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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 May 2006 (18.05.2006)

PCT

(10) International Publication Number
WO 2006/050605 A1

(51) International Patent Classification:
H04L 9/30 (2006.01)

(21) International Application Number:
PCT/CA2005/001720

(22) International Filing Date:
14 November 2005 (14.11.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/IB2004/003700
11 November 2004 (11.11.2004) IB
60/626,884 12 November 2004 (12.11.2004) US

(71) Applicant *(for all designated States except US)*: **CERTICOM CORP.** [CA/CA]; 4th Floor, 5520 Explorer Drive, Mississauga, Ontario L4W 5L1 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VANSTONE, Scott A.** [CA/CA]; 10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0 (CA). **GALLANT, Robert P.** [CA/CA]; 4788 Rosebush Road, Mississauga, Ontario L5M 5N1 (CA). **BROWN, Daniel R.L.** [CA/CA]; 6033 Paddle Road, Mississauga, Ontario L5N 1X8 (CA). **STRUIK, Marinus** [NL/CA]; 723 Carlaw, Toronto, Ontario M4K 3K8 (CA).

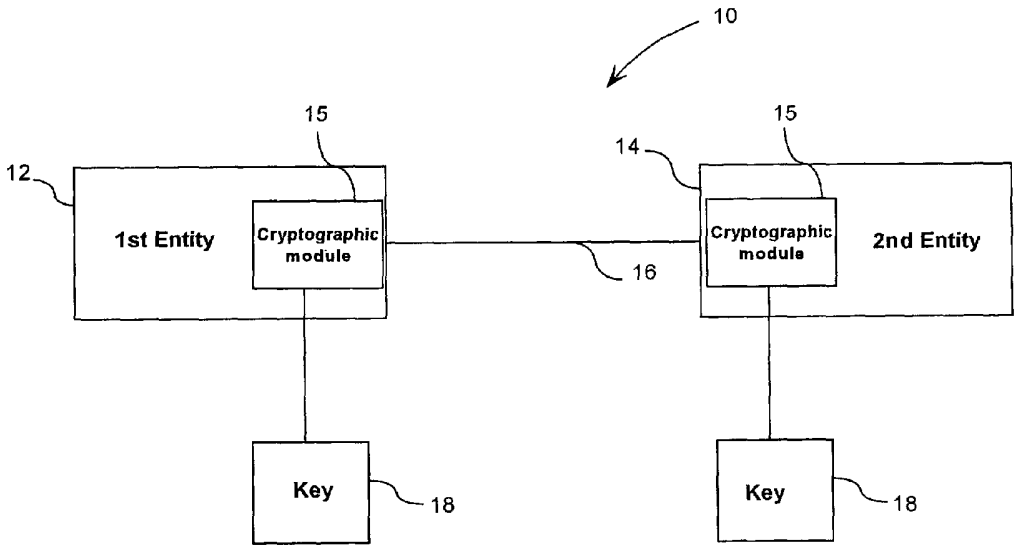
(74) Agents: **ORANGE, John R.S.** et al.; Box 25, Commerce Court West, 199 Bay Street, Suite 2800, Toronto, Ontario M5L 1A9 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: NEW TRAPDOOR ONE-WAY FUNCTION ON ELLIPTIC CURVES AND THEIR APPLICATIONS TO SHORTER SIGNATURES AND ASYMMETRIC ENCRYPTION



(57) Abstract: The present invention provides a new trapdoor one-way function. In a general sense, some quadratic algebraic integer z is used. One then finds a curve E and a rational map defining [z] on E. The rational map [z] is the trapdoor one-way function. A judicious selection of z will ensure that [z] can be efficiently computed, that it is difficult to invert, that determination of [z] from the rational functions defined by [z] is difficult, and knowledge of z allows one to invert [z] on a certain set of elliptic curve points. Every rational map is a composition of a translation and an endomorphism. The most secure part of the rational map is the endomorphism as the translation is easy to invert. If the problem of inverting the endomorphism and thus [z] is as hard as the discrete logarithm problem in E, then the size of the cryptographic group can be smaller than the group used for RSA trapdoor one-way functions.

WO 2006/050605 A1

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

NEW TRAPDOOR ONE-WAY FUNCTION ON ELLIPTIC CURVES AND THEIR APPLICATIONS TO SHORTER SIGNATURES AND ASYMMETRIC ENCRYPTION

FIELD OF THE INVENTION:

[0001] The present invention relates to trapdoor one-way encryption functions and cryptosystems utilising such functions.

DESCRIPTION OF THE PRIOR ART

[0002] A trapdoor one-way function (TOWF) is a publicly computable function, which only one entity can invert. A special secret, called a private key, is required to compute the inverse of TOWF.

[0003] The classic example of a TOWF is the RSA function based on the relationship $M^{ed} \equiv M \pmod N$. The public RSA function w is computed as follows: $W(x) = x^e \bmod N$. The numbers e and N are public values. The number N is chosen to be a product of two secret distinct primes p and q. Inverting the RSA function with the private key operation w, can be done as follows: $W^{-1}(y) = y^d \bmod N$, where $d = (1/e) \bmod (p-1)(q-1)$ and is the private key.

[0004] Inverting the RSA function without the private key is believed to be a hard problem. Factoring N to obtain the primes p, q is computationally infeasible for large values of N and therefore the private key $w = (p-1)(q-1)$ also maintains secrecy. In fact, the security of much of the online banking currently done depends on the RSA function being hard to invert without the private key. In other words, the world generally believes that the RSA function is a TOWF.

[0005] As a TOWF, the RSA function can be used as the basis of a cryptosystem that performs both digital signatures and public-key encryption. To digitally sign a message M with a trapdoor one-way function W one computes $S = W^{-1}(H(M))$ using the private key operation W^{-1} and a public hash function H. The hash function has two purposes: to compress M down to the size of digest which W^{-1} can handle and to prevent some potential attacks involving the conversion of a signature of one message to the signature of a related

but unauthorized message. To verify a signature S of message M with a trapdoor one-way function, one checks that H(M) = W(S).

[0006] Public-key encryption with a TOWF is somewhat the opposite to signing. Instead of hashing, an encoding scheme E is used. To encrypt a message M, one computes a ciphertext C = W(E(M)). To decrypt a ciphertext C, one computes $M = E^{-1}(W^{-1}(C))$. The encoding function serves to adapt M to the size needed for W to be applied, and also to prevent certain kinds of related message attacks.

[0007] An alternative cryptosystem is based on the difficulty of the discrete log problem. A particularly robust cryptosystem, which bases its security on the discrete log problem utilizes elliptic curves and has the advantage of reduced bandwidth compared with RSA TWOF cryptosystems.

[0008] Whilst elliptic curve cryptosystems reduce the bandwidth compared to the RSA TOWF, there is still a need to minimize the bandwidth whilst maintaining the desirable attributes of existing systems. Moreover, TOWF's do not rely on the random number generator and therefore in some circumstances may be easier to implement even though the bandwidth required is greater.

[0009] It is therefore an object of the present invention to provide a TOWF cryptosystem to obviate or mitigate the above mentioned disadvantages.

[0010] To facilitate the understanding of the underlying principles of the present invention, a review of the mathematical basis of these principles is set forth below.

[0011] 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 quadratic in y and a cubic in x, 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, multiplied, and divided (with the exception of zero for division). 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.

[0012] Without the loss of generality, the defining equation of the elliptic curve can be in the Weierstrass form. When the field F is derived from the 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.

[0013] The elliptic curve E includes the points (x, y), which are all solutions to the defining equation, 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 in the field over which E is defined.

[0014] A rational function r(x,y) in two variables over a field is the ratio of two polynomials in two variables each over the same field. So r(x,y) = p(x,y)/q(x,y), where p and q are polynomials in x and y. A polynomial in x and y is a sum of terms of the form $a x^m y^n$, where a is a field element (possibly depending on m and n), and m and n are non-negative integers. For example, $x^2y - 3y^4 + 1$ is a polynomial in x and y. For any rational function r(x, y) and field elements u and v, there is a value of the rational function r(x,y) at the point (u, v). The value is a field element or the point at infinity, and is written r(u, v). The value r(u, v) is obtained simply by substituting each occurrence of the variable x by the field element u and each y by v, and then evaluating all the field operations such as multiplication, addition and division. Occasionally division by zero results, which generally indicates that the value r(u, v) is actually infinity, which is regarded as an exception because the value is not in the field. Thus, it is possible to evaluate r(x,y) for points (x,y) on the curve. It is also possible to define the value of r(x,y) at the point O, this enabling evaluation of r on each point of the curve.

[0015] A rational map on an elliptic curve E is a pair of rational functions r(x,y) and s(x,y) such that if (u, v) is a point on E, then (t, w) = (r(u, v), s(u, v)) is also a point on E.

More generally, this needs to also hold if (u,v) is replaced by O, and furthermore if it is acceptable for (t, w) to be O, which corresponds to t and w both being infinity.

[0016] Rational maps on elliptic curves can actually be added just like points on the curve. The addition rules are similar, except that instead of doing operations with field elements, one instead does operations with rational functions, that is, with the symbolic functions of x and y.

[0017] A rational map (r, s) on E is considered equivalent to another rational map (r', s') on E if r is equivalent to r' and s is equivalent to s', as rational functions on E.

[0018] A special kind of rational map is an endomorphism. An endomorphism e, is a rational map e = (r, s) with the additive property, that is e(P + Q) = e(P) + e(Q) for any two points P and Q. An important theorem in elliptic curve theory says that if e is a rational map with the property e(O) = O, then e is also an endomorphism. This theorem considerably simplifies the determination of whether a given rational map is an endomorphism.

[0019] An important example of an endomorphism is e = [m] which is defined by e(P) = mP, that is, the sum of m copies of the point P. Because the addition law for curve E is defined by rational functions, then so is the iterated sum mP of m copies of P, because these rational functions can be iterated. Therefore e(P) is a rational map. Because the addition operation on the curve E is associative, we have e(P + Q) = m(P+Q) = m(P) + m(Q) = e(P) + e(Q) for e =[m] Therefore, e is an endomorphism because it has the additive property.

[0020] If there is an endomorphism different than [m], then E is said to have complex multiplication. Elliptic curves defined over finite fields always have complex multiplication. In other words, they always have an endomorphism e which is different from [m] for all integers m.

[0021] A powerful theorem of elliptic curve theory says that any endomorphism e is equivalent to a unique rational map of the form (r(x), cyr'(x)), where r(x) is a rational function of a single variable, c is a constant field element, and r'(x) is the derivate of r(x). This result is not at all obvious, but if e is in the form (f(x,y), g(x,y)), it is not too difficult to determine r(x), as outlined below.

[0022] To illustrate, one replaces each occurrence of y^2 in f(x, y) with a polynomial that is linear or constant in y. For example, if the curve's defining equation is $y^2 = x^3 + ax + b$, then each y^2 can be replaced by $x^3 + ax + b$, which is constant in y. Apply this as many times as necessary so that the numerator and denominator do not have any powers of y higher than 1, in other words they are linear in y. The modified f(x,y) has the form (a(x) + b(x) y)/ (c(x) + d(x)y), where a, b, c, and d are polynomial functions, not to be confused with previous uses of these variables. The y can be eliminated from the denominator by multiplying the top and bottom by (c(x) – d(x) y), which gives $c(x)^2 - d(x)^2 y^2 = c(x)^2 - d(x)^2 (x3 + ax + b)$ in the bottom. The y^2 in the numerator can also be eliminated. This gives a form g(x) + h(x) y where g(x) and h(x) are rational functions in x. It can be proven that h(x) = 0, because as e is an endomorphism we have e(-P) = -e(P), so e(x,-y) = -e(x,y), thus g(x) + h(x) y = g(x) – h(x) y, for all (x,y) on the curve. So now we have found r(x) as g(x). It is clear that r(x) found in this way is unique.

[0023] Similarly, the rational function g(x,y) can be expressed as a linear function h(x) + y k(x) where h(x) and k(x) are rational functions of x, and it can be shown that h(x) = 0 by similar reasons. This means that k(x) can be determined, which provides a means to find the constant c in the form (r(x), cyr'(x)). Alternately, c could be found by differentiating r(x), and then evaluating e at a some point P to solve for c.

[0024] Every endomorphism has an action on an elliptic curve group that corresponds to a quadratic algebraic integer. A quadratic algebraic integer z is a complex number such that $z^2 + uz + v = 0$ for some integers u and v. The endomorphism e corresponds to this algebraic integer if $e^2 + [u]z + [v] = [0]$, where the addition here is the addition of rational maps, as explained above. In this case, we can write e = [z], where [ ] indicates the rational map corresponding to a rational integer.

[0025] All real integers are quadratic algebraic integers, and the endomorphism [m] corresponds to the integer m. A quadratic algebraic integer that is not a real integer is the complex number i, the square root of –1, which satisfies quadratic equation $i^2 + 1 = 0$. For each quadratic algebraic integer that is not a real integer, there are only a limited set of elliptic curves that have [z] as an endomorphism. Known results give theoretical procedures for determining such curves, as well as a way of determining [z] as a rational map.

[0026] Generally, the degree of endomorphism e is the number of points P such that e(P) = O. More precisely, this is called the separable degree of e. The actual degree is the product of the separable degree and something else called the inseparable degree. When e is expressed in its canonical form as (r(x),cyr'(x)), the degree of the numerator of r(x) is the degree of e, and the degree of the denominator of r(x) is one less. (Here we assume the numerator and denominator of r(x) to be co-prime) Furthermore, for e = [z], we generally have the degree of e as $|z|^2$. The degree of the endomorphism [m], for example, is thus $|m|^2 = m^2$.

[0027] In conventional elliptic curve cryptography, the endomorphism [m] is evaluated frequently. The number m represents a private key, and [m]P = mP represents a public key. The function [m] can be computed efficiently, even for a large value of m, much faster than one could add up the m^2 terms that would appear in the fully expanded polynomial forms of the numerator and denominators of r(x) for [m]. The crucial observation here is that a large degree endomorphism can be efficiently computed.

[0028] The following example lists every possible endomorphism of degree 2 on any elliptic curve. This list is complete up to equivalence of rational maps and elliptic curves. These are taken from Silverman's *Advance Topics in the Arithmetic Elliptic Curves* (Silverman's).

[0029] The first is e = [z] = [1+ i], defined on the curve E :

$$y^2 = x^3 + x, \text{ as: } \qquad e(x,y) = \left(\frac{x^2+1}{z^2 x}, \frac{y(x^2-1)}{z^3 x^2} \right)$$

Notice that z appears as a rational function defining the action of e, so e is only defined when E is defined over a field F that contains a value corresponding to z. (This comment also applies to the two endomorphism e below)

[0030] The second is e = [z] = [$\sqrt{(-2)}$], defined on E :

$$y^2 = x^3 + 4x^2 + 2x, \text{ as: } \qquad e(x,y) = \left(\frac{x^2+4x+2}{z^2 x}, \frac{y(x^2-2)}{z^3 x^2} \right)$$

[0031] The third is e = [z] = [(1 + √(-7))/2], defined on E :

$y^2 = x^3 - 35x + 98$, as:

$$e(x,y) = \left(\frac{x^2 + x(z^2-2) - 7(1-z)^4}{z^2(x+z^2-2)}, \frac{y((x+z^2-2)^2 + 7(1-z)^4)}{z^3(x+z^2-2)^2} \right)$$

SUMMARY OF THE INVENTION

[0032] The inventors have recognized that it is possible to use the attributes of elliptic curve cryptosystems to obtain a TOWF that provides a robust cryptosystem with a reduced bandwidth.

[0033] In one aspect, the present invention provides a cryptographic system operating on an elliptic curve E of order n. The cryptosystem has an endomorphism [z] corresponding to a quadratic algebraic integer z that has the form $z^2 + uz + v = 0$, where u and v are secret integers, and v is relatively prime to n; a public key operation to apply the endomorphism [z] to cryptographic data x to obtain modified data x'; and a private key operation to apply [-w][u] + [z] to the modified data x' in order to obtain the data x, where w is an integer and wv = 1 mod n.

[0034] In another aspect, the present invention provides method for performing cryptographic operations in a cryptographic system operating on an elliptic curve E of order n. The method comprises the steps of deriving an endomorphism [z] corresponding to a quadratic algebraic integer z that has the form $z^2 + uz + v = 0$, where u and v are secret integers, and v is relatively prime to n; applying a public key operation using the endomorphism [z] to cryptographic data x to obtain modified data x'; and applying a private key operation using [-w][u] + [z] to the modified data x' in order to obtain the data x, where w is an integer and wv = 1 mod n.

BRIEF DESCRIPTION OF THE DRAWINGS

[0035] An embodiment of the invention will now be described by way of example only with reference to the accompanying drawings, in which:

[0036] Figure 1 is a schematic representation of a cryptographic exchange scenario.

[0037] Figure 2 is a schematic representation showing an application of a trapdoor one-way function.

[0038] Figure 3 is a schematic representation showing an application of the trapdoor one-way function of Figure 2 for encryption.

[0039] Figure 4 is a schematic representation showing an application of the trapdoor one-way function of Figure 2 for digital signatures.

[0040] Figure 5 is a schematic representation showing an application of the trapdoor one-way function of Figure 2 for aggregated signatures.

[0041] Figure 6 is a schematic representation showing an application of the trapdoor one-way function of Figure 2 for aggregated signatures with a single message and multiple trapdoor one-way functions for multiple signers.

DETAILED DESCRIPTION OF THE INVENTION

[0042] Referring therefore to Figure 1, a cryptosystem 10 has a first entity 12, and a second entity 14 that communicate via a communication channel 16. The first entity 12 and second entity 14 each have a cryptographic module 15 that applies public key functions or private key functions 18 available to both entities 12, 14. Each entity 12, 14 will utilize the key functions 18 with the TOWF to obtain encryption/decryption or signing/verifying as described above.

[0043] In order to implement such a system, it is necessary to determine a suitable TOWF with corresponding public key functions and private key functions. The inventors have recognized that a suitable TOWF may be obtained by use of a quadratic algebraic integer z.

One then finds a curve E and rational map defining [z] on E. The rational map [z] is the TOWF. Judicious selection of z will ensure that it has the necessary cryptographic attributes, namely:

(a) [z] can be efficiently computed

(b) that [z] is difficult to invert

(c) determination of z from the rational functions defining [z] is difficult, and

(d) knowledge of z allows one to invert [z] on a certain set of elliptic curve points.

[0044] More generally, one can use a rational map r between two different curves E and E'. The rational map can be used as a TOWF. For ease of implementation, however, it is more convenient to use E = E'. A rational map from E to E is the preferred implementation.

[0045] Because every rational map (i.e. from E to E) is a composition of a translation and an endomorphism, where the translation is easy to determine and invert, the most secure part of the rational map is the endomorphism. Therefore an endomorphism is the preferred implementation of the rational map.

[0046] The inventors have recognized that one potential way to calculate the trapdoor inverse, for inverting z, is to use the quadratic equation for z: $z^2 + uz + v = 0$, where u and v are integers. Dividing this equation by vz gives $(z+u)/v + (1/z) = 0$. Hence $(1/z) = -(z+u)/v$. Now, (1/z) is not generally a quadratic algebraic integer. More precisely, if z has degree greater than 1, then (1/z) is not a quadratic algebraic integer. Therefore, there is no endomorphism that inverts [z]. Instead there is a dual endomorphism $[z'] = [-(z+u)]$, which satisfies $[z][z'] = [v]$. In a specific field F, the order n of the elliptic curve E can sometimes be relatively prime to v, which means there is an integer w such that $wv = 1 \bmod n$. This means that [w] acts as an inverse of [v] for the points of E defined over F.

[0047] In this case, the action of [z] on E(F) is invertible by the endomorphism $[w][z'] = [-w(z+u)]$. If [z] can be found efficiently, then it is likely that [-w(z+u)] can as well. An alternate expression for this is [-w]([u] + [z]).

[0048] Accordingly, it is possible to utilize the endomorphism [z] as the public key operation and the relationship [-w][w] + [z] as the private key operation.

[0049] The integers u, v are maintained secret and are only available to the entity performing the private key function.

[0050] It will be appreciated that this will be specific to the field F and will not be true for E defined over another field F'. The points of E defined over F are sometimes indicated as E(F) to emphasize that points with coordinates outside of F are not under consideration.

[0051] In order for [z] to be a trapdoor one-way function, it should be computationally infeasible to determine u and v from the public definition of [z], otherwise its inverse on E(F) is efficiently computable as [-w]([u] + [z]). Therefore, [z] needs to be given in a form that does not allow an easy determination of u and v.

[0052] By providing [z] as a pair of rational functions, it is believed that u and v cannot easily be determined. Typically, the first coordinate is a function of x only, so that [z] is somewhat in canonical form (r(x), g(x, y)), then the description for evaluating r(x) may potentially reveal the degree of the numerator of r(x), even though the full expansion of r(x) as a ratio of two polynomials may be infeasible due to the large number of terms. Since the degree of [z] is v, it is possible that the description of [z] will reveal v. Therefore, to make sure that [z] is a one-way trapdoor, it is important to ensure that u is also not revealed, otherwise [z] could be inverted, as described above.

[0053] According to Silverman's, determining the endomorphism ring of a general elliptic curve is a non-trivial problem. Since v and u essentially determine the endomorphism ring, up to an integer factor, it is generally infeasible to determine v and u from a description of the elliptic curve alone. It is therefore plausible that from the description of a single complex endomorphism, it is still a non-trivial problem to determine the endomorphism ring. In particular, this means it is still plausible that determining u from the description of [z] as a pair of rational functions is a non-trivial problem.

[0054] Accordingly, the degree of z should be chosen such that it has a reasonably large order. This helps to ensure that all possible values of u cannot be exhausted using the

relationship $u^2 < 4v$. This follows from above, because z must be an imaginary complex number.

[0055] One possible construction for [z] is based on the following observations. As discussed above, if e = [z] = (r(x),cyr'(x)) has degree m, then r(x) = p(x)/q(x) where p and q are polynomials of degree m and m-1 respectively. The kernel of e is the set of m points elliptic $O = Z_1, Z_2, \ldots, Z_m$, such that $e(Z_j) = O$ for j from 1 to m. If $Z_j = (z_j, y_j)$ for j from 2 to m, then it can be assumed that $q(x) = (x - z_2)(x - z_3) \ldots (x - z_m)$. Moreover, $mZ_j = O$, since $[z'][z] = [m]$ where z' is the conjugate of z as determined above as $mZ_j = [m]Z_j = [z'][z]Z_j = [z']O = O$ Furthermore, the kernel of e is a subgroup of order m in the elliptic curve E, though not necessarily as a part of E(F). The elliptic curve, as a whole, generally has at least m+1 such subgroups.

[0056] Next, consider the elliptic curve containing the point $B = (0, \sqrt{b})$. Suppose that there is some point W such that $[z]W = B$. Let $W_j = W + Z_j$ for j from 1 to m. (Note $W_1 = W + Z_1 = W + O = W$) Suppose that $Wj = (wj, uj)$ for $j = 1$ to m. Then $p(x) = d(x-w_1)(x-w_2) \ldots (x-w_m)$ for some constant d.

[0057] Notice that $p(x) = d(x - w_1)u(x)$ where the roots of u(x) are essentially a rational function of the roots of q(x). When the roots of two polynomials have a simple relationship such as this, there is a transformation of the coefficients of the polynomial. For example if the roots of u(x) are the squares of the roots of q(x) then $u(x) = q(\sqrt{x})\, q(-\sqrt{x})\, (-1)^{\deg q(x)}$. In this way, it is seen that the ability to evaluate q(x) provides a means to evaluate u(x).

[0058] Applying the above observations, one may search for a subgroup of order m in some elliptic curve E, whose finite x-coordinates are the zeros of a low Hamming Weight polynomial q(x). It is desirable to have a low Hamming Weight polynomial q(x) because they are efficient to evaluate. One would then find a point W as mentioned above, which allows one to compute the numerator p(x) efficiently, as outlined above. Once p(x) and q(x) can be evaluated, then r(x) can be evaluated.

[0059] An illustration of how one may find such polynomials p(x), q(x) is as follows. Note that if Z_j is in the kernel of [z] then so is $-Z_j$ and thus z_j can appear as a double root of q(x). Suppose that q(x) has a degree m that is prime. Suppose further that m is an Elkies

prime, the precise meaning of which is not a concern for the following discussion. This means that $q(x) = s(x)^2$ for a polynomial s(x) of degree (m-1)/2, which is a factor of the m^{th} division polynomial. The Schoof-Elkies-Atkin (SEA) algorithm for counting points on an elliptic curve E(F) includes a step where a polynomial of the form s(x) is found. The coefficients of the polynomial v(x) are found by a recursion equation. Therefore, methods are known for constructing such a polynomial. In the SEA algorithm, such s(x) are found for relatively small values of m, but for the present purpose, it is advantageous to make m large.

[0060] Another possible approach is to choose an irreducible polynomial s(x) of low Hamming weight. Let z be one of its roots, where z is the x-coordinate of some point over the elliptic curve E. The point may have a finite order m. This finite order will hold for any root z of s(x), by applying Galois automorphisms. If it is also the case that these points arising from the roots of s(x) are closed under, that is, they form a subgroup of E, then s(x) has the desired form. For this to happen, we would basically need a Galois automorphism g and a point P on E such that g(P) = 2P. By searching for a g, P, and E such that this is possible, one may be able to find a polynomial s(x) of the desired form. In practice, the y-coordinate can be ignored because it can only take one of two values.

[0061] If the endomorphism's kernel intersects the group E(F) at only the point O, then the action of the endomorphism e on the group E(F) is invertible. In this case, the endomorphism e is an automorphism of the group E(F). Generally the group E(F) will be cyclic, and in the following discussion, we assume that E(F) is cyclic. If e is an automorphism of a cyclic group of order n, then an algorithm realized by the inventors determines an integer d such that e(G) = dG, where one uses additive notation for the group. The cost of this algorithm depends on the factorization of n – 1. It is known that random values of n generally have a factor f that is approximately $n^{1/3}$. Given a factor of this size, the algorithm can determine d in a constant multiple of f steps. This is considerably faster than the generic algorithms for finding d given dG. These generic algorithms take $n^{1/2}$ steps.

[0062] Therefore, it is desirable that the group E(F) has order n such that n – 1 does not have a factor f near to $n^{1/3}$. An alternative to choosing n in this way is simply to choose n slightly larger, so that cost of an attack of $n^{1/3}$ is out of reach for the adversaries under consideration. For example, at a security level of 80 bits, such a larger n could be chosen so that n is approximately 2^{240}, and at a security level of 128 bits, n could be chosen so that n is

approximately 2^{384}. However, for efficiency reasons it is preferable to use a smaller n, and therefore it is presumed that the extra work necessary to ensure n – 1 has a size similar to $n^{1/3}$ will be undertaken.

[0063] The manner in which an endomorphism e would be used is generally shown in Figure 2. The first entity 12 takes an x value. It could choose one of the two corresponding y values arbitrarily. It would then apply the public key function [z] as a rational map e = (r(x), g(x,y)) and evaluate e(x, y) to arrive at some value (x', y'). This would be the basic public key operation. A second entity 14 receives the message (x', y') and then applies e^{-1} to get the value (x, y) This would be the basic private key operation [-w][u] + [z]. Notice that if y is changed to –y, the y' changes to – y', but x' and x are unaffected. Therefore y can more or less be ignored for all practical purposes.

[0064] To apply this to encryption as shown in Figure 3, the first entity 12 sets x to the plaintext and x' to the ciphertext by application of the public key function [z]. Known sophisticated approaches to public key encryption generally apply some randomized padding to the plaintext x, so that, among other things, repeated encryption of the same plaintext give different ciphertexts. The second entity 14 decrypts the ciphertext x' using the private key function to obtain plaintext x.

[0065] To apply this to signatures as shown in Figure 4, the second entity 14 sets x' to be the message to be signed, and computes x as the signature by application of the private key function. Generally some hashing is used to create x' from a longer message, which is a standard technique for digital signatures. The first entity 12 uses the public key operation e to confirm that e(x, y) = (x', y'). The hash function is one-way, so the first entity cannot forge a signature by starting from (x, y) and applying e to get (x', y'), because the next step would be to find a message M, such that x' = Hash (M), which is considered infeasible for a one-way hash function.

[0066] If the problem of inverting [z] is as hard as the discrete logarithm problem in E, then the size of the cryptographic group can be smaller than the group used for the RSA TOWF. For example, a 3072 bit RSA modulus is consider to be roughly as secure as an elliptic curve defined over a 256-bit field. The security level of both these objects is considered to be 128 bits, which is a commercial grade security level now most widely used

across the Internet, such as for online banking. The elliptic curve trapdoor one-way function [z], the size of signature x or basic ciphertext x' is 256 bits, whereas for RSA the size is 3072 bits.

[0067] Comparing to conventional elliptic curve cryptography (ECC), a signature for a 256-bit elliptic curve is about 512 bits long, which is twice the size of the signature for an elliptic curve TOWF. A similar savings is possible for encryption.

[0068] In another embodiment and application of the present invention the TOWF is applied to the aggregation of signatures or ciphertexts. The following will be explained for signatures, but it will be appreciated that the details for ciphertexts are quite similar.

[0069] Aggregation of signatures means a single signature represents a multiplicity of messages signed by a single signer, or a single message signed by a multiplicity of signers, or a multiplicity of messages signed by a multiplicity of signers.

[0070] Referring now to Figure 5, to sign t messages $m_1, m_2, \ldots, m_t$ a signer (e.g. first entity 12) hashes each message and converts each hash to an elliptic curve point, yielding t points $P_1, \ldots, P_t$ which are then added together to yield a point $P = P_1 + \ldots + P_t$. The signer then applies the inverse function e^{-1} to obtain the signature $S = e^{-1}(P)$, which is a single message for multiple messages. Verification by another entity (e.g. second entity 14) consists then of hashing the messages, converting each hash to a point, summing to a total P, and then applying the public key 18 operation e to S by checking if e(S) = P. The advantage of doing this over simply concatenating the messages is to achieve greater flexibility for the signer wishing to change parts of the message, because the signing is additive.

[0071] The procedure described above does not impose an order of signing individual message components, i.e., signature verification is relative to an (unordered) set of signatures signed by the same entity. It should be noted, however, that this procedure can easily be generalized towards weighted sums of individual signatures, rather than the sum of individual signature components $S_1, \ldots, S_t$, provided that the individual scalar multiples (the 'weights') can be retrieved or derived by the verifying entity. This would allow the enforcement of ordering in the signing process of these t messages, by making the weights dependent on the applicable ordering.

[0072] Referring now to Figure 6, if t different signers (e.g. collectively the first entity 12) use the same elliptic curve group and have different TOWF $e_1, \ldots, e_t$, then they may form an aggregate signature of a single message as follows. To sign a message m, the first signer of the first entity 12 computes a hash of the message and convert the hash to an elliptic curve point P. Then they together (i.e. all signers of the first entity 12) compute $e_t^{-1}(e_{t-1}^{-1}(\ldots(e_1^{-1}(P))))$, by each applying their private key operation, where signing takes place by entities 1, 2, ..., t in order. Verification (e.g. by the second entity 14) consists of applying each of the corresponding public key 18 operations, in reverse order, and checking whether the resulting point P corresponds to the hash value of the signed message m.

[0073] Generally, elliptic curve endomorphisms commute, so the order in which signing of a single message by multiple entities seems irrelevant. It should be noted, however, that this procedure can easily be generalized such as to enforce an ordering in the signing process. This can be realized by, for example, having each signing entity apply an offset to the signature computed, as described below.

[0074] Suppose the individual signature by entity i on point P is $e_i^{-1}(P+A_i)$, where the elliptic curve point A_i is unique for entity i. Then the ordered aggregate signature over message m by entities 1, 2,..., t is obtained by hashing m and converting this to the elliptic curve point P (as before), and subsequently having each of the signing entities apply his own signing operation on the resulting value. This results in $S_1=e_1^{-1}(P+A_1)$, $S_2=e_2^{-1}(S_1+A_2)$, ..., $S_t=e_t^{-1}(S_{t-1}+A_t)$, where S_t is the resulting aggregate signature. Signature verification is now a trivial modification of the procedure described above, provided the individual offsets $A_1, \ldots, A_t$ can be retrieved or derived by the verifying entity and depends on computing the sequence $S_{t-1}=e_t(S_t)-A_t$, $S_{t-2}=e_t(S_{t-1})-A_{t-1}$, ..., $S_1=e_2(S_2)-A_2$, $P=e_1(S_1)-A_1$ and checking whether the elliptic curve point P corresponds with the hash value of the signed message m.

[0075] Above, a modification of the original scheme is described such as to enforce an ordering of the signing process using offsets A_i that are unique for each of the signing entities. It will be seen that variations hereof are possible, such as defining $S_i=e_i^{-1}(f(P,i))$ rather than $S_i=e_i^{-1}(P+A_i)$, where f is a mapping on E with the property that one can efficiently re-compute P from f(P,i) and public information associated with signing entity i. The ordered signing of a single message by multiple entities could be useful for signing off, for example, projects in a large organization, where multiple signatures are required and a

project needs to be signed off by authorized parties involved in a particular hierarchical order (e.g., bottom-up).

[0076] 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. The entire disclosures of all references recited above are incorporated herein by reference.

What is claimed is:

1. A cryptographic system operating on an elliptic curve E of order n, said cryptosystem having an endomorphism [z] corresponding to a quadratic algebraic integer z that has the form $z^2 + uz + v = 0$, where u and v are secret integers, and v is relatively prime to n; a public key operation to apply said endomorphism [z] to cryptographic data x to obtain modified data x'; and a private key operation to apply [-w][u] + [z] to said modified data x' in order to obtain said data x, where w is an integer and $wv = 1 \bmod n$.

2. A cryptographic system according to claim 1 wherein said integer z is a complex number having real and imaginary components.

3. A cryptographic system according to claim 1 wherein said endomorphism [z] is represented as a rational map.

4. A cryptographic system according to claim 1 wherein said cryptographic data x comprises a message m, said public key operation operates to encrypt said message m to obtain an encrypted message m', and said private key operation operates to decrypt said encrypted message m' to obtain said message m, said public key operation performed by a first entity and said private key operation performed by a second entity, said first and second entities being part of said cryptographic system.

5. A cryptographic system according to claim 1 wherein said data x' comprises a message m for signature by a first entity of said cryptographic system, said private key operation operates on said message m to obtain a signature s, and said public key operation operates on said signature s by a second entity of said cryptographic system to verify said signature, said message m being originally generated by said second entity.

6. A cryptographic system according to claim 5 wherein said message m is generated from a hash function applied to an original message M.

7. A cryptographic system according to claim 1 wherein said cryptographic data x comprises a plurality of messages to receive a signature by a first entity of said

cryptographic system, said private key operation operating on a combination of said plurality of messages to obtain said signature, and said public key operation being used by a second entity of said cryptographic system to verify said signature and thereby verify each said plurality of messages.

8. A method for performing cryptographic operations in a cryptographic system operating on an elliptic curve E of order n, said method comprising the steps of deriving an endomorphism [z] corresponding to a quadratic algebraic integer z that has the form $z^2 + uz + v = 0$, where u and v are secret integers, and v is relatively prime to n; applying a public key operation using said endomorphism [z] to cryptographic data x to obtain modified data x'; and applying a private key operation using [-w][u] + [z] to said modified data x' in order to obtain said data x, where w is an integer and $wv = 1 \bmod n$.

9. A method according to claim 8 wherein said integer z is a complex number having real and imaginary components.

10. A method according to claim 8 wherein said endomorphism [z] is represented as a rational map.

11. A method according to claim 8 wherein said cryptographic data x comprises a message m, application of said public key operation encrypts said message m to obtain an encrypted message m', and application of said private key operation decrypts said message m from said encrypted message m'.

12. A method according to claim 8 wherein said data x' comprises a message m for signature; said private key operation operates on said message m to obtain a signature s, and said public key operation operates on said signature s to verify same.

13. A method according to claim 12 wherein said message m is generated from a hash function applied to an original message M.

14. A method according to claim 8 wherein said cryptographic data x comprises a plurality of messages to receive a signature, said private key operation operates on a combination of said plurality of messages to obtain said signature, and said public key

operation operating on said signature to verify same and thereby verify each said plurality of messages.

15. A method according to claim 8 wherein said data x comprises a message to be signed by a plurality of signers, said private key operation comprising a plurality of operations corresponding to each said signer, said private key operations being applied successively to said message to obtain a signature, said public key operation comprising a plurality of operations corresponding to each said signer, said public key operations being applied successively in opposite order to said private key operations to verify said signature.

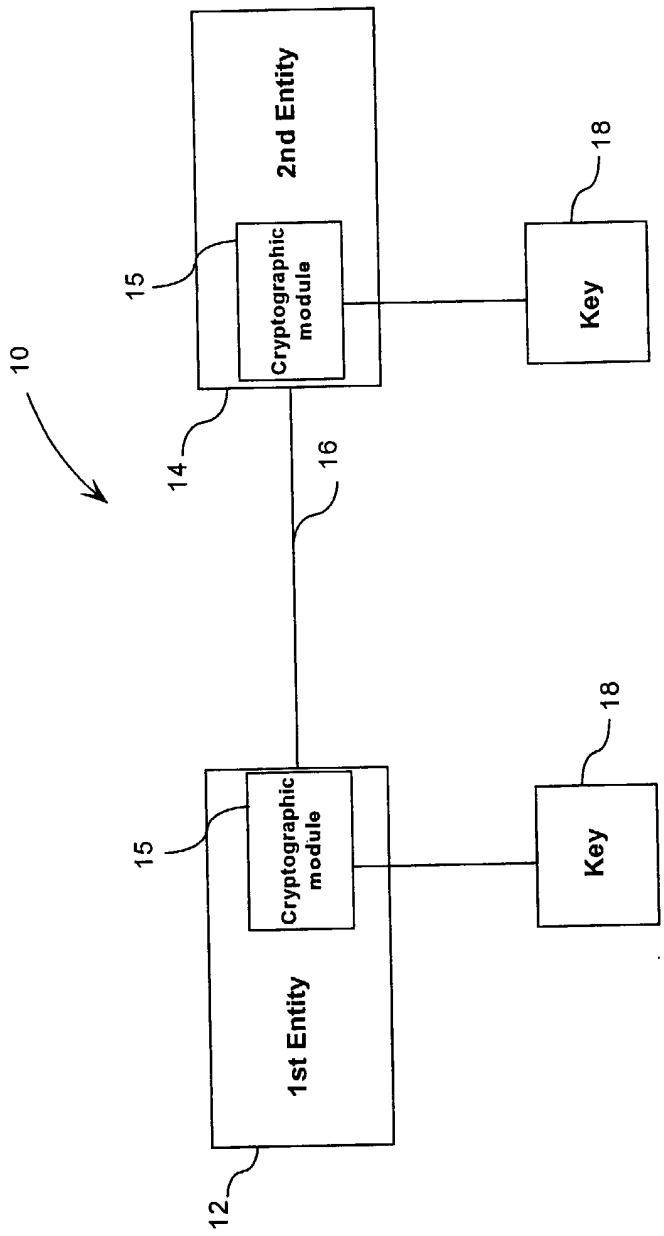

10
2nd Entity
15
Cryptographic module
18
Key
14
16
15
Cryptographic module
18
Key
1st Entity
12

Figure 1

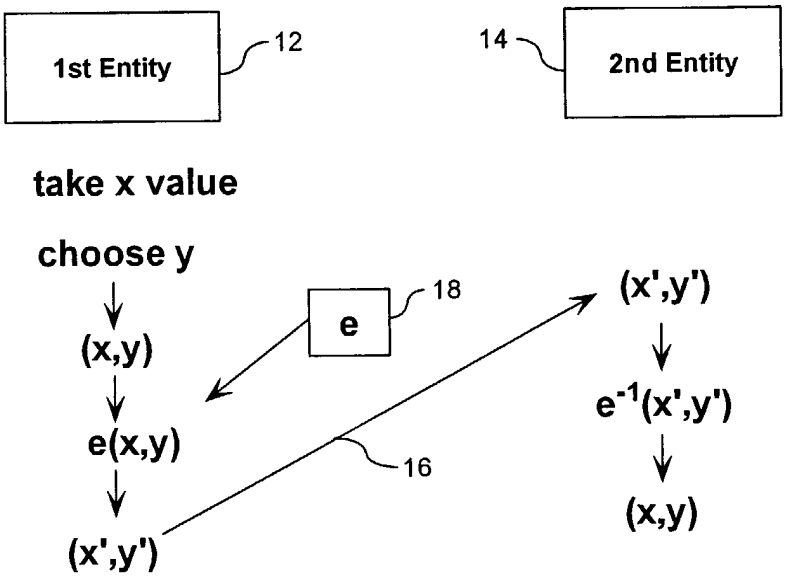


Figure 2

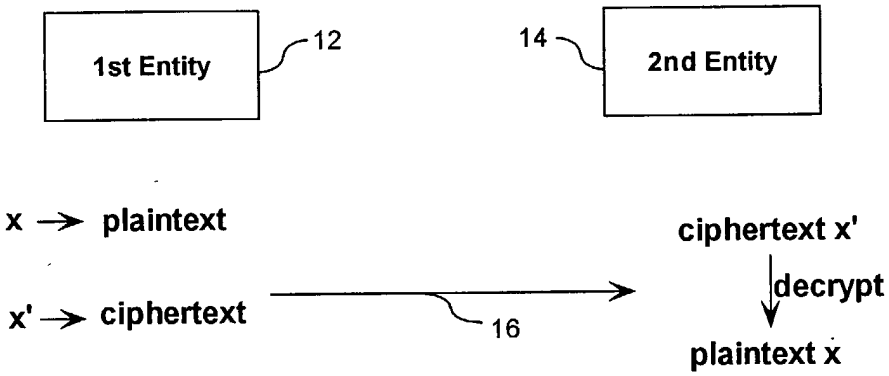


Figure 3

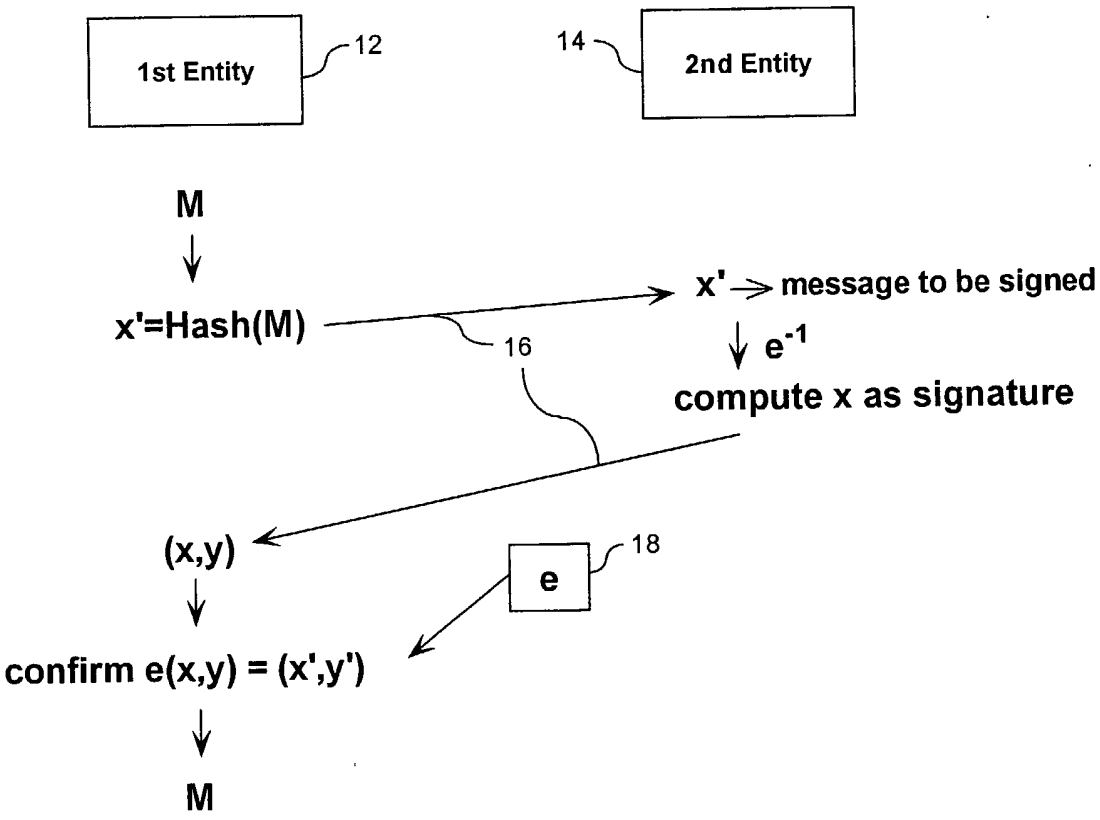

1st Entity
12
14
2nd Entity
M
x'=Hash(M)
16
x'
message to be signed
e-1
compute x as signature
(x,y)
e
18
confirm e(x,y) = (x',y')
M

Figure 4

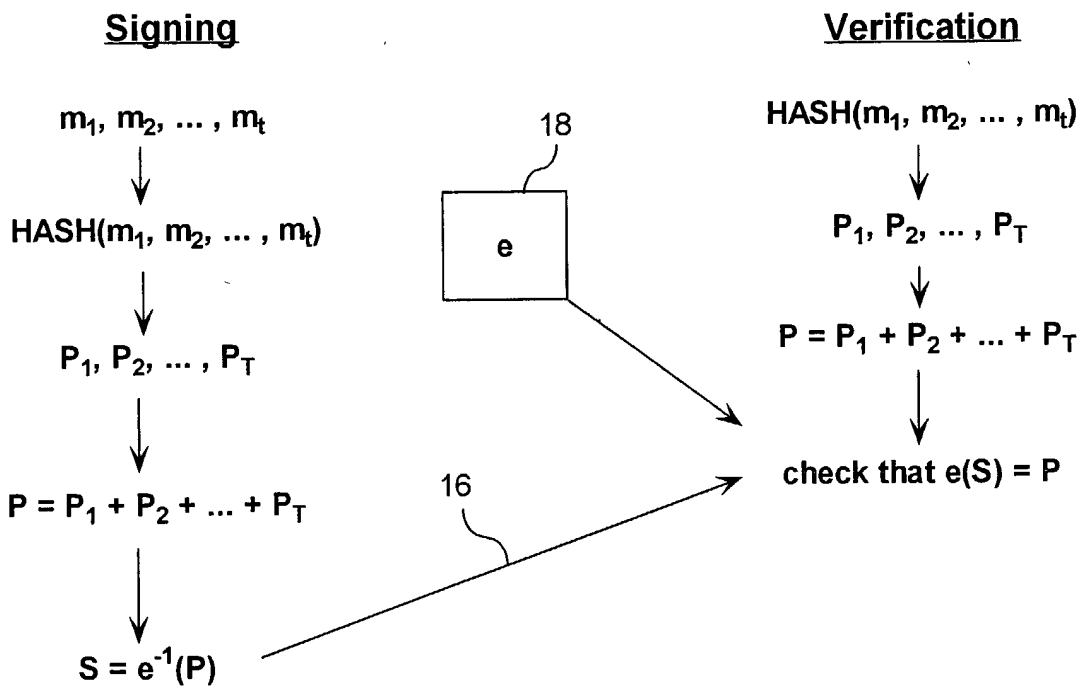

Signing
Verification
$m_1, m_2, \ldots, m_t$
$HASH(m_1, m_2, \ldots, m_t)$
$P_1, P_2, \ldots, P_T$
$P = P_1 + P_2 + \ldots + P_T$
$S = e^{-1}(P)$
18
e
16
$HASH(m_1, m_2, \ldots, m_t)$
$P_1, P_2, \ldots, P_T$
$P = P_1 + P_2 + \ldots + P_T$
check that e(S) = P

Figure 5

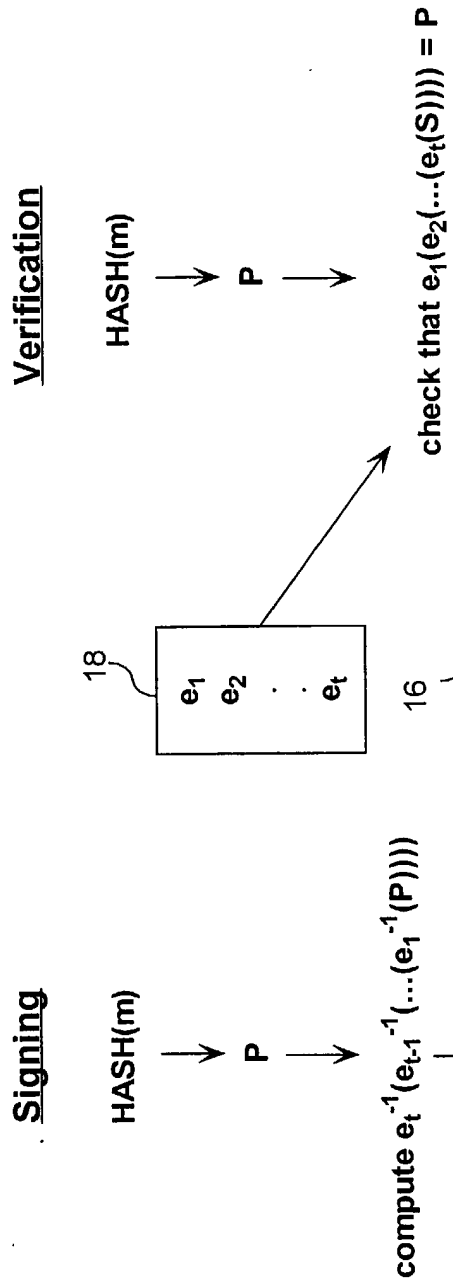

Signing
HASH(m)
P
compute $e_t^{-1}(e_{t-1}^{-1}(...(e_1^{-1}(P))))$
S
Verification
HASH(m)
P
check that $e_1(e_2(...(e_t(S)))) = P$
18
e_1
e_2
e_t
16

Figure 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/001720

A. CLASSIFICATION OF SUBJECT MATTER
IPC: H04L 9/30 (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)
H04L-9/30 (using keywords)

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)
Delphion, Canadian Patent Database, WEST
Keywords: public key, crypto$, elliptic, trapdoor, one-way, $morophism, map, rational

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US5,146,500; "Public key Cryptographic System Using Elliptiic Curves Over Rings"; Maurer, U. Sept. 8, 1992 (08-09-1992) [col. 3, lines 9-21], [col. 6, lines 9-22], [col. 14, lines 23-68], [col. 19, line 10 to col. 20 line 27], [col. 20, line 28 to col. 26, line 48], [col. 26, line 49 to col. 27, line 60], [col. 27, line 61 to col. 30, line 26], Figure 2.	1-15
A	US5,751,808; "Multipurpose High Speed Cryptographically Secure Sequence Generator Based on Zeta-One-Way Functions"; Anshel et al. May 12, 1998 (12-05-1998) [col. 2, line 49 to col. 3, line 59], [col. 8, line 32 to col. 11, line 64].	1-15
A	US6,480,605; "Encryption and Decryption Devices for Public-Key Cryptosystems and Recording Medium with Their Processing Programs Recorded Thereon"; Uchiyama et al. Nov. 12, 2002 (12-11-2002) [col. 5, line 58 to col. 6, line 15], [col. 14, line 15 to col. 17, line 22]	1-15
A,P	6,959,085; "Secure User Indentification Based on Ring Homomorphisms"; Hoffstein et al. Oct. 25, 2005 (25-10-2005) [col. 2, line 55 to col.3, line 67],[col. 4, line 1 to col. 5, line 23], Figs. 3-6	1-15

[ ] Further documents are listed in the continuation of Box C.

[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
22 February 2006 (22-02-2006)	10 March 2006 (10-03-2006)

Name and mailing address of the ISA/CA	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	Lawrence J. Engel (819) 997-2936

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/001720

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US5146500	08-09-1992	AT128297T T	15-10-1995
		DE69113245D D1	26-10-1995
		EP0503119 A1	16-09-1992
US5751808	12-05-1998	AU711911 B2	21-10-1999
		AU6894796 A	18-11-1996
		CA2214903 A1	31-10-1996
		EP0872079 A2	21-10-1998
		JP11502321T T	23-02-1999
		US5577124 A	19-11-1996
		WO9634473 A2	31-10-1996
US6480605	12-11-2002	CA2256179 A1	17-06-1999
		EP0924895 A2	23-06-1999
		JP3402441B2 B2	06-05-2003
		JP3402444B2 B2	06-05-2003
US6959085	25-10-2005	AU6889100 A	31-01-2001
		CA2369141 A1	04-01-2001
		EP1190523 A1	27-03-2002
		IL146350D D0	25-07-2002
		WO0101625 A1	04-01-2001