiple of said first elliptic curve point based on said secret value and said first input value.

92. (Previously Presented) The random number generator system of claim 91, wherein said arithmetic unit is operable to generate said updated secret value by converting said coordinate of said scalar multiple of said first elliptic curve point to an integer.

93. (Previously Presented) The random number generator system of claim 91, wherein said arithmetic unit is operable to generate said output value by:

converting said coordinate of said scalar multiple of said second elliptic curve point to an integer; and

truncating said integer.

94. (Previously Presented) The random number generator system of claim 93, wherein converting said coordinate includes converting an x coordinate.

95. (Previously Presented) The random number generator system of claim 88, wherein said arithmetic unit is operable to generate said output value by applying a one-way function to said coordinate of said scalar multiple of said second elliptic curve point.

96. (Previously Presented) The random number generator system of claim 95, wherein said arithmetic unit is operable to generate said output value by truncating said coordinate of said scalar multiple of said second elliptic curve point prior to applying said one-way function.

97. (Previously Presented) The random number generator system of claim 85, wherein said first input value represents an x coordinate of said first elliptic curve point.

98. (Previously Presented) The random number generator system of claim 85, wherein said second input value represents an x coordinate of said second elliptic curve point.

99. (Previously Presented) The random number generator system of claim 85, wherein said first input value represents two coordinates of said first elliptic curve point.

100. (Previously Presented) The random number generator system of claim 85, wherein said second input value represents two coordinates of said second elliptic curve point.

101. (Previously Presented) The random number generator system of claim 85, wherein said first input value and said second input value represent elliptic curve points on the same elliptic curve.

102. (Currently Amended) A random number generator system comprising:

an input module operable to:

obtain a verifiably random first input value that represents a first elliptic curve point;

obtain a second input value that represents a second elliptic curve point;

a register operable to store a secret value; and

an arithmetic unit operable to:

access said first input value, said second input value, and said secret value;

generate a scalar multiple of said second elliptic curve point based on said secret value and said second input value;

generate an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

provide, to a cryptographic module, said output value as a random number in accordance with a specified level of security;

generate a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generate an updated secret value based on said scalar multiple of said first elliptic curve point; and

store said updated secret value in said register.

103. (Previously Presented) The random number generator system of claim 102, wherein said first input value and said second input value represent two different elliptic curve points on the same elliptic curve.

104. (Previously Presented) The method of claim 68, wherein the first input value comprises a verifiably random first input value.

105. (Previously Presented) The method of claim 104, wherein the second input value comprises a verifiably random second input value.

106. (Canceled)

107. (Previously Presented) The method of claim 83, wherein the second input value comprises a verifiably random second input value.

108. (Previously Presented) The random number generator system of claim 85, wherein the first input value comprises a verifiably random first input value.

109. (Previously Presented) The random number generator system of claim 108, wherein the second input value comprises a verifiably random second input value.

110. (Canceled)

111. (Currently Amended) The random number generator system of claim 102 [[110]], wherein the second input value comprises a verifiably random second input value.

112. (New) The method of claim 83, wherein the first input value is generated based on an output of a hash function.

113. (New) The method of claim 112, wherein the second input value is generated based on an output of a second hash function.

114. (New) The method of claim 113, wherein the second hash function is the hash function.

115. (New) The method of claim 114, wherein the first input value and the second input value are generated based on different inputs provided to the hash function.

116. (New) The method of claim 83, wherein said one-way function includes a truncation function.

117. (New) The method of claim 83, wherein said one-way function is applied to a coordinate of an ellptic curve point obtained from said scalar multiple of said second elliptic curve point.

118. (New) The method of claim 112, wherein the first input value is generated by providing the second input value as an input to the hash function.

119. (New) The method of claim 83, wherein said verifiably random first input value is validated as a coordinate of a point on an elliptic curve prior to generating the scalar multiple based on said first input value and said secret value.

120. (New) The method of claim 119 wherein another coordinate of said point is obtained based on said verifiably random first input value.

121. (New) The random number generator system of claim 102, wherein the first input value is generated based on an output of a hash function.

122. (New) The random number generator system of claim 121, wherein the second input value is generated based on an output of a second hash function.

123. (New) The random number generator system of claim 122, wherein the second hash function is the hash function.

124. (New) The random number generator system of claim 122, wherein the first input value and the second input value are generated based on different inputs provided to the hash function.

125. (New) The random number generator system of claim 102, wherein said one-way function includes a truncation function.

126. (New) The random number generator system of claim 102, wherein said one-way function is applied to a coordinate of an elliptic curve point obtained from said scalar multiple of said second elliptic curve point.

127. (New) A non-transitory computer-readable medium comprising instructions that are operable when executed by one or more processors to perform operations, the operations comprising:

obtaining a verifiably random first input value that represents a first elliptic curve point;

obtaining a second input value that represents a second elliptic curve point;

generating a scalar multiple of said second elliptic curve point based on a secret value

and said second input value;

generating an output value by evaluating a one-way function based on said scalar multiple of said second elliptic curve point;

using said output value as a random number to achieve a specified level of security in a cryptographic operation;

generating a scalar multiple of said first elliptic curve point based on said secret value and said first input value;

generating an updated secret value based on said scalar multiple of said first elliptic curve point; and

storing said updated secret value.

128. (New) The computer-readable medium of claim 127, wherein the second input value comprises a verifiably random second input value.

129. (New) The computer-readable medium of claim 127, wherein the first input value is generated based on an output of a hash function.

130. (New) The computer-readable medium of claim 127, wherein the second input value is generated based on an output of a second hash function.

131. (New) The computer-readable medium of claim 130, wherein the second hash function is the hash function.

132. (New) The computer-readable medium of claim 131, wherein the first input value and the second input value are generated based on different inputs provided to the hash function.

133. (New) The computer-readable medium of claim 127, wherein said one-way function includes a truncation function.

134. (New) The computer-readable medium of claim 127, wherein said one-way function is applied to a coordinate of an elliptic curve point obtained from said scalar multiple of said second elliptic curve point.

REMARKS

In the Notice of Allowance dated July 3, 2012 and the Supplemental Notice of Allowability dated August 29, 2012, claims 68-71, 73-105, and 107-111 were allowed.

Claims 102 and 111 are currently amended, and claim 110 is currently canceled. New claims 112-134 are currently added. It is submitted that no new matter has been added to the application by the present amendment.

This amendment is being filed with a Request for Continued Examination and the required fee as set forth in 37 C.F.R. § 1.17(e). The fees in the amount of $220 for 1 additional independent claim are being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account authorization. Please apply any necessary charges or credits to Deposit Account 06-1050, referencing the above attorney docket number.

Respectfully submitted,

Date: September 18, 2012

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29907-0037001

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2001222220	JP		2001-08-17	Koden Electronics Co. Ltd.		☒
	2	200135573	WO		2001-05-17	Schroeppel		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29907-0037001

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Notice of Final Rejection issued in Japanese Application No. 2007-551522 on May 30, 2012; 7 pages (with translation).	☐
	2	Office Action issued in Japanese Application No. 2007-551522 on January 18, 2012; 8 pages (with translation).	☐
	3	Official Action issued in Canadian Application No. 2,594,670 on August 9, 2012; 4 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29907-0037001

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Henry/	Date (YYYY-MM-DD)	2012-09-18
Name/Print	Michael K. Henry, Ph.D.	Registration Number	59516

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Espacenet

Bibliographic data: JP2001222220 (A) — 2001-08-17

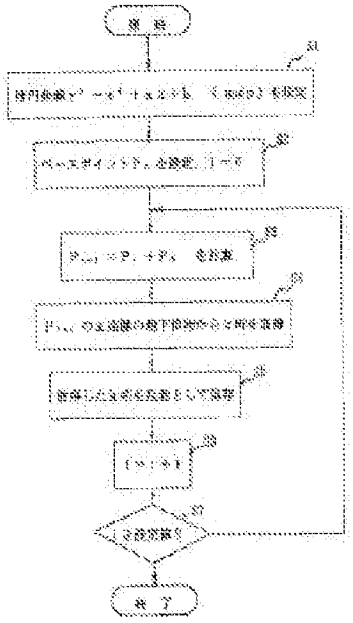
GENERATING METHOD OF RANDOM NUMBERS

Inventor(s):	KAMAGA KAZUO; FURUNO SEIZO; ONOZATO KATSURA ±
Applicant(s):	KAMAGA KAZUO; KODEN ELECTRONICS CO LTD ±

Classification:	**- international:**	***G06F7/58; G09C1/00;*** (IPC1-7): G06F7/58; G09C1/00
	- European:	
Application number:	JP20000034334 20000207	
Priority number(s):	JP20000034334 20000207	

Abstract of JP2001222220 (A)

PROBLEM TO BE SOLVED: To provide a method, which is new and difficult to be analyzed, to generate logical random numbers without depending on a feedback shift register and a mixed joint method. SOLUTION: An arbitrary point on an elliptic curve is set as a base point P0. Then, adding operations are successively conducted on the elliptic curve to successively compute &beta P0 points on the curve and random members are generated by using the coordinates of these computed points.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－222220
（P2001－222220A）
(43)公開日　平成13年８月17日(2001.8.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ	５Ｊ１０４
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ｂ	

審査請求　未請求　請求項の数５　ＯＬ　（全　４　頁）

(21)出願番号　特願2000－34334(P2000－34334)

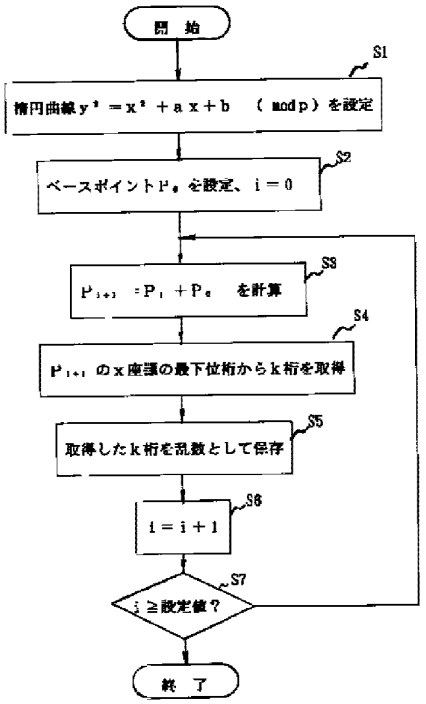
(22)出願日　平成12年２月７日(2000.2.7)

(71)出願人　500050240
釜賀　一夫
神奈川県横浜市泉区白百合２－19－32
(71)出願人　000001177
株式会社光電製作所
東京都大田区多摩川２丁目13番24号
(72)発明者　釜賀　一夫
神奈川県横浜市泉区白百合２－19－32
(72)発明者　古野　清三
東京都世田谷区奥沢８－16－12
(74)代理人　100088786
弁理士　櫻井　俊彦

最終頁に続く

(54)【発明の名称】　乱数の発生方法

(57)【要約】
【課題】ＦＳＲ（ Feedback Shift Resistor ）や混合合同法によらず、解明が困難な新規な論理乱数の発生方法を提供する。
【解決手段】本発明に係わる乱数の発生方法は、楕円曲線上に任意の点をベースポイントP_0として設定し、楕円曲線の加法演算を順次行うことによりこの楕円曲線上にβP_0の点を順次算定し、これら算定した各点の座標を使用して乱数を得るように構成されている。



【特許請求の範囲】
【請求項１】有限体上の楕円曲線上に任意の点をベースポイントＰ。として設定し、楕円曲線の加法演算を順次行うことによりこの楕円曲線上にβＰ。の点を順次算定し、これら算定した各点の座標値を使用して乱数を得ることを特徴とする乱数の発生方法。
【請求項２】請求項１において、
前記乱数は、前記算定された各点のｘ座標値又はｙ座標値中の下位若しくは上位の複数桁から成ることを特徴とする乱数の発生方法。
【請求項３】請求項１と２のそれぞれにおいて、
前記乱数は、前記算定された各点のｘ座標値又はｙ座標値中の所定桁から始まる連続的な複数桁から成ることを特徴とする乱数の発生方法。
【請求項４】請求項２と３のそれぞれにおいて、
前記乱数は、前記算定された各点のｘ座標値又はｙ座標値中の所定桁から始まる１若しくは複数桁跳びの離散的な複数桁から成ることを特徴とする乱数の発生方法。
【請求項５】請求項１乃至４のそれぞれにおいて、
前記乱数を構成する複数桁のそれぞれは、偶数か奇数かに応じて２値化されることを特徴とする乱数の発生方法。
【発明の詳細な説明】
【産業上の利用分野】
【０００１】
【発明の属する技術分野】本発明は、電気通信や情報処理などの技術分野で利用される論理乱数の発生方法に関するものである。
【０００２】
【従来の技術】電気通信の技術分野では転送データを暗号化したり、電話の不規則な発呼の間隔を模擬したりする目的などで乱数が利用される。また、情報処理の技術分野では、自然現象の解明を目的とした計算機のシミュレーションなどにおいて、無作為的に発生する事象を模擬するために乱数が利用される。
【０００３】このような乱数は、物理乱数と論理乱数（疑似乱数）とに大別される。物理乱数は、電気雑音や放射線などの不規則な物理現象を利用するものであり、公開鍵暗号の鍵の生成やブロック暗号の鍵の生成などに利用されている。これに対して、論理乱数は、算術式に基づいて生成されるものであり、混合合同法や、ＦＳＲ（Feedback Shift Resister)によるＭ系列などによって代表される。混合合同法は、プログラム言語（BASIC,Cなど）のランダム関数に利用され、Ｍ系列はスペクトラム拡散などに使用されている。
【０００４】
【発明が解決しようとする課題】論理乱数の代表的な一つであるＦＳＲによる乱数は、系列の連続した部分が所定個数以上分かると、ある種の連立方程式によって結線状態が判明して全般を解明されるおそれがあり、このような解法を困難にするために非線形化作業が必要になる。従って、本発明の目的は、ＦＳＲや混合合同法によらず分析が困難な新規な論理乱数の発生方法を提供することにある。
【０００５】
【課題を解決するための手段】本発明の乱数発生方法は、楕円曲線上に任意の点をベースポイントＰ。として設定し、楕円曲線の加法演算を順次行うことによりこの楕円曲線上にβＰ。の点を順次算定し、これら算定した各点の座標値を使用して乱数を得るように構成されている。
【０００６】
【発明の実施の形態】本発明の好適な実施の形態によれば、上記乱数は、上記算定された各点のｘ座標値又はｙ座標値中の下位若しくは上位複数桁から構成される。
【０００７】本発明の他の好適な実施の形態によれば、上記乱数は、上記算定された各点のｘ座標値又はｙ座標値中の所定桁から始まる連続的な複数桁から構成される。
【０００８】本発明の更に他の好適な実施の形態によれば、上記乱数は、上記算定された各点のｘ座標値又はｙ座標値中の所定桁から始まる１若しくは複数桁跳びの離散的な複数桁から成る。
【０００９】本発明の更に他の好適な実施の形態によれば、上乱数を構成する複数桁のそれぞれは、偶数か奇数かに応じて２値化される。
【００１０】
【原理】この発明の乱数発生方法によれば、楕円曲線上の座標値が乱数として利用される。まず、楕円曲線について説明する。この楕円曲線は次のように定義される。

$$y^2 = x^3 + ax + b \pmod{p} \quad (1)$$

ただし、ａ，ｂは、

$$4a^3 + 27b^2 \neq 0 \pmod{p} \quad (2)$$

を満たす整数、ｐは素数である。
【００１１】次に、楕円曲線上の加法演算について説明する。式(1)で定義された楕円曲線上の２点をP_1（x_1，y_1）、P_2（x_2，y_2）としたとき、$P_3 = P_1 + P_2$となる楕円曲線上の点P_3（x_3，y_3）を計算することが楕円曲線上の加法である。
【００１２】$P_1 \neq P_2$のとき

$$\lambda \equiv (y_2 - y_1) / (x_2 - x_1) \pmod{p} \quad (3)$$

$P_1 = P_2$のとき

$$\lambda \equiv (3x_1^2 + a) / (2y_1) \pmod{p} \quad (4)$$

とおけば、

$$x_3 \equiv \lambda^2 - x_1 - x_2 \quad (\mathrm{mod}\ p) \qquad (5)$$

$$y_3 \equiv \lambda (x_1 - x_3) - y_1 \quad (\mathrm{mod}\ p) \qquad (6)$$

のように計算することで、楕円曲線上の点P_3は計算できる。

【００１３】また、$P_1 = -P_2$のとき、$P_1 + P_2 = O$　となる零元を定義し、この点を無限遠点Ｏと呼ぶ。この無限遠点Ｏも楕円曲線上の点と考える。楕円曲線上の加法演算を定義することにより、楕円曲線上の点P_1を与えると、それをβ倍した点は次のように計算できる。

【００１４】まず、$P_1 + P_1 = 2P_1$となる点を、式(4)、(5)、(6)を使用して計算する。次に、式(3)、(5)、(6)を使用して$2P_1$にP_1を加算することにより、$3P_1$が計算できる。以下同様にして、P_1にP_1を（$\beta-1$）回加算することにより、βP_1点を計算することができる。以上述べたことに基づき、楕円曲線上の加法演算は、式(3)や(4)により、係数λを計算し、その値を式(5)、(6)に代入することと定義できる。

【００１５】楕円曲線上の加法演算をこのように定義することにより、式(1)のような楕円曲線とその上の点P_0（この点をベースポイントと称する）が与えられれば、βP_0のβを１ずつ増加してゆくことにより、式(1)を満足する楕円曲線上の他の点が計算できる。そして、有限体上で楕円曲線を定義しているので必ずベースポイントP_0に戻る。また、ベースポイントP_0に戻る直前の点は必ず無限遠点Ｏになる。このように、ベースポイントP_0から無限遠点Ｏまでの楕円曲線上の点が出現する。

【００１６】たとえば、楕円曲線を$y^2 = x^3 + x + 6$、ｐ＝9547とおき、P_0を（4795，4574）とする。この場合、$2P_0 \sim 7P_0$を計算すると、(3257,6425)、(0340,5389)、(6320,0741)、(7229,2320)、(2575,3027)、(1980 ,5752)となる。これらの点のｘ座標値とｙ座標値とに着目すると、出現する数値がランダム的である。従って、これらの座標値を疑似乱数として使用することができる。

【００１７】この例では、ｐの値として9547という小さな値を使用したが、実際には、後述のするように、$p = 2^{31}-1$などの大きな数を使用する。実際の使い方として、ｘ座標値だけを使用する場合、ｙ座標値だけを使用する場合、ｘ，ｙ両方の座標値を使用する場合がある。

【００１８】ｘ，ｙ座標値の一部のみを使用することにより、乱数列の解明を一層困難にすることが可能になる。まず、楕円曲線としては式(1)を使用することとし、ｐの値を十進ｎ桁、ベースポイントを$P_0 =$（x_0，y_0）とする。楕円曲線の加法演算に従い、$2P_0 =$（x_2，y_2）を計算する。ここで、ｋ＜ｎを満足する自然数ｋを選択し、x_2の値の最下位桁からｋ桁目まで選択し、その値を乱数とする。連続的なｋ桁の数値を、最下位桁からではなく最上位桁から下位桁方向にｋ桁目まで選択するたたともできる。

【００１９】あるいは、最上位桁や最下位桁を含ませることなく、最下位桁や最上位桁から所定桁離れた桁から始まる連続的な複数桁を選択することもできる。更には、ｘ又はｙ座標値中の所定桁から始めて一つ跳び、二つ跳びなどのように、１又は複数の跳びで複数の桁を選択し、これを乱数とすることもできる。このように、ｘ又はｙ座標値中の大きな桁からその一部を種々の方法によって選択して乱数とすることにより、他人による乱数列の解明を一層困難にすることができる。

【００２０】次に、$3P_0 =$（x_3，y_3）を計算し、x_2の場合と同様に、x_3の値からｋ桁の数値を取る。以下、同様にして、βP_0の係数βを１づつ増加させ、新たな係数βに対応したｘ座標値のｋ桁の数値を選択することにより乱数を生成することができる。各桁の数は十進数であるが、偶数と奇数とに分けて二進数の乱数に変化させることもできる。例えば、偶数を“０”，奇数を“１”とした場合、加算演算に従って算定された楕円曲線上の点のｘ，ｙ座標値が4795であれば、乱数として“０”“１”“１”“１”が生成される。

【００２１】以上の手順をフローチャートで表現すると、図１に示すように、ステップＳ１からステップＳ７までの処理から成る。

【００２２】以下は、楕円曲線を用いた乱数の頻度検定のシミュレーション結果である。

シミュレーションの条件

楕円曲線の式	；$y^2 = x^3 + x + 6$
素数	；$p = 2^{31}-1 = 2,147,483,647$
ベースポイント	；(2,4)
始めの係数値	；10,000
係数の増加値	；1
乱数	；計算されたｘ座標値の下位５桁を使用
検定に用いた乱数の数	；１０万

【００２３】シミュレーションの結果χ^2値は7.4であった。なお、今回は10進数のため自由度が９となり、このことから、有意水準５％のχ^2棄却域は16.9以上で、有意水準１％のχ^2棄却域は21.7以上

となる。

【００２４】

【発明の効果】以上詳細に説明したように、本発明の乱数発生方法は、有限体上の楕円曲線の加法演算に基づきこの楕円曲線上に点を順次設定してゆき、各点の座標値を用いて乱数を発生させる構成であるから、ＦＳＲや混合合同法によることなく、比較的簡易な演算によって解明が困難な論理乱数を発生できるという効果がある。

【００２５】また、本発明の乱数発生方法によれば、上述したシミュレーションの結果によって裏付けられたように、かなり良質の乱数を発生させることができるという利点もある。

【００２６】更に、本発明の一実施例によれば、算定した楕円曲線の各点の座標値中から複数桁を種々の方法で選択することにより乱数を生成する構成であるから、他人による乱数の解明を一層困難にすることが可能になるという利点がある。

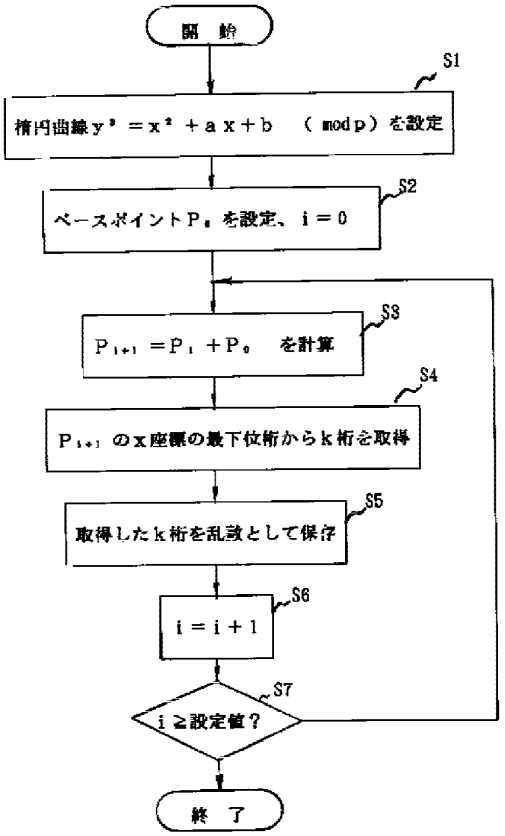
【図面の簡単な説明】

【図１】本発明の乱数発生方法の処理内容を示すフローチャートである。

【符号の簡単な説明】

S1～S7　図１のフローチャートの各処理に付された参照符号。

【図１】



フロントページの続き

(72)発明者　小野里　桂
群馬県高崎市中尾町132

Ｆターム(参考)　5J104 AA25 FA05 NA16

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35573 A1

(51) International Patent Classification[7]: H04L 9/08, 9/16, 9/28, 9/30

(21) International Application Number: PCT/US00/31014

(22) International Filing Date:
9 November 2000 (09.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/165,202	12 November 1999 (12.11.1999)	US
09/518,389	3 March 2000 (03.03.2000)	US
60/196,696	13 April 2000 (13.04.2000)	US
09/710,987	8 November 2000 (08.11.2000)	US

(71) Applicant and
(72) Inventor: **SCHROEPPEL, Richard** [—/US]; 500 South Maple Drive, Woodland Hills, UT 84653 (US).

(74) Agents: **PIERCE, Gary, D., E.** et al.; Pate Pierce & Baird, Bank One Tower, 50 West Broadway, Suite 900, Salt Lake City, UT 84101 (US).

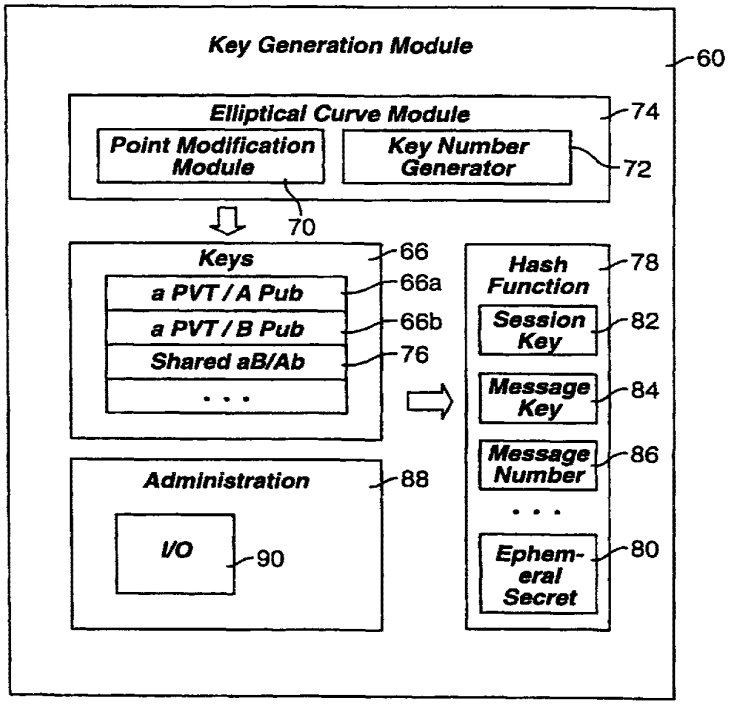
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ELLIPTIC CURVE POINT AMBIGUITY RESOLUTION APPARATUS AND METHOD



(57) Abstract: An apparatus for operating a cryptographic engine (58) may include a key generation module (60) for creating key pairs (66) for encrypting substantive content to be shared between two users over a secured or unsecured communication link. The key generation module (60) may include a point-modification module (70) as part of an elliptic curve module (74) for creating and processing keys (68). The point-modification module (70) preferably employs a point-halving algorithm for creating and processing keys (68) but may also employ any one or a combination of a variety of other algorithms. Hash functions (78) may be used to further process ephemeral secrets or ephemeral keys that may be used for transactions, sessions, or other comparatively short time increments of communication. The keys generated by the key generation module (60) may be configured to be processable by an encryption system for divulging independently to two independent parties a secret to be shared by the two independent parties. A point-halving algorithm may be provided to reduce the operation count of a cryptographic process.

WO 01/35573 A1

ELLIPTIC CURVE POINT AMBIGUITY RESOLUTION APPARATUS AND METHOD

BACKGROUND

1. The Field of the Invention

This invention relates to cryptography and, more particularly, to novel systems and methods for increasing the speed of cryptographic key computations by computers.

2. The Background Art

The science of cryptography has existed since ancient times. In recent years, cryptography has been used in special purpose software programs for a variety of purposes, such as hiding underlying contents, limiting access, inhibiting reverse engineering, authenticating sources, limiting unauthorized use, and the like.

Cryptographic Processes

Modern cryptography protects data transmitted over a network or stored in computer systems. Two principal objectives of cryptography include (1) secrecy, e.g., to prevent the unauthorized disclosure of data, and (2) integrity (or authenticity), e.g., to prevent the unauthorized modification of data. Encryption is the process of disguising plaintext data in such a way as to hide its contents, and the encrypted result is known as ciphertext. The process of turning ciphertext back into plaintext is called decryption.

A cryptographic algorithm, also known as a cipher, is a computational function used to perform encryption and/or decryption. Both encryption and decryption are controlled by one or more cryptographic keys. In modern cryptography, all of the security of cryptographic algorithms is based on the key(s) and does not require keeping the details of the cryptographic algorithms secret.

There are two general types of key-based cryptographic algorithms: symmetric and public-key. In symmetric algorithms, the encryption key can be calculated from the decryption key and vice versa. Typically, these keys are the same. As such, a sender and a receiver agree on the keys (a shared secret) before they can protect their communications using encryption. The security of the algorithms rests in the key, and divulging the key allows anyone to encrypt and decrypt data or messages with it.

In public-key algorithms (also called asymmetric algorithms), the keys used for encryption and decryption differ in such a way that at least one key is computationally infeasible

to determine from the other. To ensure secrecy of data or communications, only the decryption key need be kept private, and the encryption key can thus be made public without danger of encrypted data being decipherable by anyone other than the holder of the private decryption key.

Conversely, to ensure integrity of data or communications, only the encryption key need be kept private, and a holder of a publicly-exposed decryption key can be assured that any ciphertext that decrypts into meaningful plaintext using this key could only have been encrypted by the holder of the corresponding private key, thus precluding any tampering or corruption of the ciphertext after its encryption.

A private key and a public key may be thought of as functionally reciprocal. Thus, whatever a possessor of one key of a key pair can do, a possessor of the other key of the key pair can undo. Accordingly, secret information may be communicated without an exchange of keys.

An asymmetric algorithm assumes that public keys are well publicized in an integrity-secure manner. A sender can then know that the public key of the receiver is valid and not tampered with. One way to ensure integrity of data packets is to run data through a cryptographic algorithm. A cryptographic hash algorithm may encrypt and compress selected data. Various cryptographic hash algorithms are known, such as the Secure Hash Algorithm (SHA) and Message Digest 5 (MD5).

A certificate is a data structure associated with assurance of integrity and/or privacy of encrypted data. A certificate binds the identity of a holder to a public key of that holder, and may be signed by a certification authority (CA). In a public key infrastructure (PKI), a hierarchy of certification authorities may be provided, each level vouching for the authenticity of the public keys of subordinate levels.

A certificate may contain data regarding the identity of the entity being certified, the key held (typically a public key), the identity (typically self-authenticating) of the certifying authority issuing the certificate to the holder, and a digital signature protecting the integrity of the certificate itself. A digital signature may typically be based on the private key of the certifying authority issuing the certificate to the holder. Thus, any entity to whom the certificate is asserted may verify the signature corresponding to the private key of the certifying authority.

In general, a signature of a certifying authority is a digital signature. The digital signature associated with a certificate enables a holder of the certificate, and one to whom the certificate is asserted as authority of the holder, to use the signature of the certifying authority to verify that

nothing in the certificate has been modified. This verification is accomplished using the certificate authority's public key, thus providing a means for verifying the integrity and authenticity of the certificate and of the public key in the certificate.

Various cryptographic techniques rely on elliptic curves. Code and documentation for the use of elliptic curves in cryptography are available. For example, standard references, including certain algebra texts discussing Galois Fields, sometimes called "finite fields," are available in the art.

One reason for interest in acceleration of elliptic curve processing is the increasing size of cryptographic keys. Mathematical calculations often increase geometrically with the size of the keys. Accordingly, if the speed of elliptic curve processing can be increased, less processing time is required for more secure, longer cryptographic keys. Thus, what is needed is methods and apparatus for accelerating computations associated with creating, weaving, and processing of cryptographic keys.

Public key cryptography makes extensive use of modular arithmetic functions and concepts, especially powers. Computing A^B (mod C) is a staple operation. Hereinafter, the caret ^ means exponentiation (*i.e.*, A to the power B). Generally, the modular arithmetic can be replaced with operations in an arbitrary group, and elliptic curve groups have been found to be useful. Instead of (mod C), an elliptic curve group G can be used. The elements of G are called points. The multiplication operation (mod C) is replaced by addition of group elements (points), and the exponentiation A^B is replaced by adding B copies of the point A.

BRIEF SUMMARY OF THE INVENTION

The invention is described as a set of formulas which are implemented as a computer program. The same computations can also be carried out very efficiently in purpose-built hardware devices, or in semi-custom logic, for example, smart-cards or FPGA circuits, or as firmware controlling hardware, or as combinations of these elements.

A principal feature provided by an apparatus and method in accordance with the invention includes a point modification algorithm that manipulates points of an elliptic curve method. The point modification algorithm may be used in generating a key using a selected elliptic curve method, which may be used to encrypt substantive content using the key. The point modification

algorithm may be employed using any one or a combination of point addition, point subtraction, point fractioning, point multiplying, rotating, and negative point modification.

In one aspect of the invention, the point fractioning may be selected from integral point fractioning, corresponding to a denominator that is an integral number, and point multiplying may be selected from integral multiplication, imaginary multiplication, and complex multiplication. In selected embodiments, the point modification algorithm may be dynamically selected during use in lieu of specifying the modification operation in advance.

In another aspect of the invention, a selected property may be used to select a point on which to execute the point modification algorithm. The selection property may include without limitation membership of the point in a selected subgroup. The selection property may include reliance on a bit mask of coordinates corresponding to points in a subgroup.

A point may be selected and pre-modified by a modification operation that compensates for some of the processing steps. A point may be selected by testing whether a halving procedure can be executed on the point an arbitrary number of times selected by a user. The modification process may also include determining which of a selected number of points is to be used. The foregoing point modification processes may be repeated with a second point, which is selected by either a deterministic process or a random process.

In yet another aspect of the invention, substantive content may be sent by a sender and received by a receiver. The sender may use a modification process for encryption that is separate and distinct from the modification that the receiver uses for decryption. The key may be a symmetric key configured to be shared by two or more parties, a decryption code for processing an encrypted signal, a digital signature, an asymmetric key, or an authentication. The modification operation may also include the step of selecting a point from either a hyperelliptic, an algebraic curve, or an abelian variety.

In a further aspect of the invention, the modification process may be the halving of a point. The point to be halved may be represented in a cartesian space or the point may exist in a mapped cartesian space having a cartesian representation. The halving operation may include only a single multiplication per halving operation or multiple multiplications. The selected point may be by a cartesian tuple and halving may be accomplished using no more than two field multiplications. The halving operation may be negative halving including without limitation computation of a minus one-half multiple. The modification process may also include computing

a fractional multiple of a point represented as a proper fraction, an improper fraction, or a complex fractional multiple.

Another feature provided by an apparatus and method in accordance with the invention includes a point modification algorithm as part of an elliptic curve module within a key generation module for creating and processing keys. Hash functions may be used to further process ephemeral secrets or ephemeral keys that may be used for transactions, sessions, or other comparatively short time increments of communication. The modification algorithm preferably employs one or some combination of point addition, point subtraction, point fractioning, point multiplying, rotating, and negative point modification.

The keys generated by the key generation module may be configured to be processable by an encryption system for divulging independently to two independent parties a secret to be shared by the two independent parties. In various embodiments, a point modification algorithm is provided to reduce the operation count of a cryptographic process.

The present invention may also be embodied as an article storing an encryption engine for operating on keys configured to encrypt substantive content representing information that includes a key generation module for operating on the keys and a point modification algorithm for calculating points related to the key. The point modification algorithm may employ one or more of point addition, point subtraction, point fractioning, point multiplying, rotating, and negative point modification.

In one aspect of the invention, the point halving module may include a register for storing an ordered pair of variables selected to be operated on for executing point halving. The ordered pairs may represent a set of coordinates corresponding to a point on an elliptic curve.

The above objects may be met by one or more embodiments of an apparatus and method in accordance with the invention. Likewise, one or more embodiments of an apparatus and method in accordance with the invention may provide the desirable features as described.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects and features of the present invention will become more fully apparent from the following description and appended claims, taken in conjunction with the accompanying drawings. Understanding that these drawings depict only typical embodiments of the invention and are, therefore, not to be considered limiting of its scope, the invention will

be described with additional specificity and detail through use of the accompanying drawings in which:

Figure 1 is a schematic block diagram of an apparatus suitable for implementing a method and system in accordance with the invention for an individual user, or multiple users communicating over a network or internetwork;

Figure 2 is a schematic block diagram of select modules that may be hosted in a memory device operating on a computer of a user in accordance with the invention;

Figure 3 is a schematic block diagram of a key generation module that may implement certain aspects of a method and system in accordance with the invention;

Figure 4 is a schematic block diagram of a process for encryption using a method in accordance with the invention;

Figure 5 is a schematic block diagram of a process in accordance with the invention including generation of keys, use of the keys for encryption, and decryption of the content of a message; and

Figure 6 is a schematic block diagram of an abbreviated method of authentication in accordance with the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

It will be readily understood that the components of the present invention, as generally described and illustrated in the Figures herein, could be arranged and designed in a wide variety of different configurations. Thus, the following more detailed description of the embodiments of the system and method of the present invention, as represented in Figures 1 through 6, is not intended to limit the scope of the invention, as claimed, but it is merely representative of certain presently preferred embodiments of the invention.

The presently preferred embodiments of the invention will be best understood by reference to the drawings, wherein like parts are designated by like numerals throughout. Reference numerals having trailing letters may be used to represent specific individual items (e.g. instantiations) of a generic item associated with the reference numeral. Thus, a number 156a, for example, may be the same generic item as number 156f, but may result from a different version, instantiation, or the like. Any or all such items may be referred to by the reference numeral 156.

Referring to Figure 1, an apparatus 10 may implement the invention on one or more nodes 11, (client 11, computer 11) containing a processor 12 or CPU 12. All components may exist in a single node 11 or may exist in multiple nodes 11, 52 remote from one another. The CPU 12 may be operably connected to a memory device 14. A memory device 14 may include one or more devices such as a hard drive or non-volatile storage device 16, a read-only memory 18 (ROM) and a random access (and usually volatile) memory 20 (RAM).

The apparatus 10 may include an input device 22 for receiving inputs from a user or another device. Similarly, an output device 24 may be provided within the node 11, or accessible within the apparatus 10. A network card 26 (interface card) or port 28 may be provided for connecting to outside devices, such as the network 30.

Internally, a bus 32 may operably interconnect the processor 12, memory devices 14, input devices 22, output devices 24, network card 26 and port 28. The bus 32 may be thought of as a data carrier. As such, the bus 32 may be embodied in numerous configurations. Wire, fiber optic line, wireless electromagnetic communications by visible light, infrared, and radio frequencies may likewise be implemented as appropriate for the bus 32 and the network 30.

Input devices 22 may include one or more physical embodiments. For example, a keyboard 34 may be used for interaction with the user, as may a mouse 36 or similar pointing device. A touch screen 38, a telephone 39, or simply a telephone line 39, may be used for communication with other devices, users, or the like. Similarly, a scanner 40 may be used to receive graphical inputs which may or may not be translated to other character formats. A memory device 41 of any type (e.g. hard drive, floppy, etc.) may be used as an input device, whether resident within the node 11 or some other node 52 on the network 30, or from another network 50.

Output devices 24 may likewise include one or more physical hardware units. For example, in general, the port 28 may be used to accept inputs and send outputs from the node 11. A monitor 42 may provide outputs to a user for feedback during a process, or for assisting two-way communication between the processor 12 and a user. A printer 44 or a hard drive 46 may be used for outputting information as output devices 24.

In general, a network 30 to which a node 11 connects may, in turn, be connected through a router 48 to another network 50. In general, two nodes 11, 52 may be on a network 30, adjoining networks 30, 50, or may be separated by multiple routers 48 and multiple networks 50

as individual nodes 11, 52 on an internetwork. The individual nodes 52 (e.g. 11, 52, 54) may have various communication capabilities.

In certain embodiments, a minimum of logical capability may be available in any node 52. Note that any of the individual nodes 11, 52, 54 may be referred to, as may all together, as a node 11 or a node 52. Each may contain a processor 12 with more or less of the other components 14-44.

A network 30 may include one or more servers 54. Servers may be used to manage, store, communicate, transfer, access, update, and the like, any practical number of files, databases, or the like, for other nodes 52 on a network 30. Typically, a server 54 may be accessed by all nodes 11, 52 on a network 30. Nevertheless, other special functions, including communications, applications, directory services, and the like may be implemented by an individual server 54 or multiple servers 54. A node 11 may be a server 54.

In general, a node 11 may need to communicate over a network 30 with a server 54, a router 48, or nodes 52 or server 54. Similarly, a node 11 may need to communicate over another network (50) in an internetwork connection with some remote node 52. Likewise, individual components 12-46 may need to communicate data with one another. A communication link may exist, in general, between any pair of devices. The process and method of the invention may be performed on the hardware structure illustrated in Figure 1.

Referring to Figure 2, a memory device 20 in an apparatus 10, and more particularly in an individual computer 11, may include a cryptographic engine 58 for creating, manipulating, processing, using, and otherwise operating on cryptographic keys. Cryptographic keys are known in the art. A key generation module 60 may be responsible for creating keys that may be used to encrypt substantive content 62 for one of a multitude of purposes. As discussed above, the substantive content 62 may be used for various functionalities, including transmission of the substantive content 62 between users.

In general, a key generation module 60 may support local and remote repositories 64 of key pairs 66. A key pair 66 may involve a public key 68a and a private key 68b. In alternative embodiments, a particular key pair 66a may include symmetric keys 68a, 68b. However, in current strong cryptography, the individual keys 68a, 68b are a public/private pair used as described above for preparing and processing information to be sent and received.

In certain embodiments, keys 68a, 68b from various users may be mixed and matched between public and private keys in order to prepare woven keys 69 that are used by senders and receivers on opposite ends of a communication link to securely hide, authenticate, sign, etc., substantive content 62 that is being exchanged.

Referring to Figure 3, the key generation module 60 may include an elliptic curve module 74 in accordance with the invention. In one presently preferred embodiment, a point modification module 70 may operate in accordance with the algorithms described hereinafter, to generate the keys 68 provided by the key generation module 60. The point modification module 70 may employ one or more of point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, alone or in combination, for modifying points. A key number generator 72 may include an executable of basic simplicity or considerable sophistication in order to create keys having a desired level of security. Levels of security are typically defined in terms of the algorithms executed by key number generators 72, and equivalent processing 72 executed upon receipt of encrypted information.

Key pairs 66, such as the public/private pairs 66a, 66b or the shared, woven keys 76, may be processed by a hash function 78. The hash function 78 may typically operate on an ephemeral secret 80. An ephemeral secret 80 may be embodied in a session key 82 shared by two users over a communication link during a "session" period of time defined by the users or by their respective computers. Similarly, for a single communication of substantive content 62, an individual message key 84 may be created and relied upon. In one embodiment, a message key 84 may be embodied

simply as a message number 86 corresponding to a time, random number, or some combination of numbers associated by a user with a single message.

Practicalities of computation associated with cryptography require that some number of administration modules 88 provide support for the key generation module 60. For example, in one embodiment, input/output drivers 90 may be provided. Likewise, the input/output systems 90 may provide the wrapping, pre-processing, post-processing, maintenance, verification, and the like associated with creating, distributing, using, and management of the keys 68.

Referring to Figure 4, a method 91 for using the apparatus and systems in accordance with the invention may involve creating 92 a durable secret. A durable secret may refer to a shared

key (whether symmetric or asymmetric) that will be relied upon over an extensive period of time, such as a year.

Sharing 94 the durable secret involves an exchange, distribution, or the like of a durable secret 96 or computed secret 96 sufficiently strong to be reliable over an extensive period of time involving numerous communications between users. In order to initiate use, creating 98 a message counter may occur during individual transactions, in preparation for a short sequence of transactions, or for some other time period that is comparatively short, spanning a transaction, a few transactions, or the like.

In general, creating the message counter 98 will be used for creating 100 an ephemeral secret 80. For example, the shared secret 102 may have a duration of a single message, or a single computer session, or the like. Thus, the shared secret 102 may be an ephemeral secret 80 of a comparatively short length or suitable for processing by a comparatively simple process. However, creating 100 an ephemeral secret 80, such as the shared secret 102 may be computationally very intensive due to both the manipulations of numbers required as well as the frequency with which such creating 100 is done.

Executing 104 a hash function may be done as known in the art or as described in the art. Hashing 104 provides verification to both machines and users that no message modification, whether intentional or unintentional (*e.g.*, modification simply due to a computer glitch, has occurred. Hashing is also used to operate on the woven key 69 and the message number 86 to create an ephemeral symmetric key.

Thereafter, encrypting 106 substantive content 62 may be followed by a transmission 108 and corresponding receipt 109 of the substantive content 62. The substantive content 62 may have been prepared with a cryptographic system. Note that the substantive content 62 may merely be a signature on a document in the clear. Alternatively, substantive content 62 may have been encrypted itself and wrapped, as well as being signed, authenticated, verified, and the like.

Thus, cryptographic key generation modules 60, or more properly, key management modules 60, may manage one or more keys. Moreover, those one or more keys may be incoming, outgoing, or the like. Also, those keys 68 may be used on substantive content 62, that is destined to be outgoing, incoming, or both.

Decrypting 110 returns substantive content 62 into the clear. Decrypting 110 may be more complex, exactly the same complexity, or less complex than an encrypting process 106. Nevertheless, in certain embodiments, encrypting 106 and decrypting 110 are substantially mirror images of one another.

Referring to Figure 5, a method 111 in accordance with the invention may include generating 112 a private key 68b. Generating 112 keys may rely on executing 114 a point modification method, which may include without limitation a point halving method, in order to obtain an initial public key based on a corresponding private key. At another location, a different user who will eventually correspond to an initial user, may also generate 116 a public key from a private key relying on point modification 118, which may be a point halving 118. At this stage, the generation processes 112, 116 are performed apart.

Distributing 120 a public key 68a may require authorization or other exercise 122 of a key authority. In other words, one may execute 122 or exercise 122 a key authority, where the key authority is an actual entity or where the authority represents the authorization owned by an entity. Accordingly, in a corresponding process, a distribution 124 of a key that will end up being distributed to a first user from a second user may be completed.

Thus, a user "A" may distribute a public key "A" to a user "B." Similarly, a user "B" may distribute a public key "B" to a remote user "A." A user may receive 126 a public key from another user. Accordingly, a corresponding partner in communication may receive 28a a first user's public key.

In certain embodiments, weaving 130 one's own private key with a received public key may rely on an elliptic curve method 132. The elliptic curve method 132 results in a woven key 69. Similarly, weaving 134 results in the same woven key for a remote user. Creating 136, 138 a counter enables an encryption 106, 140 of substantive content 62 being shared between a user "A" and a user "B."

Exactly who performs the encrypting 106, 140 depends upon the directionality of a message, authentication, or other substantive content 62. Appropriately, a transmission 108 and reception 109, or a send 108 and a receive 109 will represent a particular user. Similarly an exchange 142 (which may be a send 108 or a receive 109) represents activities at a remote user.

Accordingly, decrypting 110, 144 provides the substantive content 62 in the clear. Of course, the substantive content 62 may simply be knowledge provided by transmission of

signatures, authentications, and the like. Each of the processes of generating 112 distributing 120, weaving 130, and the like may involve the processing of large numerical keys. The use of a method and apparatus in accordance with the invention may be more time-consuming or time-saving depending on the frequency and complexity of any particular key manipulation. Similarly, encrypting 106, 140 and decrypting 110, 144 may use methods in accordance with the invention, depending on the need for security, the complexity, the frequency, and so forth.

Referring to Figure 6, an embodiment of a method 145 may be simplified to receiving 146 a privately keyed document. A document may actually be a signature. Nevertheless, receiving 146 implies keyed (encrypted) processing.

Next, running 148 an elliptic algorithm using public key processed information prepared with a private key by an originator. Authenticating 150 may represent a successful calculation of a solution to an equation or set of equations using the keys 68 or a key 68.

Most public key cryptography operations such as key exchange, digital signatures, encryption, and entity authentication, can be implemented very efficiently using elliptic curve arithmetic. An apparatus and method in accordance with the invention may make elliptic curve arithmetic faster, and thereby improve the public key operations. Faster elliptic-curve key exchange, faster elliptic-curve ElGamal encryption, for faster elliptic-curve Digital Signatures, and for faster MQV authentication (see IEEE draft standard P1363), are most useful, although the methods herein may be helpful wherever computations with elliptic curves are used.

Such a method works with any field-element representation, so long as a reasonably efficient reciprocal operation is available. This includes polynomial basis representation, normal basis representation, and field-tower representation. A set of formulas in accordance with the invention may be implemented in a computer program, such as the point modification module 70. In certain presently preferred embodiments, the point modification module 70 is configured to generate a key using a point modification algorithm, as described immediately below. The same computations can also be carried out very efficiently in firmware, dedicated hardware devices, or in semi-custom logic, such as, for example, smart-cards or FPGA circuits.

In finite fields GF[2^K], addition may be performed by way of an XOR operation. Use of the XOR operation makes performance of addition and subtraction substantially equivalent operations. Use of the XOR operation also makes squaring and square-rooting operations comparatively computationally economical. In contrast to real-number operations, squaring and

square-rooting are 1-1 operations in a GF[2^K] field, as a result of every field element having exactly one square-root. The symbol "sqrt" hereinafter represents the square-root operation. Squaring and square-root are LINEAR operators, which may be represented as follows: (A+B)^2 = A^2 + B^2, and sqrt(A+B) = sqrt(A) + sqrt(B).

Qsolve is a variation on square-roots. Qsolve(C) operates on field elements C, and gives a solution to the quadratic equation Z^2 + Z = C. Only 50% of the field elements have solutions. Those that do, have two solutions, Z and Z+1. Qsolve is also linear. Although Qsolve is relatively complicated to compute, it is also relatively fast.

The TRACE of an element C in the field GF[2^K] can be computed from the formula Trace(C) = C + C^2 + C^4 + C^8 + C^16 + ... + C^(2^(K-1)). The trace is always 0 or 1. If-and-only-if the trace is 0, the equation Z^2 + Z = C has a solution (in the field). Trace is linear: Trace(C+D) = Trace(C) + Trace(D). This means, for example, that the trace of a general field element can be computed by adding up the traces of the individual bits of the field element.

The foregoing concept is used to compute the Trace-Mask for a field. The Trace- Mask T has the same number of bits as a field element. A bit is 1 in the trace-mask when the corresponding single-bit field element has trace 1. The trace of a field element C can be computed very quickly with the trace-mask: Trace(C) is simply the parity of the bitwise And of C with T. In the programs in the appendix, for GF[2^155], the trace-mask has only two 1 bits, so the trace of a field element can be computed simply by examining two of its bit positions.

For odd degree fields (when K is odd), the Half-Trace is useful. Half-Trace(C) = C + C^4 + C^16 + C^64 + C^256 + ... + C^(2^(K-1)). In the quadratic equation Z^2 + Z = C, we may take Z = Half-Trace(C). The Half-Trace function is also linear.

The most preferable elliptic curves use a field GF[2^K] with characteristic 2, and curve equation Y^2 + X Y = X^3 + A X^2 + B, where X, Y, A, B are finite field elements. A and B are constants that define the particular curve; X and Y are variables. It is best if Trace(A) = 1. If the field degree K is odd, then A may be taken as 1. B is nonzero.

A pair (X,Y) that satisfies the equation is called a "point" of the curve, by analogy with the real-variable case. One additional point, called the "point-at-infinity", is represented by the pair (0,0). The point serves as an identity element for the curve point-addition operation discussed hereinbelow. Most curve operations must check for and handle this point as a special

case. The appropriate method of handling the special case of an identity element is well known to those skilled in the art.

The number of curve points is roughly the same as the size of the finite field. The exact number depends on A and B. If Trace(A) = 1, the number of points is twice an odd number; otherwise the number of points is a multiple of 4. The Odd Subgroup is largest when Trace(A) = 1. B is chosen such that the group order is twice a prime, or has a large prime factor. The procedure preferably attempts low-hamming-weight B values. According to the procedure, for each B, the

group size is computed with Schoof's method, and factored. Under the procedure, Bs are attempted until a suitable value is found. A few hundred trials are typically needed.

As appreciated by those of skill in the art, the points of an elliptic curve form a commutative group under an operation fancifully called "Addition". Such Addition is not related to adding ordinary numbers, vectors, or finite field elements. The operation is called "Addition," because, similar to ordinary addition, the operation exhibits commutative and associative properties, has an identity element (the "point at infinity"), and inverses.

The formulas for curve-point Addition, Doubling and Negation are known to those of skill in the art. Point Negation operations are computationally relatively inexpensive. A point P and its negative -P have the same X-coordinate, but have different Y-coordinates.

Beginning with a particular curve point P = (X,Y), integer multiples of the point such as 3*P by repeated Addition: 3*P = (P+P)+P, can be formed. A special Doubling operator is preferably used, when a point is Added to itself. Thus, one may identically compute 4*P in any of a number of ways including without limitation as 2*(2*P) (using the Doubling operator twice) or as (P+(2*P))+P. Addition requires computing the reciprocal of a field element and a couple of field multiplications. Doubling is typically comparatively faster than Addition.

Halving a point is the opposite of Doubling. Halving a point P finds a point Q such that 2*Q = P.

An elliptic curve group is either cyclic (isomorphic to a group of integers mod some modulus J) or the group product of two cyclic groups. For the curves described above, over fields GF[2^K] with the quadratic-cubic equation, the group always has an even number of points. The ORDER of a POINT P is the smallest positive integer N for which N*P = the

point-at-infinity. The ORDER of a GROUP is the number of points (or elements) in the group. The order of a point always divides exactly into the order of the whole group.

The points of odd order form a subgroup, called the ODD Subgroup, which is either cyclic or the group product of two cyclic groups. The points whose order is a power of 2 form another subgroup, the EVEN subgroup, which is always cyclic and contains a power-of-2 number of elements, and is isomorphic to the group of integers modulo some power of 2. The two subgroups have one point in common, the point at infinity. Many curve points exist that are not in either subgroup. Any point of the curve can be written uniquely as the sum of an Odd Subgroup point and an Even Subgroup point.

The majority of elliptic curve cryptography implementations today use the Odd Subgroup, or a further restricted subgroup thereof. If any curve point is doubled enough times, the result point is in the Odd Subgroup. The Odd Subgroup is mapped 1-1 to itself by doubling. In the group as a whole, doubling is a 2-1 operator; pairs of points are mapped together. Halving, which is the opposite of doubling, is a 1-2 operator. Only 50% of curve points can be halved, and of those that can be halved two answers exist. A point in the Odd Subgroup can always be halved. One of the two resulting answers is also in the Odd Subgroup, and the other is not.

The most efficient methods use XR representation for curve points. The point (X,Y) is instead represented as (X,R); where R = Y/X is the ratio of Y to X. Two special case points exist, where X=0. The two special case points are the point-at-infinity, usually represented in the computer as (X,Y) = (0,0), and the curve mid-point, which has (X,Y) = (0,sqrt(B)). The XR representation for these points may be taken as just (X,Y).

In general, point halving performs at least as well as point doubling. The simplest practical method of computing a multiple of a point is known as Double-and-Add. A more refined variation is called Signed-Sliding-Window, which reduces the number of additions substantially but needs about the same number of doublings as Double-and-Add. The foregoing operations are well known to those of skill in the art. Each of these operations scans the binary representation of the multiplier from high-order to low-order bits, and intersperses doubling steps with occasional addition or subtraction steps. The formula for the multiplier is: k<=L; M = sum Bk 2^k; k=0; where L = log2(M), and Bk is the kth bit of the binary representation of M.

To use Halving instead of Doubling, the binary representation is scanned from low-order to high-order. The point P to be multiplied is presumed to be in the Odd Subgroup. The

Halve-and-Add method begins with an initial value V = (0,0) = the-point-at-infinity, and starts with Step 0. The method runs through Step L, where L is defined above. At Step k, if Bk = 1, the point P is added to V. Regardless of whether Bk=1, the step is completed by Halving V. After the Lth Step, the answer is V. Since V starts in the Odd Subgroup, and all intermediate steps leave it in the Odd Subgroup, the final answer V is also in the Odd Subgroup.

The computed multiple is (M/2^L)*P. If one is able to select the multiplier, a suitable multiplier may be selected. However, an arbitrary multiplier may also be used if it is in conjunction with a preparatory setup adjustment. If the order of the Odd Subgroup is J, then set L = ceiling(log2(J)). Then M' = M * 2^L (mod J) is computed. The binary representation of M' is used (in place of M) in the Halve-and-Add algorithm. The Halve-and-Add algorithm computes (M'/2^L)*P, which, since P is in the Odd Subgroup, turns out to be exactly the same as M*P. The refinements of Double- and-Add to produce Signed-Sliding-Window also work for Halve-and-Add, and produce the same improvements.

The order of the Odd Subgroup, designated as J, needs to be known. This is not usually a problem, since the order H of an elliptic curve group is routinely computed before it is used to guard against the chance that the order has no large prime factor. If the order H is computed, it can be checked by generating random points P and verifying H*P = point-at-infinity. It is relatively easy to compute J from H by simply shifting away the low order 0s of J. If J or H are not known, but P is known, 2^L * P can be pre-computed. M*P may be computed by starting with 2^L * P and using Halving to compute (M/2^L) * (2^L * P), which is M*P. If P is a generic point (not in the Odd Subgroup, or not known to be), it may be split into an Odd Subgroup point plus an Even Subgroup point, and these two pieces may be handled separately.

Special handling, which is discussed hereinbelow, is required for generic points not in the Odd Subgroup. If M was substantially smaller than J, then the new L used for Halving and Adding will have more steps than the old L used with Doubling and Adding. It is customary to use M of about the same size as J. Even if M is substantially smaller than J, the Halving and Adding method is sufficiently faster per step than Doubling and Adding, that Halving and Adding typically performs faster, even if more steps are needed. One exception occurs when M is less than sqrt(J), which is not the usual practice.

A discussion of the Point Halving Formula for Odd Subgroup Points When Trace(A) = 1 follows. The curve equation is Y^2 + X Y = X^3 + A X^2 + B, where Trace(A) = 1. The field

trace-mask is T. The point to be halved is (X,R), where R = Y/X. If X=0, then the special case is preferably handled as described hereinafter. First, compute M = Qsolve(X+A); then compute Tmp = X*(R+M); if Parity(Tmp & T) = 0, then add 1 to M and add X to Tmp; then compute Xh = Sqrt(Tmp), Rh = M + Xh + 1.

(Xh,Rh) is the halved point, and it is in the Odd Subgroup. A special case exists, when X=0. Depending on the application, the designer may know that this cannot occur, and omit the checking code. If R=0, the point-at-infinity is being halved, and simply returns the answer (Xh,Rh) = (0,0). If R is not 0, the routine has been mistakenly called with the curve mid-point, which is not in the Odd Subgroup and causes return of an error value, or causes some other error handling action.

With minor adjustments, this formula also works for halving generic curve points. The needed changes are: (1) The Qsolve, which computes M can fail in which case, the point is not capable of being halved; (2) The "If Parity" line should be regarded instead as a Fork; (3) One branch is the "= 0" branch, and the other is the "!= 0" branch; (4) Each branch gives one of the two half-points and no particular promise is made that either half-point is in the Odd Subgroup.

The Halving formula for generic points also works for curves with Trace(A) = 0. However, the situation with halving points in the Odd Subgroup is comparatively complicated. Although it is preferable to stay within the Odd Subgroup, checking whether a point is in the Odd Subgroup is more difficult. It is important to look ahead to determine which of the two half-points is the Odd Subgroup point. If the size of the Even Subgroup is 2^K, the procedure looks ahead K halving steps to detect halving failure. If the wrong half-point is picked after halving an Odd Subgroup point, all of the branches of the subsequent "halving tree" fail at the Kth subsequent halving step, and which path is selected through the lookahead tree is irrelevant.

The Trace test "If Parity(Tmp & T) = 0" does a computationally inexpensive one-step lookahead, guaranteeing that the (Xh,Rh) point will be halvable. When Trace(A) = 1, then the Even Subgroup is of size 2, so K=1, and one step of lookahead is sufficient. If Trace(A) = 0, then K>=2. When K=2, the order of the elliptic curve group is four (4) times an odd number. This is a common case, occurring about half the time when A=0 in the elliptic curve equation.

In this case, only two steps of halving lookahead are needed to stay in the Odd Subgroup. The second step can be provided by the Parity test, but the required fixup to M and Tmp must be done to the values in the previous round of Halving. It is possible to salvage some of the

intermediate computations, so the cost of the misstep is limited to roughly one wasted Qsolve plus one wasted multiplication. Since missteps only occur about half the time, this is not overly costly.

At the end of the Halving computation for point multiplication, it is still necessary to do the K-step halving lookahead to make sure that the final point is in the Odd Subgroup. The algorithm can be adjusted to omit the final few halving steps, but the last halving actually done must be checked with lookahead.

One may ask why not just ignore the lookahead steps and simply perform halving? The disadvantage of such an approach is the cost of adding the extra point; which is needed at least one-half of the time, thus raising the average cost of halving. This will be computationally less expensive than the K-step lookahead computational cost when K is large, but it makes Halving computationally less competitive with Doubling. It is possible to combine the generator with the base point P ahead of time, and thus save some time when both P and a generator must be added.

If this approach is used, the final point must be forced into the Odd Subgroup to obtain a canonical result. This can be done either by splitting the point into the sum of an Odd Subgroup point (the final answer) plus an Even Subgroup point (discarded), or equivalently, doing K additional halving steps and then "Doubling back" K steps.

The Halving method has been implemented in a computer program. On a 233MHz DEC Alpha, the new method of point-halving takes 8.45 microseconds to halve a point, compared with point-doubling times of 27-35 microseconds for various doubling methods. Halving is as useful as doubling. Although the raw speedup of halving is a factor of 3.5-4, this advantage will be diluted somewhat by necessary point-addition operations. Since Doubling is the principal operation, the Halving advantage will translate into at least a factor of two (2) in overall point multiplication speed, thus making elliptic curves more competitive as a public key option.

It is necessary to switch to XY form when a point addition is required. The Transition from XR to XY is trivial, requiring only one multiplication. The transition directly from XY to XR requires a reciprocal, which makes the following alternative halving algorithm useful. Halving in XY representation with two multiplies: If X=0, handle special case as described for XR algorithm; compute M = Qsolve(X+A); compute Tmp = Y + X * M; if Parity(Tmp & T) = 0, add 1 to M and add X to Tmp; compute Xh = Sqrt(Tmp), Rh = M + Xh + 1, Yh = Xh * Rh; Xh, Yh is the halved point.

Although the foregoing formula requires more computation than XR form, it uses the more standard XY format for the curve points. This can also be used to transition from XY format (as might result after a point addition) to XR format for the half-point, skipping the computation of Yh. The need to switch representations in the context of a point-doubling algorithm is well known to those of skill in the art. Those same considerations apply to point-halving.

The principle of "ambiguity-resolution by subgroup membership" is used to choose which of two half-points is in the Odd Subgroup. This principle has other uses as well. In computing a large integer multiple K of a curve point P, K may be represented in balanced-ternary, radix 3 with digits -1,0,1. Sliding Window methods can be used to reduce the number of non-zero digits. Under point triplication in Projective Coordinates, the X-coordinate of a triplicate point can be computed fairly computationally inexpensively. If the X coordinate of P is (N,D) in projective coordinates, *i.e.*, X = N/D, the X coordinate of the tripled point 3P is N * (N^8 + B N^2 D^6 + B^2 D^8) / D * (N^8 + N^6 D^2 + B^2 D^8). B is from the curve equation, and the formula does not depend on the A term of the curve equation.

The foregoing may be computed in five multiplications, a considerable improvement over the usual cost of point triplication, because the Y coordinate need not be computed. Squaring is computationally inexpensive, as is multiplication by the low-hamming-weight constant B. One may compute the terms N^2 D^6 and N^6 D^2 as N^2 D^2 times D^4 and times N^4. If several triplications are performed in this way, thus reaching 81P, a point addition must be performed, and the Y coordinate must be recovered.

Some Y coordinates can be recovered by computing X = N/D and solving the curve equation (a quadratic) for Y. Solve R^2 + R = X + A + B/X^2 for R, then Y = X R. Compute X and 1/X with only one inversion by first computing 1/(N*D). According to the foregoing, it is not known if the found Y corresponds to 81P or -81P. This ambiguity is resolved by adding P, and obtaining either -80P or 82P. These alternatives can be distinguished if the group order is a multiple of 4, and the order of P is divisible by 4. In the simplest case, where the group order in an odd multiple of 4, one of the two prospective points can be quartered, but the other cannot. While the foregoing may appear to be inefficient, most of the arithmetic for the point additions can be shared, and odd multiples of P can be added instead of P. Accordingly, the addition can

be performed with the next Sliding-Window digit. Since a real X-coordinate is recovered, D=1 may be used at the start of the next triplication cycle, saving a few multiplications.

Ambiguity resolution has at least one other use. Projective point doubling is comparatively computationally inexpensive, when using only the X coordinate. If the X-coordinate of the point P is X, then Xd = X^2 + B/X^2. Projectively, with X represented as (N,D), the double is (N^4 + B D^4, N^2 D^2), which requires only a single multiplication, either N*D or N^2 * D^2. A quadruplication requires only two multiplications and so forth.

If a low-hamming-weight multiple of P is to be computed with a long series of point doublings between the additions. These doublings are comparatively computationally inexpensive. If the projective X-coordinate of 1024 P with ten doublings has been computed, then Y needs to be determined. Y may be calculated, as discussed hereinabove, by solving the curve equation, which gives the Y-coordinate of either 1024P or -1024P. P is then added, obtaining either 1025P or -1023P, which can be distinguished because one is a triple of another point and the other is not a triple.

It is important that the curve order be a multiple of 3 (empirically, lots of curves meet this), and that the point P not be a triple of another point, which is possible by starting with a suitable initial point P0 (doubling preserves the property). It is possible to test whether a point Q is triple by attempting to solve the equation 3 Z = Q for the point Z, which involves ninth degree polynomials with mostly 0 coefficients that can be solved by the matrix method that Rosing explains for cubics. If Z is found, the result is -1023P, otherwise the result is 1025P.

Qsolve may be used in Solving the Quadratic Equation Z^2 + Z = C in a GF[2^K] field. Some shortcuts that may be used in solving the foregoing equation are discussed hereinbelow. The first shortcut is the Half-Trace explained hereinabove, which works in odd-degree fields. The function f(Z) = Z^2 + Z is LINEAR in GF[2^K] fields. The inverse function Qsolve is also linear. This means that C can be split into its constituent bits or bytes, table lookup can be used to solve the individual bits and bytes, and the solutions can be added together to obtain Z.

According to the foregoing, half of the Cs have no solution, and the other half have two solutions, Z and Z+1. C is solvable if-and-only-if Trace(C) = 0. If U is the field generator, some powers of U will have trace 1 and usually some will have trace 0. Suppose U^t is the smallest power of U with trace 1. In an odd degree field, GF[2^odd], this will be t=0, since Trace(1)=1 in this case. In any case, exactly one of C and C + U^t is solvable.

The solution table for the bits or bytes of C may be prepared by entering the solution for either C or C + U^t, whichever is solvable. The trace of the bit-or-byte in an extra bit position of the solutions may be entered in the solution table. The low-order bit of each entry is available, since the U^0 = 1 term of a solution is useless -- the two solutions of the quadratic differ by 1. At the end of combining the solutions of the pieces of C, the low order bit will have the trace of C; if it is a 0, then C is solvable. Otherwise, the solution for C+U^t is provided, which is useful under some circumstances. The foregoing discussion applies to either polynomial basis or normal basis representations. If a projective representation is being used, the preferred method is to convert the number C to a polynomial basis.

An important shortcut is available in normal basis that increases speed and eliminates the need for a solution table. Such an advantage may be compelling if the cost of multiplication and inversion do not exceed the costs in polynomial basis by a significant amount. Let Qsolve(C) represent the solution Z of the equation Z^2 + Z = C. For definiteness, suppose that the low-order bit of Z is 0, and that C is solvable.

A relationship exists between Qsolve(C) and Qsolve(C^2) as follows: Qsolve(C^2) = C + Qsolve(C) = Qsolve(C)^2, ignoring the low-order bit. In a normal basis, the successive bits represent powers U^(2^N), and Qsolve(C) can be computed by riffling an xor down the bits of C, from U^(2^(degree-1)) down through U^1. The trace of C is the parity of the representation of C, so if the riffle finishes with a 0, C is solvable.

In a polynomial basis, the Qsolve relationship can be used. Even powers of the generator, U^(2k), can be folded to their square roots. If a binomial or trinomial is being used as the field polynomial, half of the odd powers of the generator can also be folded away, leaving only degree/4 of the bits to participate in the table lookup.

If a field-tower representation is being used, the even powers of the outer field generator can be folded. Typically, the odd powers can also be folded by using the outer-field extension polynomial. This will mostly reduce the problem to Qsolve of lower-field elements. If the extension is of degree 2, and the extension equation is V^2 + V = K, with K in the lower field, a typical upper-field element is C V + D. This element is solvable if-and-only-if C is solvable in the lower field as follows: Qsolve(C V + D) = E V + F; where E = Qsolve(C), and F = Qsolve(D + K E^2). If the Qsolve for F fails, add 1 to E, and add Qsolve(K+U^t) to F. Or, just recompute F from the formula.

A clever programmer will precompute and cache Qsolve(K+U^t). If the lower field is odd-degree, take K=1 and t=0, and the formula for F simplifies to F = E + Qsolve(D+E).

An example with extension degree 3: suppose the field equation is V^3 + V = K, with K in the lower field, then a typical upper-field element is C V^2 + D V + E, and the equation to be solved is Z^2 + Z = C V^2 + D V + E.

The V^2 term can be folded into the V term with the relationship Qsolve(C V^2) = sqrt(C) V + Qsolve(sqrt(C) V). The sqrt is comparatively computationally inexpensive. The Qsolve(E) can be separately split off, and table-lookup or bit-or-byte splitting for Qsolve of the V term can be used.

In another example, with extension degree 5, Suppose the field equation is V^5 + K V = 1. A typical upper-field element is C V^4 + D V^3 + E V^2 + F V + G. The V^4 term can be folded into the V^2 term, which can be folded into the V term. But the V^3 term may also be discarded by replacing D V^3 with D V^8 + K D V^4. The method is: (1) replace the V^3 term; (2) fold the V^8 term into V^4; (3) fold that into V^2; (4) fold that into V; (5) use table-lookup on the V term; and (6) separately solve G.

These principles also apply to towers with more than two levels. Point-Halving is most effective when the order of the elliptic curve group is twice an odd number, when the point to be multiplied is in the Odd Subgroup, and when the user is free to select the multiplier. Nevertheless, point-halving is still useful when these conditions are not satisfied.

If the user is not free to select the multiplier, but must instead use a multiplier M that is provided, the user can convert the multiplier to an equivalent multiplier M' to use with point-halving, so long as the group order is known (the formula is set forth above). Alternatively, when the base point to be multiplied is known ahead of time, the base point can be pre-doubled enough times to compensate for the later halving.

If the point to be multiplied is not in the Odd Subgroup, the point can be split into the sum of an Odd Subgroup point and an Even Subgroup point, each of which is separately multiplied, and the resulting points are added. The Odd Subgroup point is handled according to the principles set forth hereinabove.

Suppose the order of the Even Subgroup is 2^K. The even-subgroup point is multiplied by the low-order K bits of the multiplier. In typical cases, K is 3 or less, and table lookup can be used. The Even Subgroup point will be one of the 2^K elements in the Even Subgroup, and

it will appear in the table. The Even Subgroup is cyclic, so the point's table-index is multiplied by the low-order K bits of the multiplier, and the result trimmed to K low-order bits and used to look up the answer. Note that the table need only contain half of the points, since the others will have the same X-coordinate. Also, a significant chance exists that the X-coordinate is 0, and the subgroup point is either (0,0), the point-at-infinity, or (0,sqrtB) (the curve midpoint). These can be handled efficiently even without a table, especially in the case when K=1.

One defining property of an Odd Subgroup point is that it can be halved indefinitely. Any other point can be halved at most K-1 times. For this test, either half-point may be selected at each halving step. For example, if the point can be halved K times, it is in the Odd Subgroup. Typically, the trace function can be used to determine if the current halving step will succeed. When K=1, no halvings actually need to be done, because the trace function does all the work.

If the Hth halving fails, a fixup is required. Suppose Q is a point that generates the Even Subgroup, then the generator Q may be subtracted from the point that cannot be halved, which will make it capable of being halved. Then the halving operation is continued, subtracting Q again, whenever needed at any subsequent halving failure, until K halvings have been completed. The last halving can simply be predicted by using the trace.

At this point the Odd Subgroup and Even Subgroup points need to be computed. The pattern formed by the incapability of being halved for each of the halvings is recorded and regarded as a bit pattern in reverse. A point capable of being halved is a 0 bit, a point that is not capable of being halved is a 1 bit. K bits exist that correspond to the K halvings. The final halving determines the high-order bit, and the first halving determines the low- order bit of a K-bit number N. The Even Subgroup element is simply N*Q, which may be determined by table lookup or computed directly. The Odd Subgroup point is computed by subtracting the point N*Q from the original generic point.

If a multiplier is chosen, but applying the multiplier to a generic point splits the generic point into the sum of an Odd Subgroup point and an Even Subgroup point, then the Even Subgroup point may usually be discarded, and the Odd Subgroup point used in place of the generic point. To calculate the integer-equivalent-multiplier, M/2^L (mod J) can be used for Odd Subgroup points. (J is the order of the Odd Subgroup.) If an equivalent multiplier for general points is needed, then 2^K * (M/2^(L+K) (mod J)) may be used. The order of the Even Subgroup is 2^K.

Multipliers may be expressed in non-standard radices and as algorithms. Expression in non-standard radices and as algorithms may be applied to elements of any group, not just elliptic curves. The multiplier is typically expressed in binary, but other options exist. If subtraction of points or group elements is hard, but there is a method to negatively double a point, going from P to -2P, then it is natural to convert the multiplier to radix -2 (negabinary). When using point triplication, then the multiplier will be converted to ternary. Balanced ternary may be used, with digits -1, 0, and 1. Special curves with complex multiplication may use Gaussian complex integers as multipliers. Typically the unusual numbers have equivalent integer multipliers within the group.

For point-halving, the radix is ½. For point-thirding, the radix is 1/3. Some special curves have easy point-thirding algorithms. It would be equally easy to use the negative of point halving, with radix -1/2. It is also possible devise a scheme for multiplying a point by 3/2, or -4/3, and use corresponding radices. A scheme that had good algorithms for both point doubling and tripling may use a mixed radix scheme, using both 2s and 3s.

If a user is picking the multiplier, a random digit string can be used in the preferred radix. The typical requirement is that the string be selected from a large enough space. Roughly 2^160 possibilities is current practice, although somewhat smaller numbers such as 2^112 may be acceptable for low security applications. It is preferable that the selection be reasonably uniform, with no "popular values" that are much more likely to be selected. Popular values that have 10-fold extra likelihood are not a problem, but popularity reaching higher than 10-fold extra likelihood reduces security. As a rule of thumb, the security should be derated by the popularity. A scheme that selects from 2^200 possibilities and had maximum popularity 2^20 still has security 2^180.

It is preferable that different choices of digit strings lead to different multipliers. For radices discussed above, it is sufficient to use the correct set of digits to avoid accidental overlapping multipliers (a multiplier is typically popular, if it has lots of different representations). In general, digits can go from 0 up to limit-1, or from -(limit-1)/2 to limit/2 in balanced schemes. Limit is the radix, when it is a positive integer, or its absolute value when it is a negative integer (radix -2 has limit 2), or the larger of |numerator| and |denominator|, when the radix is a fraction. When the radix is complex, first take the norm. If these rules are followed, the maximum overlap is about limit, and often it is 1 or 0.

An interesting danger and opportunity exists. One may be tempted to use random addition-subtraction chains as an equivalent multiplier. The temptation arises because the entropy of the random choice of which elements of the chain to add or subtract contributes to the overall multiplier entropy, allowing many fewer add/sub/double steps to achieve a selection space of 2^160 choices. This practice is risky for ordinary addition/subtraction chains, since many different chains lead to identical multipliers, giving a severe popular-values problem. However, when doubling, halving, or tau-ing are cheap, the addition chain scheme can be corrected by using many doubling steps and the like between additions. Where tau-ing is a bit-rotation, applying a random k-bit rotation to the left (multiplier tau^k) or to the right (multiplier 1/tau^k) between addition/subtraction operations is a high entropy manipulation, and will give good security for minimal computation. If rotation cost depends on k, or if left and right rotations have different costs, it is typically preferable to limit the positive and negative range of k.

One reasonably secure method is easy to use. If the group size is much larger than the security requirement, then it is safe to choose low-hamming-weight multipliers, thus substantially reducing the number of addition-like steps. For example, suppose the security requirement is 2^160, but the group has order around 2^256, with a prime divisor around 2^255. Then a random number of 255 bits with hamming-weight 40 could safely be selected as the multiplier, since the number of choices, binomial(255,40) exceeds 2^160. This would require about 255 doublings, but only 40 additions in a simple double-and-add scheme.

If both addition and subtraction are being used, and have a few more digits available such as 3,5,7, a smaller group can be used while achieving the same level of security. This method is applicable to both halving and doubling, and the idea extends to other radices. As the computational cost of doubling/halving/tauing drops relative to the cost of addition/subtraction, it is important to rebalance the choice of multipliers by moving towards the computationally less expensive operations.

Shamir's trick is useful in computing a linear combination of two multipliers (M,N) dotted with two curve points (P,Q), such as M * P + N * Q. This arises, for example, in checking a digital signature. The procedure is to precompute P+Q, and then run a single double-and-add bit-scan over both M and N; if a bit of M is 1, add P to the running value; if a bit of Q is 1, add Q; if both bits are 1, add P+Q. The number of doubling steps drops from log2(M)+log2(N) to max(log2(M),log2(N)).

Generally, Halving can be used to replace Doubling, by either adjusting the points P and Q, or adjusting the multipliers M and N, or some of each. The strategies are the same as the single point case. Extensions to more than two curve points are also possible.

In the halving scheme, it is natural to use the Signed-Sliding-Window method. This uses a table of odd multiples of the base point, such as 1, 3, 5, and 7, and adds or subtracts a multiple after doing several halving steps. It is equally possible to use fractional digits such as 1/16, 3/16, 5/16, and 7/16; which is better will depend on details such as the available hardware and the like.

Many variations of the invention are possible. For example, the user might choose different curve equations, or use another representation besides XR that is computationally interconverted with XR in a computationally economic manner.

Qsolve, viewed as an operator, commutes with many other operators including without limitation: (1) squaring; (2) square-root; (3) the polynomials Z^4+Z & Z^4+Z^2+Z and their inverses, and (4) many others. This allows great flexibility in rearranging the equations for the elliptic curve operations to produce mathematically equivalent results, or results that are economically converted to mathematically equivalent results, while offering no significant advantage over the present methods. A plurality of different, but equivalent, equations for elliptic curves exist. The methods of the present invention can be transformed as well to apply to other curve equations, generally with no particular advantage or disadvantage.

The methods of the present invention are applicable to many other groups, although the detailed formulas will differ. In particular, other algebraic curves, such as hyperelliptic curves, and algebraic surfaces, seem susceptible to disambiguation by subgroup membership.

The use of alternative methods such as point-halving or point-(1/tau)- ing or even addition chains to do key exchange is blind-interoperable with the standard methods like Double-and-Add, as well as with other alternative methods. For creating elliptic- curve signatures, the explicit integer equivalent value of the multiplier being used must be known. In all cases, this value can be calculated, typically comparatively computationally inexpensively.

The algorithms of the present invention are independent of the particular methods used for the field arithmetic. The algorithms will work with any method of doing multiplication or division, or squaring or square-rooting, or solving the special quadratic equation.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all

respects only as illustrative, and not restrictive. The scope of the invention is, therefore, indicated by the appended claims, rather than by the foregoing description. All changes that come within the meaning and range of equivalency of the claims are to be embraced within their scope.

5

CLAIMS

1. A method comprising:

selecting an elliptic curve method;

executing a point modification algorithm to manipulate points of the elliptic curve method;

generating a signal having a distinct characteristic using the selected elliptic curve method;

providing substantive content; and

manipulating the substantive content using the distinct characteristic.

2. The method of claim 1, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

3. The method of claim 1, wherein manipulating the substantive content comprises encrypting the substantive content.

4. The method of claim 1, wherein manipulating the substantive content comprises decrypting the substantive content.

5. The method of claim 1, wherein the distinct characteristic is selected from a key and a signature.

6. The method of claim 2, wherein point fractioning is selected from integral point fractioning, corresponding to a denominator that is an integral number.

7. The method of claim 2, wherein point multiplying is selected from integral multiplication, imaginary multiplication, and complex multiplication.

8. The method of claim 1, further comprising dynamically specifying the point modification algorithm in lieu of specifying the modification operation in advance.

9. The method of claim 2, further comprising selecting a first point for execution of the point modification algorithm, based on a selected property.

10. The method of claim 9, wherein the selected property is a membership condition placing the first point in a subgroup.

11. The method of claim 10, further comprising repeating the point modification algorithm with a second point selected by another entity selected from a deterministic process, a random process, and a third party.

12. The method of claim 11, wherein the second point is communicated to the point modification algorithm in a format selected from a message and a certificate.

13. The method of claim 2, further comprising selecting a first point and pre-modifying the first point by a modification operation configured to compensate for some of the processing steps, added and corresponding to execution of a series of steps in accordance with the method.

14. The method of claim 1, further comprising sending by a sender and receiving by a receiver the substantive content, and wherein the sender executes a first operation during modification for encryption and the receiver executes a second and distinct operation during modification for decryption.

15. The method of claim 1, wherein generating the distinct characteristic further comprises creating a distinct characteristic selected from a symmetric key configured to be shared by two or more parties, a decryption code for processing an encrypted signal, a digital signature, an asymmetric key, and an authentication.

16. The method of claim 1, further comprising selecting a point and wherein the point is of a type selected from a hyperelliptic curve, an algebraic curve, and abelian variety.

17. The method of claim 1, wherein modifying a point further comprises halving a point represented in a cartesian space and a point existing in a mapped cartesian space having a cartesian representation.

18. The method of claim 17, wherein halving further comprises executing a single multiplication per halving operation.

19. The method of claim 18, further comprising selecting a point characterized by a cartesian tuple and completing halving using no more than two field multiplications.

20. The method of claim 19, wherein halving further comprises negative halving including computation of a minus one-half multiple.

21. The method of claim 1, further comprising computing a fractional multiple of a point selected from a proper fraction, an improper fraction, and a complex fractional multiple.

22. The method of claim 18, further comprising determining a selection of points to execute a halving operation with respect to, based on testing for membership in a subgroup.

23. The method of claim 22, wherein testing further comprises reliance on a bit mask of coordinates corresponding to points in the subgroup.

24. The method of claim 23, wherein testing is executed by testing whether a halving procedure can be executed an arbitrary number of times selected by a user.

25. The method of claim 24, further comprising determining which of a selected number of points is to be used.

26. An apparatus comprising:

a system for creating a distinct characteristic configured to support cryptographic manipulation of information;

a memory device operably connected to the system for storing the distinct characteristic and executables programmed to operate on the distinct characteristic;

an encrypting device operably connected to the system for controlling an encryption process using the distinct characteristic;

the system further configured to execute an elliptic curve method for generating the distinct characteristic; and

the system further configured to execute a point modification algorithm for generating the distinct characteristic.

27. The apparatus of claim 26, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

28. The apparatus of claim 26, wherein the distinct characteristic is configured to be processable by the system for divulging independently to two independent parties a secret to be shared by the two independent parties.

29. An article comprising a computer-readable memory storing operational and executable data, the operational and executable data comprising:

an encryption engine for operating on distinct characteristics configured to encrypt substantive content representing information;

the encryption engine, further comprising a distinct characteristic generation module for operating on the distinct characteristics;

the distinct characteristic generation module, further comprising an elliptic curve module for providing the distinct characteristics; and

the elliptic curve module, further comprising a point modification algorithm for calculating points related to the distinct characteristic.

30. The article of claim 29, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof.

31. The article of claim 30, wherein point fractioning is selected from integral point fractioning, corresponding to a denominator that is an integral number.

32. The article of claim 30, wherein point multiplying is selected from integral multiplication, imaginary multiplication, and complex multiplication.

33. The article of claim 29, further comprising dynamically specifying the point modification algorithm in lieu of specifying the modification operation in advance.

34. The article of claim 30, further comprising selecting a first point for execution of the point modification algorithm, based on a selected property.

35. The article of claim 29, wherein the distinct characteristics are selected from a key and a signature.

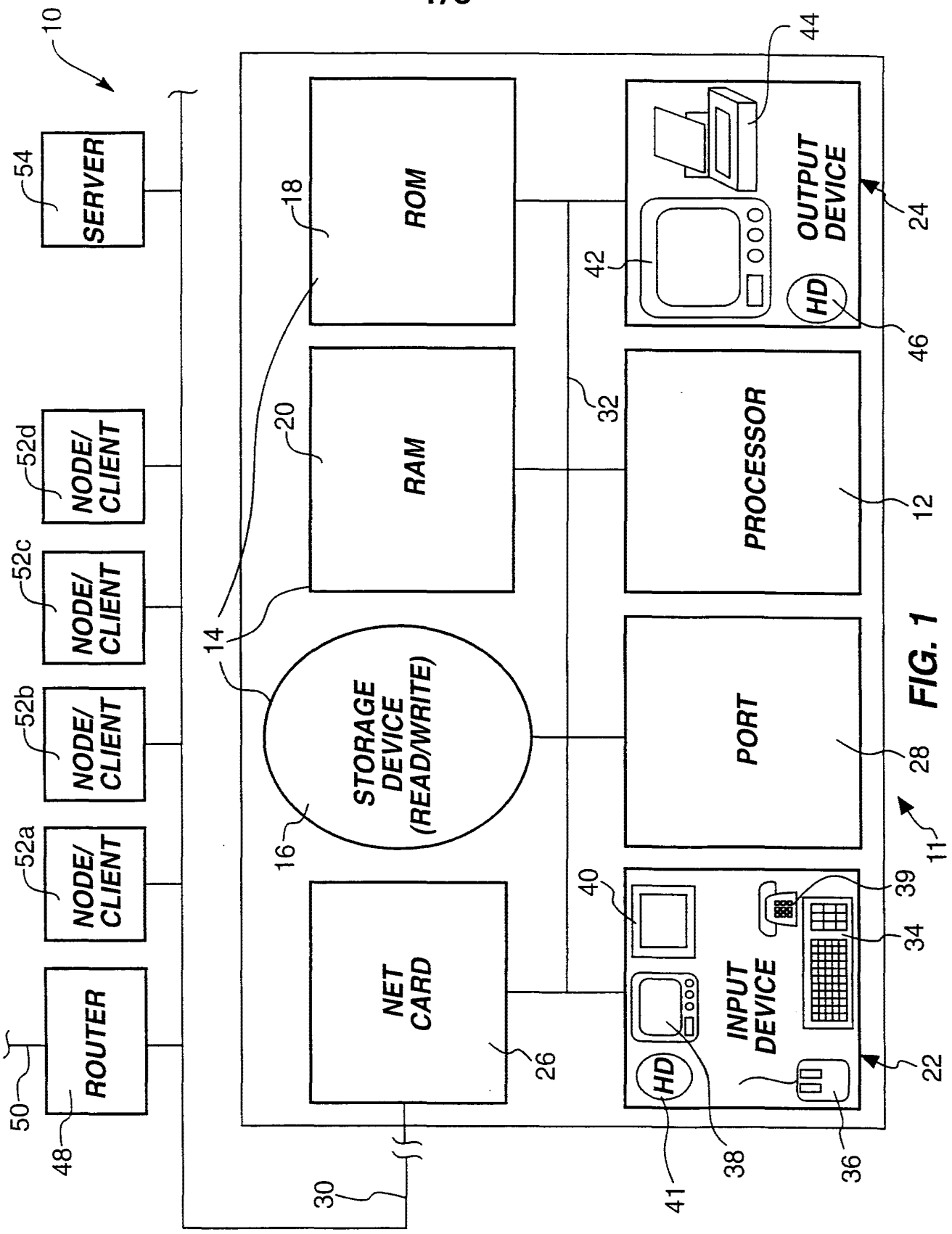

10
SERVER
54
NODE/ CLIENT
52d
NODE/ CLIENT
52c
NODE/ CLIENT
52b
NODE/ CLIENT
52a
ROUTER
50
48
ROM
18
RAM
20
STORAGE DEVICE (READ/WRITE)
16
NET CARD
26
PROCESSOR
12
32
PORT
28
OUTPUT DEVICE
24
42
HD
46
44
INPUT DEVICE
22
HD
41
38
36
40
34
39
14
30
11

FIG. 1

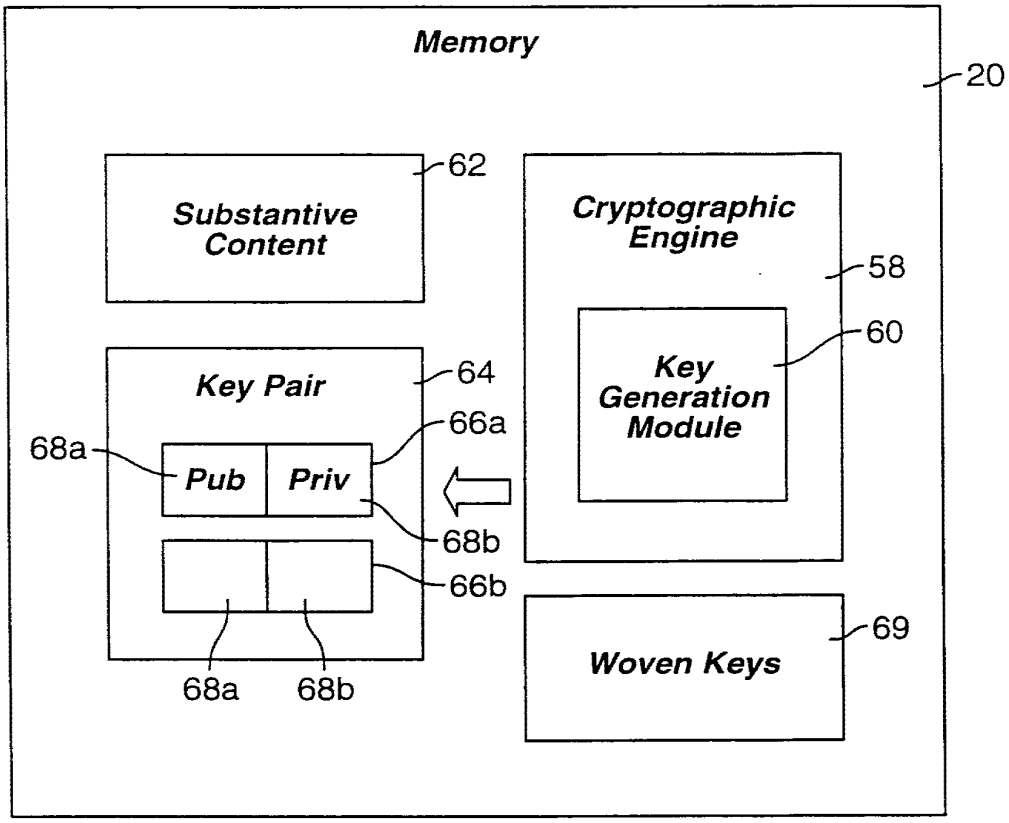

Memory
20
Substantive Content
62
Cryptographic Engine
58
Key Generation Module
60
Key Pair
64
66a
68a
Pub
Priv
68b
66b
68a
68b
Woven Keys
69

FIG. 2

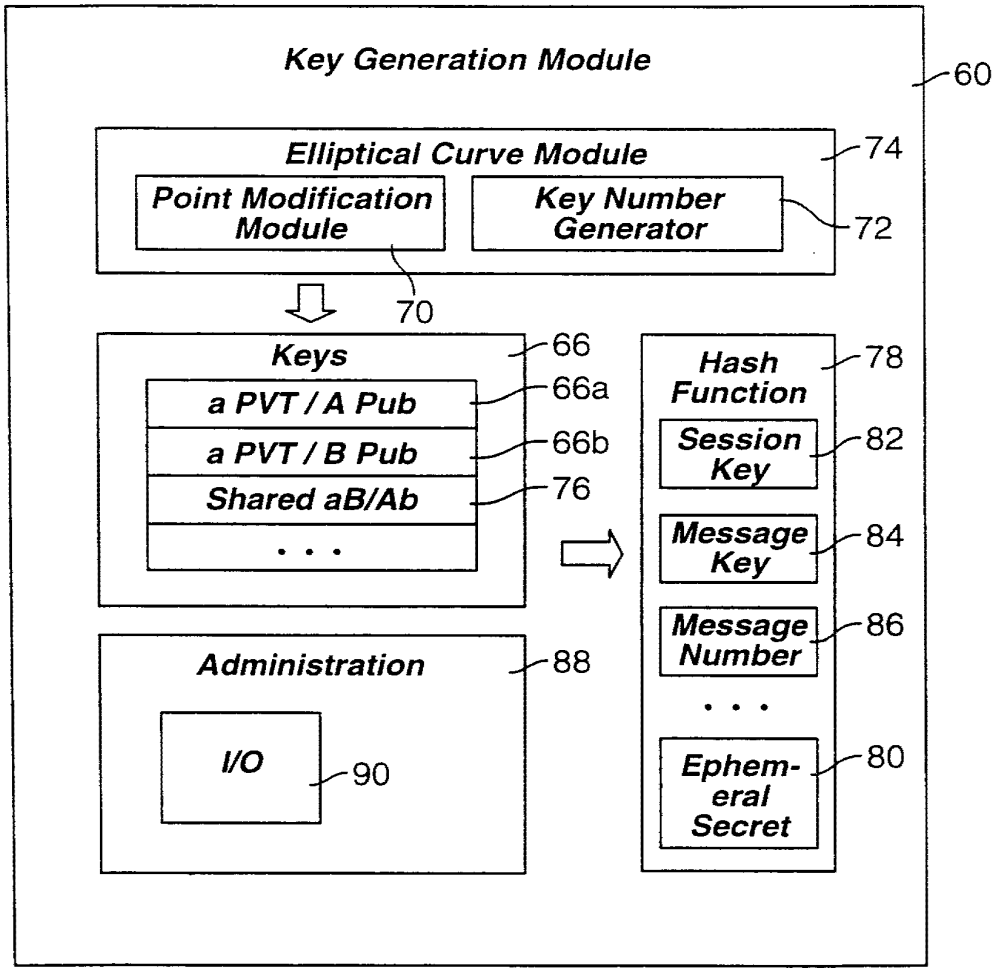

Key Generation Module
60
Elliptical Curve Module
74
Point Modification Module
Key Number Generator
72
70
Keys
66
a PVT / A Pub
66a
a PVT / B Pub
66b
Shared aB/Ab
76
. . .
Hash Function
78
Session Key
82
Message Key
84
Message Number
86
. . .
Ephem-eral Secret
80
Administration
88
I/O
90

FIG. 3

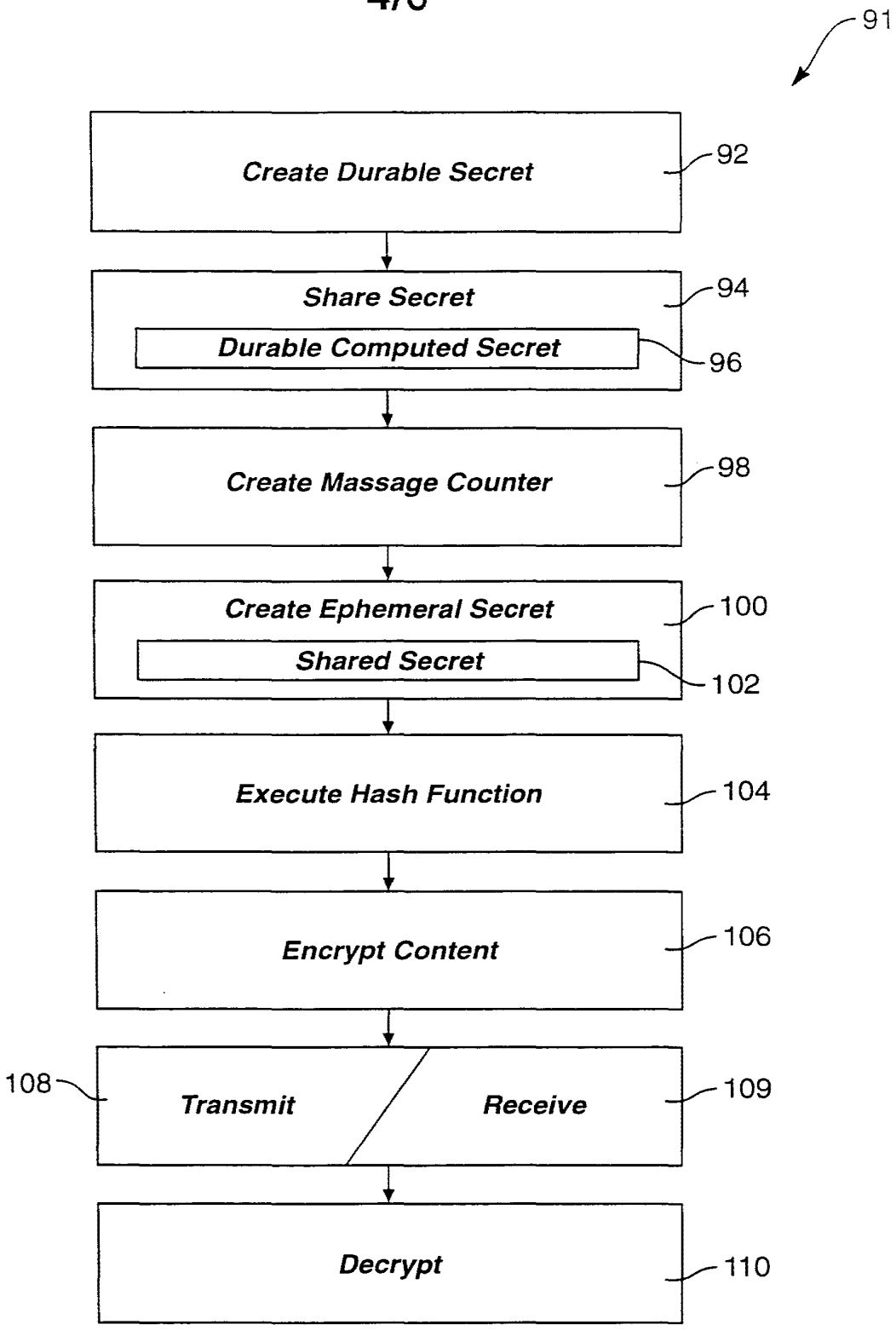

91
Create Durable Secret
92
Share Secret
94
Durable Computed Secret
96
Create Massage Counter
98
Create Ephemeral Secret
100
Shared Secret
102
Execute Hash Function
104
Encrypt Content
106
108
Transmit
Receive
109
Decrypt
110

FIG. 4

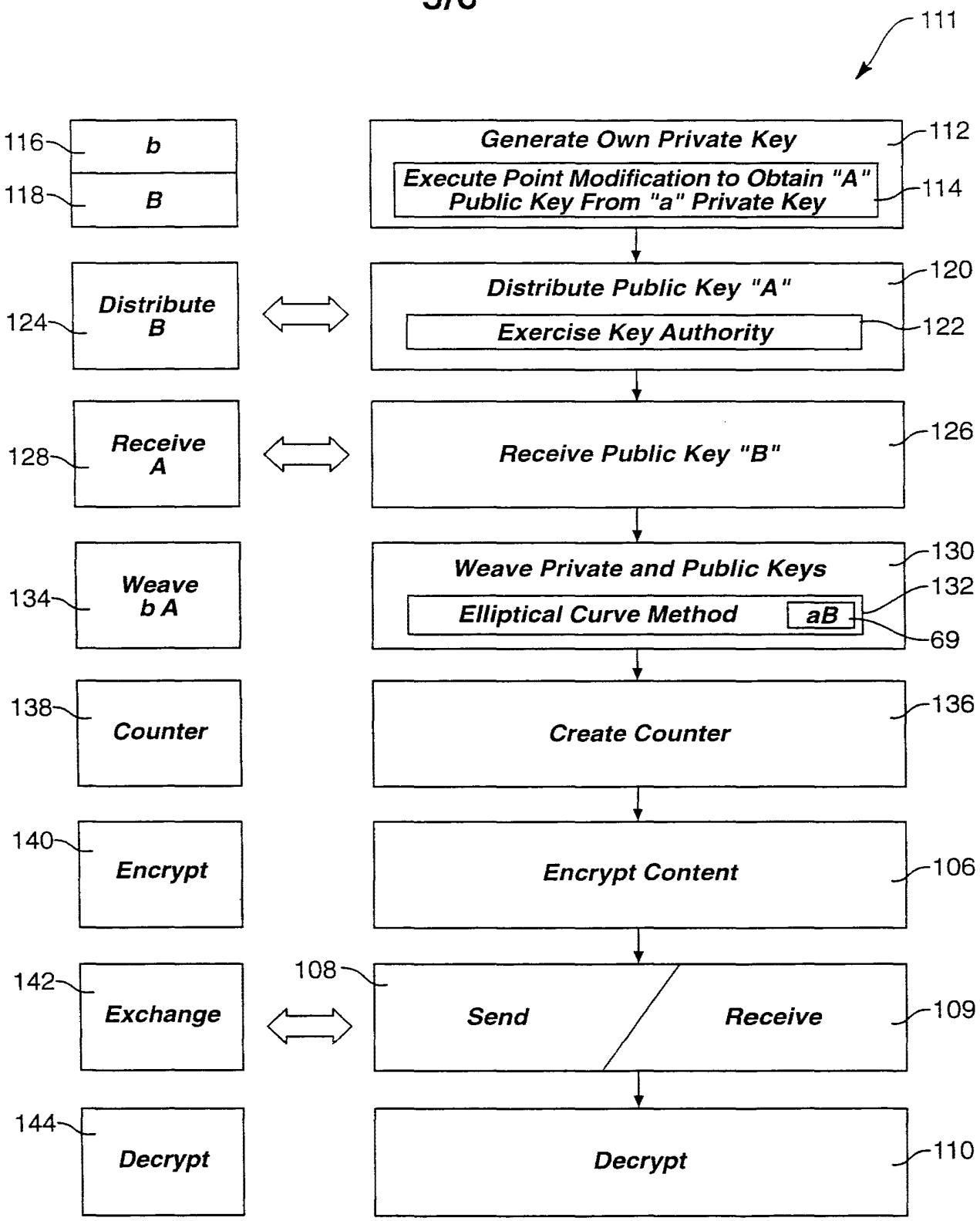

111
116
b
118
B
Generate Own Private Key
112
Execute Point Modification to Obtain "A" Public Key From "a" Private Key
114
124
Distribute B
Distribute Public Key "A"
120
Exercise Key Authority
122
128
Receive A
Receive Public Key "B"
126
134
Weave b A
Weave Private and Public Keys
130
Elliptical Curve Method
aB
132
69
138
Counter
Create Counter
136
140
Encrypt
Encrypt Content
106
142
Exchange
108
Send
Receive
109
144
Decrypt
Decrypt
110

FIG. 5

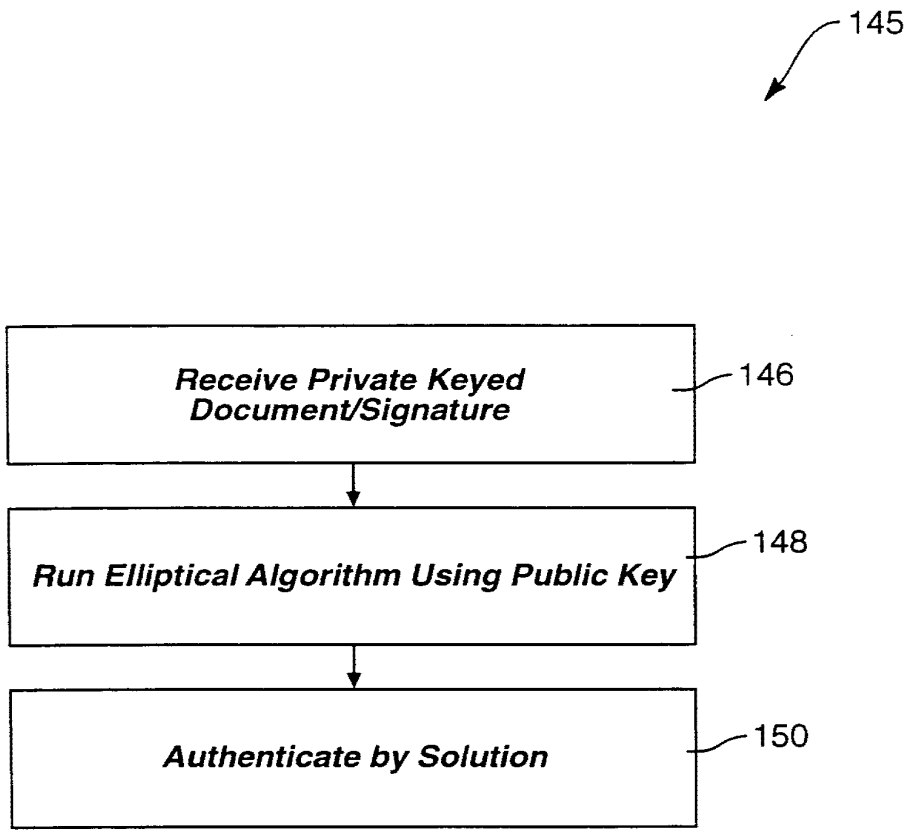

145
Receive Private Keyed Document/Signature
146
Run Elliptical Algorithm Using Public Key
148
Authenticate by Solution
150

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/31014

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/08, 9/16, 9/28, 9/30

US CL : 380/28, 30, 44, 262, 279, 282, 286

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/28, 30, 44, 262, 279, 282, 286

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Alfred J. Menezes, "Elliptic Curve Public Key Cryptosystems," Kluwer Academic Publishers, 1993.

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	SCHROEPPEL, R. et al., Fast Key Exchange with Elliptic Curve Systems, Advances in Cryptology - CRYPTO '95, 31 August 1995, pages 43-56, especially page 44 (paragraphs 4-7), pages 45-46 (section 3.1), pages 46-47 (section 3.3), pages 49-51 (section 4.4), pages 51-53 (section 5), pages 53-54 (section 6), and page 54 (paragraph 1).	1, 3-5, 14-16, 26, 28, 35 ---------- 2, 6-13, 17-19, 21-23, 27, 30-34
Y	KOYAMA, K. et al., New Public-Key Schemes Based on Elliptic Curves over the Ring Zn, Advances in Cryptology Crypto '91, 1991, pages 252-266, especially pages 258-260 (sections 6.2 and 7).	2, 6-13, 17-23, 27, 30-34
Y	VANSTONE, S.A. et al., Elliptic Curve Cryptosystems Using Curves of Smooth Order over the Ring Zn, IEEE Trans. on Information Technology, July 1997, Vol. 43 No. 4, pages 1231-1237, especially pages 1233-1235 (sections VII and VIII).	2-13, 9, 10, 13, 21, 27, 30-34
Y,P	US 6,141,420 A (VANSTONE et al.) 31 October 2000 (31.10.2000), column 16, lines 23-67 and column 17, lines 1-67.	8, 33
Y	US 5,442,707 A (MIYAJI et al.) 15 August 1995 (15.08.1995), column 1, lines 49-62 and column 12, lines 10-37.	11, 12
Y	US 5,805,703 A (CRANDALL) 08 September 1998 (08.09.1998), column 7, lines 63-67 and column 8, lines 1-51.	11, 12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

15 January 2001 (15.01.2001)

Date of mailing of the international search report

23 FEB 2001

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Tod R. Swann

James R. Matthews

Telephone No. (703) 308-0873

Form PCT/ISA/210 (second sheet) (July 1998)

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	Michael K. Henry/Christie Loven
Attorney Docket Number:	29907-0037001

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Independent claims in excess of 3	1201	1	250	250
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	1801	1	930	930
		Total in USD ($)		**1180**

Electronic Acknowledgement Receipt

EFS ID:	13773294
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Christie Loven
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	29907-0037001
Receipt Date:	18-SEP-2012
Filing Date:	23-JAN-2006
Time Stamp:	13:05:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1180
RAM confirmation Number	9963
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Request for Continued Examination (RCE)	29907-0037001_RCE.pdf	143775 b3e331b005f1e832ad3c63fc1681a8f7ecaa6d6c	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2		29907-0037001_Response.pdf	94473 5993c09835c848f4a417fc9fccd5d3cc2ee9812f	yes	11
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	10	
	Applicant Arguments/Remarks Made in an Amendment		11	11	
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	29907-0037001_IDS.pdf	31680 2e472f28a92cd2e0fb897aa6229a25d0efaff1a2	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Foreign Reference	JP2001222220.pdf	367776 d044e305399bbf04ade2a36b78d101eb15cb090d	no	5
Warnings:					
Information:					
5	Foreign Reference	WO2001035573.pdf	1942349 443b88775b65acfb18241e5bd2baab51996b28cc	no	40
Warnings:					
Information:					
6	Non Patent Literature	29907-0037JP1OAMay2012.pdf	391127 9a94bfc558f8b87c3ea690ce89e53b270376e5c3	no	7
Warnings:					
Information:					
7	Non Patent Literature	29907-0037JP1OAJan2012.pdf	392201 120d16b09dfbf42d09fc1101c88308efbe82879f	no	8

Warnings:					
Information:					
8	Non Patent Literature	29907-0037CA1OAAug2012.pdf	438378 effd54231fe84afaa3afcb0f3e8fac375f2243b2	no	4
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	32374 1457a93bb4434c2688ba77979b8cbb4babeef18c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3834133		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/336,814	01/23/2006	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
FOR	NUMBER FILED	NUMBER EXTRA					
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **09/18/2012**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 64	Minus	** 57	= 7	X $ =		OR	X $60=	420
Independent (37 CFR 1.16(h))	* 5	Minus	***4	= 1	X $ =		OR	X $250=	250
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**670**

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DEBORAH NASH/

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 09/19/2012

DNASH1 SALE #00000001 Mailroom Dt: 09/18/2012 061050 11336814
01 FC : 1202 420.00 DA

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

94149 7590 11/08/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER
LAKHIA, VIRAL S

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 11/08/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	29907-0037001	1834

TITLE OF INVENTION: ELLIPTIC CURVE RANDOM NUMBER GENERATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	02/08/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

94149 7590 11/08/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	29907-0037001	1834

TITLE OF INVENTION: ELLIPTIC CURVE RANDOM NUMBER GENERATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	02/08/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAKHIA, VIRAL S	2431	380-044000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel R. L. Brown	29907-0037001	1834

94149 7590 11/08/2012

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

EXAMINER	
LAKHIA, VIRAL S	

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 11/08/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 702 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 702 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Viral Lakhia*. (3)_____.

(2) *Michael Henry*. (4)_____.

Date of Interview: *27 September 2012*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *127*.

Identification of prior art discussed: *NA*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner and applicant's representative discussed the background of the invention and summary of independent claim 127 (new). Applicant's representative described how the new claims are same in functionality to previously allowed claim(s), only the pre-amble are different for example previously were method and system claim(s), while the new claim(s) are non-transitory computer readable medium claim(s). Examiner will further conduct focused search and submitted the written response .

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Viral S Lakhia/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

Notice of Allowability	Application No.	Applicant(s)	
	11/336,814	BROWN ET AL.	
	Examiner	Art Unit	
	VIRAL LAKHIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *9/18/2012*.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *68-71, 73-105, 107-109, 111, 112-134*.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Viral S Lakhia/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

DETAILED ACTION

Claim(s) 68-71, 73-105, 107-109, 111, 112-134 are allowed.

REASONS FOR ALLOWANCE

The following is an examiner's statement of reasons for allowance:

Examiner finds applicant's representative's argument dated 9/18/2012 persuasive for reason of allowance. The applicant's claim amendment(s) are persuasive in indication of allowable subject matter: The conducted search on new claim(s) does not teach nor suggest applicant's claim limitation element of: "Using Elliptical Cryptography to generate updated secret value based on scalar multiple of first elliptical curve point ", as described in amended independent claim(s) on 9/18/2012. Further newly added claim(s) perform the same functionality of method steps and system steps as allowed before on 6/22/2012, the new set of claim(s) are directed towards non - transitory computer - readable medium.

Updated search does not teach or fairly suggest the claimed limitations.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viral Lakhia whose telephone number is (571) 270 - 3363. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Viral S Lakhia/

Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/336,814	Applicant(s)/Patent Under Reexamination BROWN ET AL.	
	Examiner VIRAL LAKHIA	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,308,096	12-2007	Okeya et al.	380/28
*	B	US-7,197,527	03-2007	Naslund et al.	708/492
*	C	US-6,307,935	10-2001	Crandall et al.	380/28
*	D	US-6,263,081	07-2001	Miyaji et al.	380/28
*	E	US-7,225,341	05-2007	Yoshino et al.	713/193
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Satoh A, Scalable dual-field elliptical curve cryptographic processor, April 2003, IEEE, Volume 52, Pages 452 - 456.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	11336814
Filing Date	2006-01-23
First Named Inventor	Daniel R.L. Brown
Art Unit	2431
Examiner Name	Viral S. Lakhia
Attorney Docket Number	29907-0037001

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2001222220	JP		2001-08-17	Koden Electronics Co. Ltd.		☒
	2	200135573	WO		2001-05-17	Schroeppel		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

Receipt date: 09/18/2012	Application Number	11336814 11336814 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-01-23
	First Named Inventor	Daniel R.L. Brown
	Art Unit	2431
	Examiner Name	Viral S. Lakhia
	Attorney Docket Number	29907-0037001

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Notice of Final Rejection issued in Japanese Application No. 2007-551522 on May 30, 2012; 7 pages (with translation).	☐
	2	Office Action issued in Japanese Application No. 2007-551522 on January 18, 2012; 8 pages (with translation).	☐
	3	Official Action issued in Canadian Application No. 2,594,670 on August 9, 2012; 4 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Viral Lakhia/	Date Considered	09/25/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.L./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L19	0	(daniel brown scott vanstone).in. and L18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2012/09/27 15:46
L18	3	(first hash input value elliptic curve point secret register scalar multiple second random number level of security cryptographic operation)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	OFF	2012/09/27 15:46
L17	63	(daniel brown scott vanstone).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2012/09/27 15:45
L13	10	(point$2) with (random$4 pseudorandom$3) same (ECC (elliptic$3 with curve)) same (hash$5 encrypt$4) same (first and second) and (scalar$2 multiple$2 constant$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 14:47
L12	8	(point$2) with (random$4 pseudorandom$3) same (ECC (elliptic$3 with curve)) same (hash$5 encrypt$4) same (first and second) and (scalar$2 multiple$2 constant$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121" and "380".clas.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 14:47
L11	5	(point$2) with (random$4 pseudorandom$3) same (ECC (elliptic$3 with curve)) same (hash$5 encrypt$4) same (first and second) and (scalar$2 constant$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121" and "380".clas.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 14:44
L10	23	(point$2) with (random$4 pseudorandom$3) same (ECC (elliptic$3 with curve)) same (hash$5 encrypt$4) and (first and second) and (scalar$2 constant$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121" and "380".clas.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 14:29
L9	2	"11336814"	US-PGPUB;	OR	ON	2012/09/27

			USPAT; EPO; DERWENT; IBM_TDB			14:29
L8	34	(point$2) with (random$4 pseudorandom$3) same (ECC (elliptic$3 with curve)) and (first and second) and (scalar$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121" and "380".clas.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 14:26
L7	57	(point$2) with (random$4 pseudorandom$3) same (ECC (elliptic$3 with curve)) and (first and second) and (scalar$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 14:25
L6	9	(point$2) with (random) same (ECC (elliptical with curve)) and (first and second) and (scalar$2) and (escrow secret seed) and @ad<"20050121" and "380".clas.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 13:32
L5	0	(point$2) with (random) same (ECC (elliptical with curve)) same (first and second) and (scalar$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 13:31
L4	23	(point$2) with (random) same (ECC (elliptical with curve)) and (first and second) and (scalar$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 13:31
L3	24	(point$2) with (random) same (ECC (elliptical with curve)) and (scalar$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 13:31
L2	18	(point$2) with (random with generat$4) same (ECC (elliptical with curve)) and (scalar$2) and (escrow secret seed) and (cryptograp$3) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 13:30
L1	19	(point$2) with (random with generat$4) same (ECC (elliptical with curve)) and (scalar$2) and (escrow secret seed) and @ad<"20050121"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 13:30

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L15	11	(point$2) with (random$4 pseudorandom$3) same (ECC (elliptic$3 with curve)) same (hash$5 encrypt$4) same (first and second) and (scalar$2 multiple$2 constant$2) and (escrow secret seed) and (cryptograp$3)	USPAT; UPAD	OR	ON	2012/09/27 15:43
L14	0	"11336814"	USPAT; UPAD	OR	ON	2012/09/27 15:43

9/27/2012 3:47:42 PM
C:\Users\vlakhia\Documents\EAST\Workspaces\11336814.i..wsp

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
11336814	BROWN ET AL.
Examiner	**Art Unit**
VIRAL LAKHIA	2431

ORIGINAL		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
380	44	H 0 4 L 9 / 00 (2006.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
380	286	28	45	46	
713	157				

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	68	20	85	36	101	49	119								
2	69	21	86	39	102	50	120								
3	70	22	87	40	103	51	121								
4	71	23	88	14	104	52	122								
5	73	24	89	15	105	53	123								
6	74	25	90	19	107	54	124								
7	75	26	91	37	108	55	125								
8	76	27	92	38	109	56	126								
9	77	28	93	41	111	57	127								
10	78	29	94	42	112	58	128								
11	79	30	95	43	113	59	129								
12	80	31	96	44	114	60	130								
13	81	32	97	45	115	61	131								
14	82	33	98	46	116	62	132								
17	83	34	99	47	117	63	133								
18	84	35	100	48	118	64	134								

/VIRAL LAKHIA/ Examiner.Art Unit 2431	10/12/2012	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	64	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431	07/02/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	68	2

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	Art Unit
	VIRAL LAKHIA	4144

SEARCHED

Class	Subclass	Date	Examiner
380	28-30	6/17/09	V.L.
380	44-47	6/17/09	V.L.
380	277-286	6/17/09	V.L.
713	Search 713 with key word search of elliptic curve number generator	6/17/09	V.L.
726	Search 726 with key word search of elliptic curve number generator	6/17/09	V.L.
380	28-30	4.5.2011	V.L.
380	28- 30/283-286	6/27/2012	v.l.
713	171	6/27/2012	v.l.
380	20-30, 44	9/27/2012	v.l.
713	170-171	9/27/2012	v.l.

SEARCH NOTES

Search Notes	Date	Examiner
Key words and combination : elliptic curve number generator (creator, producer, intiator), message, digest, hash, random	7/17/09	V.L.
Get assistance with Fast and Focused Search department for the case	7/17/09	V.L
Get assistance from Peter Poltriak for claim interpretation and understanding of invention	7/17/09	V.L
Search Google Patents, NPL and wikipedia for elliptic curve technology	7/17/09	V.L
Update East with key word search	7/15/2010	V.L.
Update East with key word search.	4.6.2011	V.L.
Search INventor name for double patent issues.	4.6.2011	V.L.
Update East with key word search.	3/3/2012	v.l.
Search Google Patents, NPL and wikipedia for elliptic curve technology	3/3/2012	v.l.
Conduct plus search for independent claims	3/3/2012	v.l.
Examiner reached out to N.Flynn - T.Swann for 101 issue clarification, 101 rejection based on Todd Swan's comments.	3/5/2012	v.l.
Update East with key word search.	6/26/2012	v.l.
Search Inventor name for double patent isssue.	6/26/2012	v.l.
Update East with key word search.	9/27/2012	v.l.
Search Inventor name for double patent isssue.	9/27/2012	v.l.
Udpated claim sheet(s)	10/12/2012	v.l.

/V. S. L./ Examiner.Art Unit 2431	

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**
380	277-286	3/3/2012	v.l.
380	28-30	3/3/2012	v.l.
380	28-30	6/27/2012	v.l.
380	28-30	9/27/2012	v.l.

/V. S. L./ Examiner.Art Unit 2431	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012	08/14/2012	09/27/2012	
	1	✓		÷		✓	-	-	-	
	2	✓		÷		✓	-	-	-	
	3	✓		÷		✓	-	-	-	
	4	✓		÷	✓	✓	-	-	-	
	5	✓		÷	✓	✓	-	-	-	
	6	✓		÷	✓	✓	-	-	-	
	7	✓		÷	✓	✓	-	-	-	
	8	✓		÷	✓	-	-	-	-	
	9	✓		÷	✓	✓	-	-	-	
	10	✓		÷	✓	✓	-	-	-	
	11	✓		÷	✓	✓	-	-	-	
	12	✓		÷	✓	-	-	-	-	
	13	✓		÷	✓	✓	-	-	-	
	14	✓		÷	✓	✓	-	-	-	
	15	✓		÷	✓	✓	-	-	-	
	16	✓		÷	✓	✓	-	-	-	
	17	✓		÷	✓	✓	-	-	-	
	18	✓		÷	✓	✓	-	-	-	
	19		✓	÷	-	-	-	-	-	
	20			÷	✓	✓	-	-	-	
	21			÷	✓	✓	-	-	-	
	22			÷	✓	✓	-	-	-	
	23			÷	✓	✓	-	-	-	
	24			÷	✓	✓	-	-	-	
	25			÷	✓	✓	-	-	-	
	26			÷	✓	✓	-	-	-	
	27			÷	✓	✓	-	-	-	
	28			÷	✓	✓	-	-	-	
	29			÷	✓	✓	-	-	-	
	30			÷	-	-	-	-	-	
	31			÷	-	-	-	-	-	
	32			÷	-	-	-	-	-	
	33			÷	-	-	-	-	-	
	34			÷	-	-	-	-	-	
	35			÷	-	-	-	-	-	
	36			÷	-	-	-	-	-	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012	08/14/2012	09/27/2012	
	37					✓	-	-	-	
	38					✓	-	-	-	
	39					✓	-	-	-	
	40					✓	-	-	-	
	41					✓	-	-	-	
	42					✓	-	-	-	
	43					✓	-	-	-	
	44					✓	-	-	-	
	45					✓	-	-	-	
	46					✓	-	-	-	
	47					✓	-	-	-	
	48					✓	-	-	-	
	49					✓	-	-	-	
	50					✓	-	-	-	
	51					✓	-	-	-	
	52					✓	-	-	-	
	53					✓	-	-	-	
	54					✓	-	-	-	
	55					✓	-	-	-	
	56					✓	-	-	-	
	57					✓	-	-	-	
	58					✓	-	-	-	
	59					✓	-	-	-	
	60					✓	-	-	-	
	61					✓	-	-	-	
	62					✓	-	-	-	
	63					✓	-	-	-	
	64					✓	-	-	-	
	65					✓	-	-	-	
	66					✓	-	-	-	
	67					✓	-	-	-	
	68						=	=	=	
	69						=	=	=	
	70						=	=	=	
	71						=	=	=	
	72						=	-	-	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012	08/14/2012	09/27/2012	
	73						=	=	=	
	74						=	=	=	
	75						=	=	=	
	76						=	=	=	
	77						=	=	=	
	78						=	=	=	
	79						=	=	=	
	80						=	=	=	
	81						=	=	=	
	82						=	=	=	
	83						✓	=	=	
	84						✓	=	=	
	85						=	=	=	
	86						=	=	=	
	87						=	=	=	
	88						=	=	=	
	89						=	=	=	
	90						=	=	=	
	91						=	=	=	
	92						=	=	=	
	93						=	=	=	
	94						=	=	=	
	95						=	=	=	
	96						=	=	=	
	97						=	=	=	
	98						=	=	=	
	99						=	=	=	
	100						=	=	=	
	101						=	=	=	
	102						=	=	=	
	103						=	=	=	
	104						=	=	=	
	105						=	=	=	
	106						=	-	-	
	107						=	=	=	
	108						=	=	=	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	**Art Unit**
	VIRAL LAKHIA	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/17/2009	06/18/2009	03/08/2010	07/15/2010	04/07/2011	03/05/2012	08/14/2012	09/27/2012	
	109						=	=	=	
	110						=	=	-	
	111						=	=	=	
	112								=	
	113								=	
	114								=	
	115								=	
	116								=	
	117								=	
	118								=	
	119								=	
	120								=	
	121								=	
	122								=	
	123								=	
	124								=	
	125								=	
	126								=	
	127								=	
	128								=	
	129								=	
	130								=	
	131								=	
	132								=	
	133								=	
	134								=	

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

94149 7590 11/08/2012

Fish & Richardson P.C.
P.O. Box 1022
Minneapolis MN 55440-1022
United States

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	01/23/2006	Daniel Richard L. Brown	29907-0037001	1834

TITLE OF INVENTION: ELLIPTIC CURVE RANDOM NUMBER GENERATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300		$2070	02/08/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAKHIA, VIRAL S.	2431	380-044000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
[ ] Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
[ ] "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Fish & Richardson P.C.
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE
Certicom Corp.

(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Mississauga, Ontario, Canada

Please check the appropriate assignee category or categories (will not be printed on the patent) : [ ] Individual [X] Corporation or other private group entity [ ] Government

4a. The following fee(s) are submitted:
[X] Issue Fee
[X] Publication Fee (No small entity discount permitted)
[ ] Advance Order - # of Copies _____

4b. Payment of Fee(s):
[ ] A check in the amount of the fee(s) is enclosed.
[ ] Payment by credit card. Form PTO-2038 is attached.
[X] The Director is hereby authorized to charge the required fee(s), or credit any overpayment, to Deposit Account Number 06-1050

5. **Change in Entity Status** (from status indicated above)
[ ] a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. [ ] b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

The Director of the USPTO is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.
NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Michael K. Henry/ Date February 6, 2013

Typed or printed name Michael K. Henry, Ph.D. Registration No. 59,516

90660045

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit :	2431
Serial No.	: 11/336,814	Examiner :	Viral S. Lakhia
Filed	: January 23, 2006	Confirmation No.:	1834
		Notice of Allowance Date:	November 8, 2012
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

MAIL STOP ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

COMMENTS ON EXAMINER'S REASONS FOR ALLOWANCE

Applicant recognizes that in accordance with M.P.E.P. § 1302.14, the Examiner's reasons for allowance need not set forth all of the details as to why the claims are allowed.

Applicant does not concede that the Examiner's stated reasons for allowance are the only reasons for which the claims are allowable. The claims may be allowable for other reasons as well. In particular, Applicant does not concede that all of the limitations identified by the Examiner are necessary to distinguish the prior art of record or to satisfy the requirements of 35 U.S.C. § 112. In addition, the Examiner does not assert, and Applicant would not concede, that the Examiner's reasons have any bearing on the patentability of claims in any other applications directed to the disclosed subject matter.

In addition, each dependent claim stands on its own and is allowable on its own merits. In particular, each dependent claim may be allowable on the basis of a combination of some of the features recited in the dependent claim and its base claim(s), which combination of features may not include all of the limitations identified in the Examiner's reasons for allowance.

Please apply any charges or credits related to this paper to our Deposit Account No. 06-1050.

Respectfully submitted,

Date: February 6, 2013

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

90660037

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	Michael K. Henry/Christie Loven
Attorney Docket Number:	29907-0037001

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1770	1770
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2070**

Electronic Acknowledgement Receipt

EFS ID:	14888619
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Joe Farrell
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	29907-0037001
Receipt Date:	06-FEB-2013
Filing Date:	23-JAN-2006
Time Stamp:	13:08:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2070
RAM confirmation Number	10337
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Post Allowance Communication - Incoming	29907-0037001_Response.pdf	67001 2bb6e7301e27afe092c677dd518ba70912b6e8d3	no	1
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	29907-0037001_IssueFee.pdf	106863 4482b439dc0df905f463e89a2732c5488f51ddb3	no	1
Warnings:					
Information:					
3	Post Allowance Communication - Incoming	29907-0037001_Comments.pdf	65081 5cad4c34caa5c43e456dd6e6d782e7c022959850	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32153 7561b0e9df5f94fb443f78402ccd143508e1b85b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	271098		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit :	2431
Serial No.	: 11/336,814	Examiner :	Viral S. Lakhia
Filed	: January 23, 2006	Confirmation No.:	1834
		Notice of Allowance Date:	November 8, 2012
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

MAIL STOP ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTICE OF ALLOWANCE

In response to the Notice of Allowance mailed November 8, 2012, enclosed is a completed Part B - Fee(S) Transmittal.

Examiner Interview Summary. An Examiner-initiated interview was conducted on 27 September 2012. Examiner Viral Lakhia and the Assignee's representative Michael K. Henry participated. During the interview, the Assignee's representative confirmed that new claims had been added to the application, and the Examiner stated that all claims presented in the amendment filed September 18, 2012 would be examined. No formal agreement was reached during the interview.

The issue fee and publication fees in the amount of $2070 are being paid concurrently herewith. In addition, please apply any other necessary charges or credits to Deposit Account 06-1050, referencing the above attorney docket number.

Respectfully submitted,

Date: February 6, 2013

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11336814	BROWN ET AL.
	Examiner	Art Unit
	VIRAL LAKHIA	2431

ORIGINAL	
CLASS	SUBCLASS
380	44

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
380	286	28	45	46	
713	157				

INTERNATIONAL CLASSIFICATION					
CLAIMED					NON-CLAIMED
H	0	4	L	9 / 00 (2006.01.01)	

Change(s) applied to document,
/L.A.S./
9/5/2012

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	68	20	85	36	101										
2	69	21	86	39	102										
3	70	22	87	40	103										
4	71	23	88	14	104										
5	73	24	89	15	105										
6	74	25	90	19	107										
7	75	26	91	37	108										
8	76	27	92	38	109										
9	77	28	93	41	110										
10	78	29	94	42	111										
11	79	30	95												
12	80	31	96												
13	81	32	97												
16	82	33	98												
17	83	34	99												
18	84	35	100												

/VIRAL LAKHIA/ Examiner.Art Unit 2431 (Assistant Examiner)	06/26/2012 (Date)	**Total Claims Allowed:** 42
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431 (Primary Examiner)	07/02/2012 (Date)	O.G. Print Claim(s) 68 / O.G. Print Figure 2

IIFW

8.29.12

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/336,814	03/12/2013	8396213	29907-0037001	1834

94149 7590 02/20/2013

Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 1283 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Daniel R. L. Brown, Mississauga, CANADA;
Scott A. Vanstone, Campbellville, CANADA;

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit	: 2431
Patent No.	: 8,396,213	Examiner	: Viral S. Lakhia
Issue Date	: March 12, 2013	Conf. No.	: 1834
Serial No.	: 11/336,814		
Filed	: January 23, 2006		

Title : ELLIPTIC CURVE RANDOM NUMBER GENERATION

Attention Certificate of Corrections Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF REQUEST FOR CERTIFICATE OF CORRECTION

Applicant hereby requests that a certificate of correction be issued for the above patent in accordance with the attached request.

One or more of the errors sought to be corrected were made by applicant. The fees in the amount of $100 are being paid concurrently herewith.

Please apply any other necessary charges or credits to Deposit Account 06- 1050, referencing the above attorney docket number.

Respectfully submitted,

Date: May 1, 2013

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

90684992

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 8,396,213

APPLICATION NO.: 11/336,814

ISSUE DATE: : March 12, 2013

INVENTOR(S) : Scott Alexander Vanstone

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

First Page, Column 2 (Other Publications), Line 1: Delete "correctnes" and insert -- correctness --, therefor.

Column 10, Line 43, Claim 47: Delete "ellptic" and insert -- elliptic --, therefor.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Fish & Richardson, P.C.
P.O. Box 1022
Minneapolis, MN 55440

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	Michael K. Henry/Christie Loven
Attorney Docket Number:	29907-0037001

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Certificate of Correction	1811	1	100	100
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**100**

Electronic Acknowledgement Receipt

EFS ID:	15666727
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Christie Loven
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	29907-0037001
Receipt Date:	01-MAY-2013
Filing Date:	23-JAN-2006
Time Stamp:	16:43:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$100
RAM confirmation Number	3649
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Request for Certificate of Correction	29907-0037001_RequestCertificateCorrection.pdf	125891 8b669ec45e2ec708590349c1f952f7010f9c18e3	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30096 ea1c28c518e1c2051544070e61f36ebd7f2692a1	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	155987	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Daniel R. L. Brown et al.	Art Unit	: 2431
Patent No.	: 8,396,213	Examiner	: Viral S. Lakhia
Issue Date	: March 12, 2013	Conf. No.	: 1834
Serial No.	: 11/336,814		
Filed	: January 23, 2006		
Title	: ELLIPTIC CURVE RANDOM NUMBER GENERATION		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPLICATION FOR PATENT TERM ADJUSTMENT UNDER 37 C.F.R. § 1.705(d)

Patentees hereby request reconsideration of the Patent Term Adjustment (PTA) accorded the above-referenced patent. Reconsideration of the final PTA calculation to increase total PTA from 1,283 days to 1,934 days is respectfully requested. In the alternative, Patentees request that total PTA be increased from 1,283 days to 1,408 days.

"A Delays" are defined as delays by the U.S. Patent and Trademark Office (PTO) under 35 U.S.C. § 154(b)(1)(A), which guarantees prompt PTO response. "B Delays" are defined as delays by the PTO under 35 U.S.C. § 154(b)(1)(B), which guarantees no more than three year application pendency. Patentees respectfully submit that the Office did not apply the proper standard for determining the period of "B Delay" under 35 U.S.C. § 154(b)(1)(B).

REVIEW OF PATENT TERM ADJUSTMENT CALCULATION

Applicant Delay

A reply to an Office Action was due on or before September 23, 2009 (the date that is three months after June 23, 2009, the date on which the Office Action was mailed). Patentees filed a response to the Office Action on October 23, 2009, thereby according an Applicant Delay of 30 days. Patentees do not dispute the PTO's calculation for this Applicant Delay from September 24, 2009 (the day after the date that is three months after the date on which the Office Action was mailed), to October 23, 2009. See 37 C.F.R. § 1.704(b).

Patentees filed an Information Disclosure Statement on December 10, 2009, subsequent to a reply filed on October 23, 2009. Patentees were accorded a delay of 48 days for a

supplemental response. Patentees do not dispute the PTO's calculation for this Applicant Delay from October 24, 2009, to December 10, 2009. See 37 C.F.R. § 1.704(c)(8).

A reply to an Office Action was due on or before November 23, 2010 (the date that is three months after August 23, 2010, the date on which the Office Action was mailed). Patentees filed a response to the Office Action on February 23, 2011, thereby according an Applicant Delay of 92 days. Patentees do not dispute the PTO's calculation for this Applicant Delay from November 24, 2010 (the day after the date that is three months after the date on which the Office Action was mailed), to February 23, 2011. See 37 C.F.R. § 1.704(b).

Patentees filed a Supplemental Reply on February 24, 2011, subsequent to a reply filed on February 23, 2011. Patentees were accorded a delay of 1 day for a supplemental response. Patentees do not dispute the PTO's calculation for this Applicant Delay from February 24, 2011, to February 24, 2011. See 37 C.F.R. § 1.704(c)(8).

A reply to an Office Action was due on or before July 15, 2011 (the date that is three months after April 15, 2011, the date on which the Office Action was mailed). Patentees filed a response to the Office Action on August 15, 2011, thereby according an Applicant Delay of 31 days. Patentees do not dispute the PTO's calculation for this Applicant Delay from July 16, 2011 (the day after the date that is three months after the date on which the Office Action was mailed), to August 15, 2011. See 37 C.F.R. § 1.704(b).

Patentees filed an Information Disclosure Statement on September 29, 2011, subsequent to a reply filed on August 15, 2011. Patentees were accorded a delay of 45 days for a supplemental response. Patentees do not dispute the PTO's calculation for this Applicant Delay from August 16, 2011, to September 29, 2011. See 37 C.F.R. § 1.704(c)(8).

In view of the periods of Applicant Delay detailed above, the total Applicant Delay for this patent should be calculated as 247 days (i.e., the sum of 30 days, 48 days, 92 days, 1 day, 31 days, and 45 days).

"A Delay"

A first PTO action was due on or before March 23, 2007 (the date that is fourteen months after January 23, 2006, the date on which the application was filed). The PTO mailed the first

non-final Office Action on June 23, 2009, thereby according a PTO Delay of 823 days. Patentees do not dispute the PTO's calculation for this "A Delay" from March 24, 2007 (the day after the date that is fourteen months after the date on which the application was filed), to June 23, 2009. See 37 C.F.R. §§ 1.702(a)(1) and 1.703(a)(1).

A PTO action was due on or before February 23, 2010 (the date that is four months after October 23, 2009, the date on which a response to Office Action was filed). The PTO mailed a non-final Office Action on March 22, 2010, thereby according a PTO Delay of 27 days. Patentees do not dispute the PTO's calculation for this "A Delay" from February 24, 2010 (the day after the date that is four months after the date on which a response to Office Action was filed), to March 22, 2010. See 37 C.F.R. §§ 1.702(a)(2) and 1.703(a)(2).

A PTO action was due on or before August 22, 2010 (the date that is four months after April 22, 2010, the date on which a response to Office Action was filed). The PTO mailed a final Office Action on August 23, 2010, thereby according a PTO Delay of 1 day. Patentees do not dispute the PTO's calculation for this "A Delay" from August 23, 2010 (the day after the date that is four months after the date on which a response to Office Action was filed), to August 23, 2010. See 37 C.F.R. §§ 1.702(a)(2) and 1.703(a)(2).

A PTO action was due on or before December 15, 2011 (the date that is four months after August 15, 2011, the date on which a response to Office Action was filed). The PTO mailed a final Office Action on March 22, 2012, thereby according a PTO Delay of 98 days. Patentees do not dispute the PTO's calculation for this "A Delay" from December 16, 2011 (the day after the date that is four months after the date on which a response to Office Action was filed), to March 22, 2012. See 37 C.F.R. §§ 1.702(a)(2) and 1.703(a)(2).

In view of the periods of "A Delay" detailed above, the total "A Delay" for this patent should be calculated as 949 days (i.e., the sum of 823 days, 27 days, 1 day, and 98 days).

"B Delay"

There is no dispute that the Office failed to issue a patent within three years of the filing date of the application and that Patentees are entitled to "B Delay" to compensate for that Office delay. The only issue in contention is the correct length of the "B Delay" period.

"B Delays" are defined as delays by the PTO under 35 U.S.C. § 154(b)(1)(B), which guarantees no more than three year application pendency. The period beginning on January 24, 2009 (the day after the date that is three years after the date on which the application was filed), and ending March 12, 2013 (the date the patent was issued), is 1,509 days in length. The "PTA 36 Months" entry in the PAIR/PALM system indicates that a total of 760 days were awarded for "B Delay" for this patent. The PTO excluded from "B Delay" the number of days corresponding to the period beginning on February 23, 2011 (the date on which a request for continued examination was first filed) and ending on March 12, 2013 (the date the patent was issued). Patentees respectfully submit that the PTO's calculation of this "B Delay" is incorrect.

Patentees respectfully contest the "B Delay" calculation on the following two alternative bases.

(i) Primary Argument: PTO erred by reducing PTA based on a request for continued examination filed after the 3-year "guaranteed" deadline

According to the decisions in Exelixis, Inc. v. Kappos, No. 1:12-cv-96 (E.D. Va. November 1, 2012) and Novartis v. Kappos, No. 1:10-cv-01138 (D.D.C. November 15, 2012), a Request for Continued Examination operates to toll the three year "guaranteed" deadline of 35 U.S.C. § 154(b)(1)(B) only if it is filed within three years of the application filing date. If filed after the three year deadline has passed, a Request for Continued Examination has no impact on PTA.

For the present patent, no Request for Continued Examination was filed during the first three years of application pendency. The Requests for Continued Examination filed on February 23, 2011, and September 18, 2012, therefore do not operate to reduce the "B Delay" award. As a result, the patent is entitled to 1,509 days of "B Delay", measured from January 24, 2009 (the day after the date that is three years after the date on which the application was filed) to March 12, 2013 (the date the patent was issued).

(ii) Secondary Argument: PTO erred by counting the time between the notice of allowance and the patent issue date as "time consumed by continued examination of the application"

This subsection presents an alternative calculation of "B Delay" in the event that the argument in subsection (i) above is deemed unpersuasive.

The Examiner's mailing of a Notice of Allowance on November 8, 2012, closed examination of the application on that date. Section 154(b)(1)(B)(i) of Title 35 excludes from "B Delay" "time consumed by continued examination of the application." The statute does not provide for exclusion from "B Delay" of time from the mailing of a Notice of Allowance until issuance (a period during which continued examination did not occur). Thus, no continued examination took place during the 125 day period from November 8, 2012 (the mailing date of the Notice of Allowance) until March 12, 2013 (the date the patent was issued). Accordingly, 125 days of "B Delay" should have been included in addition to the 760 days accorded by the Director, for a total "B Delay" of 885 days.

Overlap of "A Delay" and "B Delay"

To the extent that the periods of delay overlap, the period of any term adjustment shall not exceed the actual number of days the issuance of the patent was delayed.
35 U.S.C. § 154(b)(2)(A). In view of the remarks above, the period of overlap of "A Delay" and "B Delay" should be calculated as follows. The primary argument below is based on the "B Delay" presented in subsection (i) above. The secondary argument below is based on the "B Delay" presented in subsection (ii) above.

(i) Primary Argument: PTO erred by reducing PTA based on a request for continued examination filed after the 3-year "guaranteed" deadline

As detailed above, 949 days of "A Delay" accumulated during the following periods:

March 24, 2007, to June 23, 2009;

February 24, 2010, to March 22, 2010;

August 23, 2010, to August 23, 2010; and

December 16, 2011, to March 22, 2012.

As detailed above, 1,509 days of "B Delay" accumulated during the following period:

January 24, 2009, to March 12, 2013.

As such, the periods of "A Delay" and "B Delay" overlap (i.e., occur on the same calendar day) for a total of 277 days, from January 24, 2009, to June 23, 2009, February 24, 2010, to March 22, 2010, August 23, 2010, to August 23, 2010, and December 16, 2011, to March 22, 2012.

(ii) Secondary Argument: PTO erred by counting the time between the notice of allowance and the patent issue date as "time consumed by continued examination of the application"

As detailed above, 949 days of "A Delay" accumulated during the following periods:

March 24, 2007, to June 23, 2009;

February 24, 2010, to March 22, 2010;

August 23, 2010, to August 23, 2010; and

December 16, 2011, to March 22, 2012.

As detailed above, 885 days of "B Delay" accumulated during the following periods:

January 24, 2009, to February 23, 2011; and

November 8, 2012, to March 12, 2013.

As such, the periods of "A Delay" and "B Delay" overlap (i.e., occur on the same calendar day) for a total of 179 days, from January 24, 2009, to June 23, 2009, February 24, 2010, to March 22, 2010, and August 23, 2010, to August 23, 2010.

Terminal Disclaimer

This patent is not subject to a terminal disclaimer.

Conclusion

In consideration of the events described above, Patentees believe the PTA calculation of 1,283 days is incorrect. As such, Patentees respectfully request reconsideration of the PTA in the following alternative manners. The primary argument below is based on the "B Delay" presented in subsection (i) above. The secondary argument below is based on the "B Delay" presented in subsection (ii) above.

(i) Primary Argument: PTO erred by reducing PTA based on a request for continued examination filed after the 3-year "guaranteed" deadline

1) Total PTO Delay should be calculated as 2,181 days (i.e., the sum of 949 days of "A Delay" and 1,509 days of "B Delay" minus 277 days of overlap);

2) Total Applicant Delay should be calculated as 247 days; and

3) Total PTA should be calculated as 1,934 days.

(ii) Secondary Argument: PTO erred by counting the time between the notice of allowance and the patent issue date as "time consumed by continued examination of the application"

1) Total PTO Delay should be calculated as 1,655 days (i.e., the sum of 949 days of "A Delay" and 885 days of "B Delay" minus 179 days of overlap);

2) Total Applicant Delay should be calculated as 247 days; and

3) Total PTA should be calculated as 1,408 days.

The fee of $200 required under 37 C.F.R. § 1.18(e) is being submitted herewith. Please apply any other required charges or credits to Deposit Account No. 06-1050, referencing attorney docket number 29907-0037001.

Respectfully submitted,

Date: May 7, 2013

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Fish & Richardson P.C.
Customer Number 94149
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

Electronic Patent Application Fee Transmittal

Application Number:	11336814
Filing Date:	23-Jan-2006
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Filer:	Michael K. Henry/Christie Loven
Attorney Docket Number:	29907-0037001

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Application for patent term adjustment	1455	1	200	200
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**200**

Electronic Acknowledgement Receipt

EFS ID:	15713951
Application Number:	11336814
International Application Number:	
Confirmation Number:	1834
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel R. L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Christie Loven
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	29907-0037001
Receipt Date:	07-MAY-2013
Filing Date:	23-JAN-2006
Time Stamp:	15:56:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$200
RAM confirmation Number	2582
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Patent Term Adjustment Petition	29907-0037001_PTAPetition.pdf	103626 e757610ba8075c8415fa05bcd1e2ee0962380473	no	7
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30603 3101fae20fcfcae17afada48d3640bd5a141a4b3	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	134229	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,396,213 B2
APPLICATION NO. : 11/336814
DATED : March 12, 2013
INVENTOR(S) : Scott Alexander Vanstone

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title Page, Column 2 (Other Publications), Line 1: Delete "correctnes" and insert -- correctness --, therefor.

In the Claims:

Column 10, Line 43, Claim 47: Delete "ellptic" and insert -- elliptic --, therefor.

Signed and Sealed this
Fourth Day of June, 2013

Teresa Stanek Rea
Acting Director of the United States Patent and Trademark Office