A New Elliptic Curve Based Analogue of RSA

N. Demytko

Telecom Australia Research Laboratories
770 Blackburn Road, Clayton, Victoria, 3168
Australia

Abstract. A new public key cryptosystem based on elliptic curves over the ring Z_n is described. The scheme can be used for both digital signature and encryption applications, does not expand the amount of data that needs to be transmitted and appears to be immune from homomorphic attacks. The main advantage of this system over other similar elliptic curve based systems is that there is very little restriction on the types of elliptic curves and types of primes (comprising the arithmetic modulus, n) that can be used. In addition, the system works on fixed elliptic curves. Problems associated with imbedding plaintext onto a curve are avoided by working within a multiple group structure. This enables the encryption and decryption operations to be performed on only the first coordinate of points on the given curve. The security of the system relies on the difficulty of factorising large composite numbers.

1 Introduction

An analogue of the Diffie-Hellman key exchange protocol [1] based on the use of elliptic curves was first proposed by Miller [2] in 1985. Elliptic curve based analogues of the ElGamal scheme and the Massey-Omura scheme followed in 1987 and are described in [3]. The first elliptic curve based analogue to the RSA scheme was introduced in 1991 [4]. Three trapdoor one-way functions (TOFs), based on elliptic curves over the ring Z_n, were proposed. The first class of function, denoted a "type 0" TOF, can only be used in a digital signature scheme, and not in a public key cryptosystem. The second, denoted a "type 1" TOF, has the commutative property and can be used for the same applications as RSA, however, its use restricts the types of primes (forming the arithmetic modulus) and the types of elliptic curves that can be used. The third class, denoted "type 2", is the Rabin generalisation of the type 1 scheme.

In this paper a new public key cryptographic scheme (or TOF) based on elliptic curves over a ring Z_n is proposed that overcomes most of the limitations of the schemes proposed in [4]. In common with RSA, security is based on the difficulty of factorising composite numbers formed by the product of two large primes (and not the discrete logarithm problem on elliptic curves on which the schemes presented in [2] and [3] are based). In the new scheme the message or plaintext is represented by the first (or x) coordinate of a point $P = (x, y)$ on an elliptic curve, $y^2 \equiv x^3 + ax + b$ modulo n, with fixed parameters (a and b). Ciphertext, x_e, is produced by computing the first coordinate only of the point P multiplied by e (the encryption multiplier). The plaintext is recovered by computing the first co-ordinate only of the point $eP = (x_e, y_e)$ multiplied by one of four possible decryption multipliers, d_i, $i = 1$ to 4

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 40-49, 1994.

(assuming n is the product of two large primes, p and q). The appropriate value of d_i to be used is determined by the values of the two Legendre symbols $\left(\frac{w}{p}\right)$ and $\left(\frac{w}{q}\right)$ where $w \equiv x_e^3 + ax_e + b$ modulo n. Digital signatures are produced in a similar fashion. The Chinese Remainder Algorithm may also be used to reduce the computation time involved in the decryption procedure and in the production of digital signatures.

A brief review of the basic definitions and facts about elliptic curves over a finite field is given in Section 2. Section 3 introduces the concept of a "complementary" group on an elliptic curve over a finite field. The proposed encryption scheme and the rules used to compute the first coordinate of a point on an elliptic curve are described in Sections 4 and 5, respectively. Sections 6 and 7 summarise the encryption and digital signature schemes in terms of the first coordinate of a point on an elliptic curve. Finally, the basis for scheme's immunity to homomorphic attack is given in Section 8.

2 Elliptic Curves (mod p)

Let p be a prime, greater than 3, and let a and b be integers chosen such that

$$4a^3 + 27b^2 \not\equiv 0 \pmod p). \qquad (1)$$

Then $E_p(a,b)$ denotes the elliptic group modulo p whose elements, (x,y), are pairs of non-negative integers less than p satisfying

$$y^2 \equiv x^3 + ax + b \pmod p, \qquad (2)$$

together with a special (identity) element denoted ∞ and called the point at infinity. The operation on two points, P and Q, to produce a third point, R, is termed "addition" and is written as

$$P + Q = R. \qquad (3)$$

If $P = (x_1,y_1)$ and $Q = (x_2,y_2)$, then $R = (x_3,y_3)$ is determined by the following rules:

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p \qquad (4)$$

$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod p \qquad (5)$$

where

$$\lambda \equiv \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } x_1 \not\equiv x_2 \pmod p \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } x_1 \equiv x_2 \text{ and } y_1 \not\equiv -y_2 \pmod p \end{cases} \tag{6}$$

If Q is the identity element, then P + Q = Q + P = P.

If $x_1 \equiv x_2$ and $y_1 \equiv -y_2 \pmod p$, then $P + Q = \infty$, i.e., $P = -Q$ or $(x_2,-y_2) \equiv -(x_2,y_2) \pmod p$.

The order of the group, denoted $|E_p(a,b)|$, is given by:

$$|E_p(a,b)| = 1 + \sum_{x=1}^{p} \left(\left(\frac{z}{p}\right) + 1 \right) \tag{7}$$

where $\left(\frac{z}{p}\right)$ is the Legendre symbol and $z \equiv x^3 + ax + b \pmod p$.

This equation is easy to verify by noting that, in addition to the point at infinity, for a given value of x:

(1) there are two values of y that correspond to that value of x, if z is a quadratic residue modulo p;

(2) there is one value of y that corresponds to that value of x, if $z \equiv 0$ modulo p; and

(3) there are no values of y that correspond to that value of x, if z is a quadratic non-residue modulo p.

A polynomial-time algorithm, due to Schoof [5], for computing the order of an elliptic group over a finite field exists. However, even though it is far more efficient than computing (7) directly, it is not practical for large p. Practical techniques for computing the order of an elliptic group modulo p, for large p with stated properties, are discussed in [6]. Two particular cases using these techniques are described in [7] and are as follows.

In the first case, if p is an ordinary prime which is congruent to 1 modulo 4, r is a complex prime that divides p and is congruent to 1 modulo 2 + 2i, and D is any integer not divisible by p then the order of $E_p(-D,0)$ is

$$|E_p(-D,0)| = p + 1 - \overline{\left(\frac{D}{r}\right)_4}\, r - \left(\frac{D}{r}\right)_4 \overline{r} \tag{8}$$

where $\left(\frac{x}{r}\right)_4$ is the fourth power symbol and $\overline{r}$ is the conjugate of the complex integer r.

For example, if p = 13 and r = 3 + 2i, then

$$\begin{aligned}
|E_{13}(-1,0)| &= 14 - (1)(3 + 2i) - (1)(3 - 2i) = 8\\
|E_{13}(1,0)| &= 14 - (-1)(3 + 2i) - (-1)(3 - 2i) = 20\\
|E_{13}(-2,0)| &= 14 - (i)(3 + 2i) - (-i)(3 - 2i) = 18\\
|E_{13}(2,0)| &= 14 - (-i)(3 + 2i) - (i)(3 - 2i) = 10.
\end{aligned}$$

In the second case, if p is an ordinary prime which is congruent to 1 modulo 3, r is a cubic prime that divides p and is congruent to 2 modulo 3, and D is any integer not divisible by p then the order of $E_p(0,D)$ is

$$|E_p(0,D)| = p + 1 + \overline{\left(\frac{4D}{r}\right)_6}\, r + \left(\frac{4D}{r}\right)_6 \overline{r} \qquad (9)$$

where $\left(\frac{x}{r}\right)_6$ is the sixth power symbol and $\overline{r}$ is the conjugate of the cubic integer r.

For example, if p =13 and $r = -4 - 3\omega$, where $\omega = e^{2\pi i/3}$, then

$$\begin{aligned}
|E_{13}(0,1)| &= 14 + (\omega^2)(-4 - 3\omega) + (\omega)(-1 + 3\omega) = 12\\
|E_{13}(0,2)| &= 14 + (-1)(-4 - 3\omega) + (-1)(-1 + 3\omega) = 19\\
|E_{13}(0,3)| &= 14 + (1)(-4 - 3\omega) + (1)(-1 + 3\omega) = 9\\
|E_{13}(0,4)| &= 14 + (\omega)(-4 - 3\omega) + (\omega^2)(-1 + 3\omega) = 21\\
|E_{13}(0,5)| &= 14 + (-\omega^2)(-4 - 3\omega) + (-\omega)(-1 + 3\omega) = 16\\
|E_{13}(0,6)| &= 14 + (-\omega)(-4 - 3\omega) + (-\omega^2)(-1 + 3\omega) = 7
\end{aligned}$$

Note: It is well known that

$$|E_p(a,b)| = p + 1 + \alpha, \qquad \text{where } |\alpha| \le 2\sqrt{p} \qquad (10)$$

for every elliptic curve over F_p.

3 Complementary Group on a Given Elliptic Curve (mod p)

Definition: Let p be a prime, greater than 3, and, again, let a and b be integers chosen such that (1) holds. In addition, let $E_p(a,b)$ denote the elliptic group modulo p whose elements, (x,y), satisfy equation (2), as before, but where y is an indeterminant in the field F_p for non-negative integer values of x. That is, y is of the form $y \equiv u\sqrt{v}$ (mod p), where u is a non-negative integer less than p and v is a fixed quadratic non-residue modulo p. The identity element, ∞, and the "addition" operation are identical to those defined in the previous section.

It is easy to show that all group axioms hold for the above definition. For example, if $P = (x_1,y_1) = (x_1,u_1\sqrt{v})$ and $Q = (x_2,y_2) = (x_2,u_2\sqrt{v})$ are two elements in the group, then $R = (x_3,y_3) = (x_3,u_3\sqrt{v})$ is also in the group (closure), i.e.,

$$(x_1,y_1) + (x_2,y_2) \equiv (x_3,y_3) \pmod{p}, \qquad (11)$$

where, if $x_1 \not\equiv x_2 \pmod{p}$,

$$x_3 \equiv \left(\frac{u_1 - u_2}{x_1 - x_2}\right)^2 v - x_1 - x_2 \pmod{p} \tag{12}$$

$$y_3 \equiv \left(\left(\frac{u_1 - u_2}{x_1 - x_2}\right)(x_1 - x_3) - u_1\right)\sqrt{v} \pmod{p}, \tag{13}$$

or, if $x_1 \equiv x_2$ and $y_1 \not\equiv -y_2 \pmod{p}$,

$$x_3 \equiv \left(\frac{3x_1^2 + a}{2u_1 v}\right)^2 v - x_1 - x_2 \pmod{p} \tag{14}$$

$$y_3 \equiv \left(\left(\frac{3x_1^2 + a}{2u_1 v}\right)(x_1 - x_3) - u_1\right)\sqrt{v} \pmod{p} \tag{15}$$

The order of this "complementary" group is given by

$$| \overline{E_p(a,b)} | = 1 + \sum_{x=1}^{p}\left(1 - \left(\frac{z}{p}\right)\right) \tag{16}$$

where $\left(\frac{z}{p}\right)$ is the Legendre symbol and $z \equiv x^3 + ax + b \pmod{p}$.

In this case, in addition to the point at infinity, for a given value of x:

(1) there are two values of y that correspond to that value of x, if z is a quadratic non-residue modulo p;

(2) there is one value of y that corresponds to that value of x, if $z \equiv 0$ modulo p; and

(3) there are no values of y that correspond to that value of x, if z is a quadratic residue.

Suppose there are A values of x for which $\left(\frac{z}{p}\right) = 1$, B values of x for which $\left(\frac{z}{p}\right) = 0$ and C values of x for which $\left(\frac{z}{p}\right) = -1$. In addition, since x must be in one of p possible residue classes,

$$A+B+C = p. \tag{17}$$

From (7) and (10),

$$|E_p(a,b)| = 1 + 2A + B = 1 + p + \alpha,$$

$$\text{i.e., } 2A + B = p + \alpha \tag{18}$$

Consequently, from (16), (17) and (18),

$$| \overline{E_p(a,b)} | = 1 + 2C + B = 1 + 2p - (2A + B) = 1 + p - \alpha \qquad (19)$$

4 Encryption Scheme

Select two primes, p and q, and let n = pq denote the arithmetic modulus. Select an elliptic curve with the parameters a and b where $\gcd(4a^3 + 27b^2, n) = 1$. Let $|E_p(a,b)| = 1+p+\alpha$, $| \overline{E_p(a,b)} | = 1+p-\alpha$, $|E_q(a,b)| = 1+q+\beta$ and $| \overline{E_q(a,b)} | = 1+q-\beta$. It is assumed that the order of these groups can be determined using the techniques referred to in Section 2. In addition, let x represent the plaintext and s the ciphertext (where $0 \leq x, s \leq n-1$).

Encryption is then defined as

$$(s,t) \equiv (x,y)\#e \quad (\mathrm{mod}\ n), \qquad (20)$$

where (x,y)#e (or eP) denotes the point P = (x,y) "multiplied" by e. Multiplication of a point P by i is defined as the addition of the point P to itself i times.

Decryption is defined as

$$(x,y) \equiv (s,t)\#d_i \quad (\mathrm{mod}\ n), \qquad (21)$$

where

$$e.d_i \equiv 1 \quad (\mathrm{mod}\ N_i), \quad i = 1 \text{ to } 4, \qquad (22)$$

$$\gcd(e, N_i) = 1, \quad i = 1 \text{ to } 4, \qquad (23)$$

$$N_1 = \mathrm{lcm}(p+1+\alpha, q+1+\beta) \qquad \text{if } \left(\frac{w}{p}\right) = 1 \text{ and } \left(\frac{w}{q}\right) = 1, \qquad (24)$$

$$N_2 = \mathrm{lcm}(p+1+\alpha, q+1-\beta) \qquad \text{if } \left(\frac{w}{p}\right) = 1 \text{ and } \left(\frac{w}{q}\right) \neq 1, \qquad (25)$$

$$N_3 = \mathrm{lcm}(p+1-\alpha, q+1+\beta) \qquad \text{if } \left(\frac{w}{p}\right) \neq 1 \text{ and } \left(\frac{w}{q}\right) = 1, \qquad (26)$$

$$N_4 = \mathrm{lcm}(p+1-\alpha, q+1-\beta) \qquad \text{if } \left(\frac{w}{p}\right) \neq 1 \text{ and } \left(\frac{w}{q}\right) \neq 1, \qquad (27)$$

$$z \equiv x^3 + ax + b \quad (\mathrm{mod}\ n), \qquad (28)$$

$$y = \sqrt{z}, \qquad (29)$$

$$w \boxminus s^3 + as + b \quad (\mathrm{mod}\ n), \text{ and} \qquad (30)$$

$$t = \sqrt{w}. \qquad (31)$$

Alternatively, the decryption time may be reduced, by a factor approaching 4, by computing (21) modulo p and modulo q and then combining the results via the Chinese Remainder Theorem.

Note that only the first coordinates, x and s, have to be computed in this scheme. Computation of the second coordinates, y and t, can be avoided using the rules and algorithm described in [7]. The rules are summarised in the following section.

Note also that if p, q, a and b are chosen so that $\alpha = \beta = 0$ in equations (24) to (27), then $N_i = \mathrm{lcm}(p+1, q+1)$ remains fixed for all i. Consequently, d_i is fixed for all i, and decryption is independent of the Legendre symbols, $\left(\frac{w}{p}\right)$ and $\left(\frac{w}{q}\right)$.

5 Rules for Computing the First Coordinate of a Point on an Elliptic Curve

In the elliptic group $E_p(a,b)$ (or $\overline{E_p(a,b)}$), let $(x_i,y_i) \equiv (x,y)\#i \pmod p$. If $y_i \not\equiv 0 \pmod p$, then

$$x_{2i} \equiv \frac{(x_i^2 - a)^2 - 8bx_i}{4(x_i^3 + ax_i + b)} \pmod p. \qquad (32)$$

In addition, if $x_i \not\equiv x_{i+1}$ and $x \not\equiv 0 \pmod p$, then

$$x_{2i+1} \equiv \frac{(a - x_i x_{i+1})^2 - 4b(x_i + x_{i+1})}{x(x_i - x_{i+1})^2} \pmod p \qquad (33)$$

Unfortunately congruence (33) cannot be used if $x \equiv 0$ modulo p (or q). However, it can be shown that the congruence can be rearranged to give

$$x_{2i+1} \equiv \frac{4b + 2(a - x_i x_{i+1})(x_i + x_{i+1})}{(x_i - x_{i+1})^2} - x \pmod p \qquad (34)$$

which is valid for all $0 \leq x \leq p-1$ (and consequently for all $0 \leq x \leq n-1$ when computations are performed modulo n). It can be shown that x_i is never congruent to x_{i+1} modulo p (or q) during the course of computing $s \equiv x_e$ modulo n, as given by (20). Similarly s_i is never congruent to s_{i+1} modulo p (or q) during the course of computing (21). However, it is possible (although extremely unlikely) that y_i may become congruent to 0 modulo p (or q) during the course of computations and therefore for (32) to become undefined. The way around this problem is to use homogeneous coordinates and therefore avoid division until the final stage of the encryption or decryption procedure.

Homogeneous coordinates are formed by setting $x \equiv \frac{X}{Z}$ (mod p) and $y \equiv \frac{Y}{Z}$ (mod p). If $(x_i, y_i) \equiv (X_i/Z_i, Y_i/Z_i) \equiv (X/Z, Y/Z)\#i$ (mod p), computational rules (32) and (34) can be restated in the following form.

$$X_{2i} \equiv (X_i^2 - aZ_i^2)^2 - 8bX_iZ_i^3 \pmod{n} \tag{35}$$

$$Z_{2i} \equiv 4Z_i(X_i^3 + aX_iZ_i^2 + bZ_i^3) \pmod{n} \tag{36}$$

$$\begin{aligned} X_{2i+1} \equiv\ & Z[4bZ_i^2Z_{i+1}^2 + 2(aZ_iZ_{i+1} + X_iX_{i+1})(X_iZ_{i+1} + X_{i+1}Z_i)] \\ & - X(X_iZ_{i+1} - X_{i+1}Z_i)^2 \pmod{n} \end{aligned} \tag{37}$$

$$Z_{2i+1} \equiv Z(X_iZ_{i+1} - X_{i+1}Z_i)^2 \pmod{n} \tag{38}$$

6 The Encryption Scheme in Terms of the First Coordinate of a Point on an Elliptic Curve

Encryption and Decryption as defined in (20) and (21) can be rewritten in terms of the notation of Section 5 as:

$$s \equiv x_e \equiv X_e/Z_e \pmod{n} \qquad \text{where } X = x \text{ and } Z = 1\text{, and} \tag{39}$$

$$x \equiv s_{d_i} \equiv S_{d_i}/Z_{d_i} \pmod{n} \tag{40}$$

where S = s, Z = 1 and d_i is as defined by (22) to (31).

7 Digital Signature Scheme in Terms of the First Coordinate of a Point on an Elliptic Curve

A digital signature, s, is formed by computing:

$$s \equiv X_{d_i}/Z_{d_i} \pmod{n} \tag{41}$$

where X = x is the message or plaintext, Z = 1 and d_i is as defined by (22) to (31) with $z \equiv x^3 + ax + b$ (mod n) replacing w in (24) to (27).

Signature verification is performed by computing:

$$x \equiv S_e/Z_e \pmod{n} \qquad \text{where } S = s \text{ and } Z = 1. \tag{42}$$

8 Homomorphic Attack

Let s_1 and s_2 represent two signatures produced for the messages x_1 and x_2 respectively. If it is possible to determine the second coordinates, t_1, t_2, y_1 and y_2, corresponding to the the above first coordinates, then it is possible to create a new signature, s, on a new message, x, by using the addition rules given in Section 2 (using modulo n rather than modulo p arithmetic), i.e., a new signature point:

$$(s,t) = (s_1,t_1) + (s_2,t_2) \tag{43}$$

can be computed that corresponds to the new message point:

$$(x,t) = (x_1,y_1) + (x_2,y_2). \tag{44}$$

In fact, only t_1 and t_2 need to be determined since x can be found, once s is known, by using congruence (42).

Values for t_1 and t_2 can be treated as indeterminants and computed using (30) and (31), i.e.,

$$t_1 = \sqrt{w_1} \quad \text{where} \quad w_1 \equiv s_1^3 + as_1 + b \pmod n$$

$$t_2 = \sqrt{w_2} \quad \text{where} \quad w_2 \equiv s_2^3 + as_2 + b \pmod n$$

The next step is to eliminate one of the indeterminants, say t_2. If t_2 is written in the form, $t_2 = u\sqrt{w_1}$, then s is given by (see Section 3):

$$s \equiv \left(\frac{1 - u}{s_1 - s_2}\right)^2 w_1 - s_1 - s_2 \pmod n \tag{45}$$

The only remaining problem is to determine the value of $u \equiv \sqrt{w_2/w_1} \pmod n$. However, it is impossible to find a square root modulo n unless the prime factors of n are known. Consequently, u cannot be determined from w_2 and w_1, even if w_2/w_1 is a quadratic residue modulo n (in most cases, an integer value of u will not exist, since w_2/w_1 will not be a quadratic residue modulo n). Thus, whilst it is possible to add a point to itself any number of times in this scheme, it is impossible to add two arbitrary points together if only the first coordinates of the points are known (unless the primes (p and q) comprising the arithmetic modulus, n, are also known). As a result, it appears that a new signature cannot be created from two old signatures. For the same reason, the active attack described in [4] will also not succeed.

9 Conclusions

A new public key cryptographic scheme based on elliptic curves over a ring Z_n has been proposed. The main advantage of the scheme is that it can be used on elliptic curves with arbitrary parameters. In addition, digital signatures can be produced that are of the same size as the message. Furthermore, the scheme does not appear to be prone to homomorphism attacks. Finally, the techniques used in this scheme can be employed to produce an elliptic curve analogue of the Pollard Rho method of factorisation.

10 Acknowledgement

The permission of the Director, Research, of Telecom Australia to publish this paper is hereby acknowledged.

11 References

[1] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, pp. 644-654, 1976.

[2] V.S. Miller, "Use of Elliptic Curves in Cryptography", Advances in Cryptology: Proceedings of CRYPTO '85, Lecture Notes in Computer Science, Vol. 218, pp. 417-426, Springer-Verlag, 1986.

[3] N. Koblitz, A Course in Number Theory and Cryptography, Spinger-Verlag, New York, 1987.

[4] K. Koyama, U.M. Maurer, T. Okamoto and S.A. Vanstone, "New Public-Key Schemes Based on Elliptic Curves over the Ring Zn", CRYPTO '91 Abstracts, Santa Barbara, CA, pp. 6-1 to 6-7, August 11-15, 1991.

[5] R.Schoof, "Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p", Mathematics of Computation, Vol.44, No.170, pp. 483-494, 1985.

[6] A.K. Lenstra and H.W. Lenstra, Jnr., "Algorithms in Number theory", University of Chicago, Department of computer Science, Technical Report # 87-008, 1987.

[7] D.M. Bressoud, Factorisation and Primality Testing, Springer-Verlag, New York, 1989.