IJCS
International Journal of Cryptography and Security
Volume 1, Issue 2, 2011, pp-10-13
Available online at http://www.bioinfo.in/contents.php?id=115

SINGULAR CUBIC CURVE BASED PKC: AS SECURE AS FACTORING

SAHADEO PADHYE
Department of Mathematics, Motilal Nehru National Institute of Technology, Allahabad, 211004, UP, India
*Corresponding author. E-mail: sahadeo_mathrsu@yahoo.com

Received: Received: July 29, 2011; Accepted: August 11, 2011

Abstract- The public key cryptosystem (PKC) given by Rabin was as secure as factoring. This feature attracted Mayer et al to generate such PKC based on nonsingular cubic curve. The mathematical concept as cubic curve was quite popular to be used for public key by that time. The object of this paper is to propose a public key cryptosystem that is as secure as factoring and based on the singular cubic curve over Z_n. In the scheme given by Mayer et al the size of ciphertext is a 5tuples. The size of ciphertext, in our proposed scheme is only 3tuples. We have shown that the proposed scheme is about two times faster than that of the scheme given by Mayer et al for a 2-*log n* bit long message.
Keywords- Public Key Cryptosystem, RSA scheme, Rabin scheme, singular cubic curve

Introduction

Since the seminal paper given by Diffie and Hellmann [1], numerous public key cryptosystems have been proposed. The first practical and most popular public key cryptosystem is RSA [13] given by Ravist, Shamir, and Adlemann. The security of RSA is based on the difficulty of factoring large integer *n,* which is product of two large primes *p* and *q.* In the RSA scheme, an user U (1) - Chooses two large primes *p* & *q*, computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. (2) - Chooses a random integer *e* less than and relatively prime to $\varphi(n)$ (3) - U then chooses an integer *d* such that $ed \equiv 1 \bmod \varphi(n)$. The secret key for U is (*d*, *p, q*) and the public is (*e, n*) respectively. The ciphertext as well as plaintext is [1, *n*-1]. To encrypt any plaintext M, the sender S computes the ciphertext as $C = M^e \bmod n$. The ciphertext C is decrypted by computing $M = C^d \bmod n$. If an efficient algorithm of factoring exists, the attacker can break the RSA scheme easily. But it is not known whether there is some easier way to break RSA other than factoring.

In 1979, Rabin [12] proposed a public key cryptosystem and digital signature based on the quadratic residue theory. That scheme was proved to be as intractable as factoring. In other words, as long as factorization of large integer into primes remains practically intractable, this scheme remains computationally secure. Its security is much better than RSA in theory, but it is susceptible to chosen ciphertext attack. Rabin's original scheme has some disadvantages in practice, such as the ambiguity of four plaintexts to one ciphertext. This ambiguity can be avoided by knowledge of side information of the plaintext, for example: the plaintext must be in English words. But random key is when transmitted, there is no such knowledge to distinguish the four solutions. In practice, this problem is overcome by adding pre-specified redundancy to the original plaintext before encryption. (For example character of the message i.e. odd or even and the Jacobi symbol of the message, or last 64 bits of the plaintext). Then, with high probability, exactly one of the four square roots of a legitimate ciphertext *C* has this redundancy. So the receiver can select this one as the intended plaintext. Williams [15] solved these problems of ambiguity through quadratic residue theory. Harn and Keisler [3] proposed to integrate coding techniques into Rabin cryptosystem. Their variation uses parity bits as redundancy. The problem of ambiguity is naturally solved. Because redundancy is added to solve ambiguity, for one identical plaintext message, the ciphertext in Rabin cryptosystem is longer than RSA. When Rabin scheme is used in signature, the signature is longer then RSA too. Harn and Keisler [4, 5] proposed some variations to eliminate this disadvantage.

The use of elliptic curve in cryptography was first time proposed by Miller [9] and independently by Koblitz [8]. The security of these cryptosystems is based on the discrete logarithm problem (DLP) in a group of

points on an elliptic curve. This is known as ECDLP problem in literature. Later, Mourer et al. [7] proposed a public key cryptosystem using elliptic curve over the ring Z_n, where n is a product of two large primes. The security of their cryptosystem is based on the factoring problem for n but it is not known whether decryption is equivalent to factoring n. They used elliptic curve of special form such that the factorization of n directly give the order of the group. The knowledge of the order of group is important in the decryption process. The details about elliptic curve cryptosystem can be found in [10]. Later, Koyama [6] replaced elliptic curve by singular cubic curve to propose a fast RSA type scheme. By using the idea given by Williams [15] and Mourer et al [7], Meyer et al [11] proposed a public key cryptosystem based on elliptic curves over Z_n whose security is equivalent to factoring n. Now, in this paper we propose a public key cryptosystem, which is as secure as factoring and based on singular cubic curve over the ring Z_n, where n is a product of two large primes. The proposed system is about two times faster than that of the scheme given by Mayer et al. Also, the size of ciphertext of the scheme proposed by Mayer et al is a 5tuple where as in our scheme is a 3tuple.

Singular cubic curve

In this section, first we discuss some basic facts about singular cubic curve over the finite field F_p and the ring Z_n where n is the product of two distinct odd primes greater then 3.

Consider the congruence equation

$$y^2+axy = x^3+bx^2 \bmod p\ ,\ a\ ,b \in Z_p. \qquad (1)$$

The set of all solutions $(x, y) \in F_p \times F_p$ to (1) denoted by $C_p(a, b)$ is called singular cubic curve .

Let F_p be a finite field with p elements and F_p^* be the multiplicative group of F_p. Clearly the order of F_p^* denoted by $\#F_p^* = p-1$.

A non-singular part of singular cubic curve denoted by $C_p(a, b)$ is defined as the set of solutions $(x, y) \in F_p \times F_p$ to equation (1) excluding a singular point (0, 0), but including the "point at infinity", denoted by O.

It is well known that the same addition laws defined by the chord and tangent method in the case of elliptic curve still holds in the singular cubic curve [14, 10]. For any point $P \in C_p(a, b)$, the sum $P + O$ is by definition, equal to P, which is also equal to $O + P$. For $P = (x_0, y_0)$, we define $-P$ the additive inverse of P as the point $(x_0, -y_0 - ax_0)$. The sum of $P + (-P)$ is defined to be O. For $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $P_1 \neq P_2$ the sum $P_1+P_2 = (x_3 , y_3)$ is calculated as follows:

$$x_3 = \gamma^2 + a\gamma - b - x_1 - x_2 \qquad (2)$$

$$y_3 = \gamma(x_1 - x_3) - y_1$$

Where

$\gamma = (y_2 - y_1)/(x_2 - x_1)$, if $(x_1, y_1) \neq (x_2, y_2)$ and

$\gamma = (3x_1^2+2bx_1 - ay_1)/(2y_1+ax_1)$, if $(x_1, y_1) = (x_2 , y_2)$.

The existence of such addition law makes $C_p(a, b)$ a finite abelian group . In fact, the group structure of $C_p(a, b)$ is well known [2, 14]. For any $k \in F_p$ the multiplication operation $\times$ is defined as bellow:

$k \times (x ,y) = (x, y) + (x, y) + (x, y) + \ldots + (x, y)$ k times over $C_p(a ,b)$.

An isomorphism between $C_p(a, b)$ and F_p^* is defined in [10,14] for the curves $(y - \alpha x)(y - \beta x) = x^3$ over F_p^*, where $\alpha, \beta \in F_p^*$, which is equivalent to equation (1) with $a = -\alpha - \beta \pmod p$ and $b = -\alpha\beta \pmod p$. When $b = 0$ we can put $\alpha = 0$ and $\beta = -a$ ($\neq 0$).

An isomorphism mapping from $C_p(a, 0)$ to F_p^* and inverse of that are given in the following theorem:

Theorem 2.1[10]**.** The mapping $\omega: C_p(a , 0) \rightarrow F_p^*$ defined by

$\omega: O \rightarrow 1$ and $(x, y) \rightarrow 1 + ax/y = x^3/y^2$

is a group isomorphism . The group isomorphism mapping $\omega^{-1}: F_p^* \rightarrow E_p(a, 0)$ is defined by

$\omega^{-1}: 1 \rightarrow O$ and $v \rightarrow (a^2v/(v-1)^2, a^3v/(v-1)^3)$

Hence, with this isomorphism, the order of $C_p(a, 0)$ is denoted by $\#C_p(a, 0) = p-1$.

Let n be the product of two primes p and q (>3). Let $Z_n = \{0, 1, 2, 3,\ldots..n-1\}$ and Z_n^* be a multiplicative group of Z_n , we consider similarly the congruence

$y^2 + axy = x^3 + bx^2$ over Z_n , $a, b \in Z_n$ (3)

A non-singular part of a singular cubic curve over Z_n denoted by $C_n(a, b)$, is defined as the set of solutions $(x, y) \in Z_n \times Z_n$ to equation (3) excluding a singular point which is either congruent to (0,0) modulo p or congruent to (0, 0) modulo q , but including a "point at infinity" O. By Chinese Remainder Theorem, $C_n(a, b)$ is isomorphic as a group to $C_p(a, b) \times C_q(a ,b)$.

An addition operation on $C_n(a, b)$ is defined by chord and tangent method. Although the addition is not always defined, the probability of such a case is negligible small for large p and q.

By using **Theorem 2.1** and Chinese Remainder Theorem, the following theorem holds:

Theorem 2.2 [2]. For (x_1, y_1) and (x_i , y_i) satisfying $(x_i , y_i) = i \times (x_1, y_1)$ over $C_n(a , 0)$, we have

$$1+ax_i/y_i = (1+ax_1/y_1)^i \bmod n$$

i.e. $$x_i/y_i = (x_1/y_1)^i \bmod n \qquad (4)$$

Rabin Cryptosystem

In 1979, Rabin [12] proposed a public key encryption and digital signature scheme. Rabin scheme is based on quadratic residue theory and its security is as intractable as factoring. In this section, quadratic

residue theory is introduced and a brief introduction of Rabin scheme is also given.

Quadratic Residue Theory
First, we will give a brief introduction of quadratic residue theory.

Quadratic Residue and Principal Residue
Let p be an odd prime and u is an integer not divisible by p. Then u is called quadratic residue mod p if $x^2 = u$ (mod p) has one integer solution. Otherwise, u is called quadratic non-residue. **QR** denotes the set of all quadratic residues and **QNR** denotes the set of all quadratic non-residues. There are exactly $(p-1)/2$ quadratic residues mod p and the same number of quadratic non-residues mod p. If u is a quadratic residue mod p then u has exactly two roots, one of them between 0 and $(p-1)/2$ and the other between $(p-1)/2$ and $(p-1)$. One of these square roots is also a quadratic residue mod p that is called principle square root. When n is composite, for u to be a quadratic mod n, it must be a quadratic residue modulo all the prime factors of n. Rabin scheme uses $n = pq$, where p and q are primes. In this case, there are exactly $(p-1)(q-1)/4$ quadratic residue mod n. A quadratic residue mod n must be a quadratic residue (mod p) and a quadratic residue (mod q). One quadratic residue normally has four different square roots. However, certain quadratic residue has either p or q as a divisor. Their quadratic residues have just two square roots. But, if n is product of two large primes then only a negligible portion of quadratic residue has two square roots. The chance of these happening is very small and can be ignored. So each quadratic residue has exactly four square roots when large primes are used in Rabin scheme.
Legendre and Jacobi symbol are used to describe whether any number is quadratic residue mod k are not, where k is any integer.

Legendre Symbol
Legendre symbol is defined to describe whether any number u is quadratic residue modulo any prime p. Legendre symbol, written as $L(u, p)$ is defined when u is any integer and p is any odd prime.
$L(u,p) = 0$; if u is divisible by p
$L(u,p) = 1$; if u is quadratic residue mod p
$L(u,p) = -1$; if u is quadratic non-residue mod p

Jacobi Symbol
Jacobi symbol is written as $J(u, n)$, is a generalization of Legendre symbol to composite. Far any integer u and any odd integer n,
$J(o,n) = 0$
$J(u,n) = L(u, n)$ if n is prime
$J(u, n) = J(u,p_1)\, J(u,p_2)\, J(u,p_3) \ldots\ldots J(u, p_m)$

If $n = p_1 p_2 \ldots\ldots p_m$

Rabin Cryptosystem
It is interesting to observe that the security of all RSA type public key cryptosystems is based on difficulty of factoring. More precisely, it is well known that if one is able to factor the modulus $N = pq$ (where p and q are large primes of equally size) for that system, then the system can be broken. However, if the system is broken by way of some attack than it does not necessarily mean that it is possible to factor into required primes. This became possible in the Rabin scheme and is called the scheme as secure as factoring.
Rabin scheme gets its security from the difficulty of finding square roots modulo a composite number. This problem is equivalent to factoring. To generate keys the receiver chooses two large primes p and q both congruence to 3 (mod 4) and computes $n = pq$. The public key for the receiver R (say) is n and the secret keys are p and q respectively. To encrypt any plaintext M, the sender S (say) computes $C = M^e \bmod n$ and sends the ciphertext C to the receiver. Now, the receiver R who knows secret keys p and q can computes the square root of C as follows. R first computes $m_1 = C^{(p+1)/4} \pmod p$, $m_2 = (p - C^{(p+1)/4}) \pmod p$, $m_3 = C^{(q+1)/4} \pmod q$, $m_4 = (q - C^{(q+1)/4}) \pmod q$. Then by using the Chinese Remainder Theorem the receiver can computes all possible four roots of C under modulo n.
One of the disadvantages of the scheme given by Rabin is that, corresponding to one plaintext; there are four possible ciphertexts. According to William [15], all four roots of ciphertext can be divided into two types. Type I with the Jacobi Symbol 1 and the type II with the Jacobi symbol –1. Further, each one of those types contains two different square roots, one even and the other odd. Thus, if the sender sends the character of plaintext M such as the Jacobi symbol of M under mod n and the even or oddness of M then receiver can easily determine which root is proper one.

Proposed Cryptosystem
Suppose the sender S wants to send a message pair (m_x, m_y) belongs to $Z_n^* \times Z_n^*$ such that $m_x^3 \neq m_y^2 \bmod n$ to the receiver R. Here n is the product of two large primes p and q both congruence to 3 mod 4. n is the public key for the receiver R and the secret keys are p and q respectively.

Encryption Process
To encrypt the message pair (m_x, m_y), the sender S first computes the isomorphic image M of (m_x, m_y) by using the isomorphism defined as above. Then, s/he computes the complete ciphertext (C, a, t) as follows:

$M = (m_x^3/m_y^2) \bmod n$
$C = M^2 \bmod n$
$a = (m_x^3 - m_y^2)/m_x m_y \bmod n$
$t = 1$ if J(N, n) = 1 and M is odd
$t = -1$ if J(N, n) = -1 and M is odd
$t = 2$ if J(N, n) = 1 and M is even
$t = -2$ if J(N, n) = -1 and M is even
S sends the complete ciphertext (C, a, t).

Decryption Process

To decrypt the ciphertext, receiver R first determines all the square roots of C by using the secret keys p and q. Let M_1, M_2, M_3, M_4 are four square roots of the ciphertext C. Next, he/she first checks the Jacobi symbol of M_i and even and oddness of M_i for i =1,2,3,4. With the help of the information of t, he/she can ensure that which one is proper square root of C, i.e. the plaintext M. Now, he computes the inverse isomorphic image of M by using the inverse isomorphism. Finely, he/she gets the plaintext pair (m_x, m_y).

Analysis

The cryptosystem presented in this paper is a generalization and improvement of the scheme presented in [6]. The use of small exponent 2, increases the speed of the encryption process. In fact, one exponent modulo p and one exponent modulo q and the use of Chinese Remainder Theorem are needed to get required square root. In the Koyama scheme [6], decryption process requires to compute, one exponent under modulo p and one exponent under modulo q and use of Chinese Remainder Theorem. There fore the decryption speed of proposed scheme is about the same as that of the Koyama scheme. Next, although the encryption process of our scheme is computationally same expansive than that of the scheme proposed by Mayer et al. [11] based on nonsingular cubic curve but in our scheme, 2-*log n* bit message is encrypted at a time where as, the scheme proposed by Mayer et al. [11] encrypts *log n* bit message. Hence, our proposed scheme is about two times faster than that of the Mayer et al scheme for the 2-log n bit message. In addition, in our scheme the size of ciphertext is a 3tuple where as in the Mayer et al scheme it is a 5tuple.

Thus the advantage of our proposed scheme over Mayer et al scheme is that, it is about 2 times faster and its ciphertext is 0.6 times smaller than that of the Koyama scheme. The advantage over Koyama scheme is that, the encryption speed of proposed scheme is very fast than that of the Koyama scheme.

Conclusion

In this paper we proposed a public key cryptosystem that is as secure as factoring and based on the singular cubic curve over Z_n. In the scheme given by Mayer et al the size of ciphertext is a 5tuples. The size of ciphertext, in our proposed scheme is only 3tuples. We have shown that the proposed scheme is about two times faster than that of the scheme given by Mayer et al for a 2-*log n* bit long message.

References

[1] Whitfield Diffie and Martin Hellmann (1976) *IEEE Transaction on Information Theory*, v.22, 644-654.

[2] Husemaller D. (1987) *Elliptic curves. Springer Verlag.*

[3] Harn L. and Kiesler T. (1989) *Proc. of Workshop on Applied Computing'89*.

[4] Harn L. and Kiesler T., Electronics Letter v.25,n.15,pp 1016(1989).

[5] Harn L. and Kiesler T. (1990) *Fifth Annual Computer Security Applications Conference, IEEE Computer Society Press,* 263-270.

[6] Koyama K. (1995) *Proceeding in LNCS EUROCYPT* '95, Springer Verlag , Volume - 921 , PP. 329-340.

[7] Koyama K., Maurer U., Okamoto T., Vanstone S.A. (1991) *Crypto'91*, 252-266.

[8] Neal Koblitz (1985) *Math.Comput.*48.203-209.

[9] Miller V. (1985) *LNCS CRYPTO'85*, pp 417-426.

[10] Menezes A. (1993) *Kluwer Acadamic Publisher.*

[11] Meyer Bernd and Volker Muller (1996) *LNCS EUROCRYPT'96*,v.1070, 33-38.

[12] Rabin M.O. (1979) *MIT Lab for Computer Science , Tech. Rep.LCS/TR* 212.

[13] Rivest R.L., Shamir A., Adlemann L. (1978) *Communication of the ACM* 1,2 ,120-126.

[14] Silverman J.H. (1986) *The arithmetic of elliptic curve. Graduate text in mathematics vol.106 . Springer Berlin*.

[15] Williams H.C. (1980) *A IEEE Transaction on Information Theory IT*-26, 726-729.