A PUBLIC KEY CRYPTOSYSTEM BASED ON SINGULAR CUBIC CURVE

Sahadeo Padhye
School of Studies in Mathematics,
Pt.Ravishankar Shukla University,
Raipur (C.G.),India.
Email: *sharmabk_nib@sancharnet.in*

Abstract

An efficient and semantically secure public key cryptosystem based on singular cubic curve is proposed in this paper. It is about two times faster than the cryptosystem of David at the same security label and more efficient than the Koyama scheme at high security level. Further, the partially known plaintext attack and the linearly related plaintext attacks are analyzed and concluded that those are not possible in the proposed scheme.

2000 Mathematics Subject Classification. 94A60.

Key Words : RSA, DRSA problem, Singular cubic curve, Semantic security.

1. Introduction

The most striking development in the history of cryptography came in 1976 when Diffie and Hellman published "New Direction in Cryptography" [9]. This paper introduced the revolutionary concept of public key cryptosystem and also provided a new and ingenious method for key exchange, the security of which depends on the intractability on the discrete logarithm problem . In such a system each user secretly obtains a crypto cell (E, D) and then publishes the encryptor E in a public file. The user keeps secret the details of his corresponding decryption procedure D. Clearly the central requirement of such a system is that it be prohibitively difficult to figure out the decryptor $D = E^{-1}$ from a knowledge of E but D and E are easy to compute. In 1978, Ravist ,Shamir and Adleman discovered the first practical public key encryption and signature scheme known as RSA [19]. The security of RSA scheme was based on factoring product of two large prime numbers, which is a very hard mathematical problem.

The efficiency and security are two important goals for any cryptosystem. The details about the all kinds of attacks and security notions we refer the

This work is supported under CSIR (JRF) scheme, India (2002).

reader to the paper by Bellare et.al [1]. In 1984, Goldwasser and Micalli [11] defined a security notion, that an encryption scheme should satisfy, namely semantic security. This notion means that the ciphertext does not leak any useful information about the plaintext. The encryption scheme proposed by T. ElGamal [10] based on the Diffie -Hellman [9] problem was semantically secure . Its semantic security was related to the Decisional Deffie-Hellmann problem [9]. However, because of the computational load, this scheme never became very popular. Some other security notions were non-malleability [8] and Plaintext-Awareness [2]. Non-malleability means that any attacker can not modify a ciphertext while keeping any control over the relation between the resulting plaintext and original one and the Plaintext-Awareness means that no one can produce a valid ciphertext without knowing the corresponding plaintext.

The speed of the standard RSA cryptosystem was very low and many attacks [7] on RSA cryptosystem were identified. Hence, to increase the security and /or efficiency of the standard RSA cryptosystem other variants of RSA were developed. The standard RSA cryptosystem was not semantically secure but its variants such as [2, 18, 5] were semantically secure against chosen plaintext attack and chosen ciphertext attack but, not all of them were more efficient than the ElGamal [10] encryption scheme. It was David [6] who proposed a new DRSA problem and introduced an efficient RSA version of ElGamal encryption with some security properties, namely semantically security against chosen-plaintext attacks. The scheme given by David was 6 times faster than the ElGamal encryption scheme.

On the other hand, singular cubic curve was first time used by Koyama for the construction of RSA type public key cryptosystem. Koyama [14] and Koyama et al [15, 16] have constructed three different PKCs analogue to RSA based on singular cubic curve. In these schemes, two plaintexts m_x, m_y are used to form a point $M = (m_x, m_y)$ on the singular cubic curve over Z_n, and the ciphertext is a point $C = e \times M$ on the same curve. Later, Seng et al [21] have shown that all three schemes are equivalent and become insecure if a linear relation is known between two plaintexts. In all the schemes proposed by Koyama, the partially known plaintext attack and linearly related plaintext attack is admissible. The partially known plaintext and linearly related plaintext attack are possible only when the ciphertext belongs to the same curve where the plaintext belongs. Also, Koyama schemes are not semantically secure.

Following the line of Koyama, in this paper, we propose a semantic secure public key cryptosystem based on singular cubic curve over Z_n. Our scheme has not only enhanced speed as compare to Koyama and David [6] schemes but is secured against the partially known plaintext [3] and linearly related plaintext attack [21] .

2. Singular Cubic Curve [12, 20].

In this section 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

$$y^2 + axy = x^3 + bx^2 mod\, p \tag{1}$$

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

2.1 Singular Cubic Curve Over F_p

Let $F_p{}^\star$ be the multiplicative group of F_p. A nonsingular part of singularcubic 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 $\bigcirc$. 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 [20, 17]. For any point $P \in C_p(a, b)$. For the sum $P + \bigcirc$, by definition, is equal to P, which is also equal to $\bigcirc + P$. 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 $\bigcirc$. 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:

$$x_3 = \gamma^2 + a\gamma - b - x_1 - x_2 \qquad y_3 = \gamma(x_1 - x_3) - y_1 \tag{2}$$

where

$$\gamma = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } (x_1, y_1) \neq (x_2, y_2), \\ \frac{3x_1^2 + 2bx_1 - ay_1}{2y_1 + ax_1} & \text{if} (x_1, y_1) = (x_2, y_2). \end{cases}$$

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 [12, 20]. For any $k \in F_p$ the multiplication operation $\otimes$ is defined as bellow :

$k \otimes (x, y) = \overbrace{(x, y) \oplus (x, y) \oplus (x, y) \oplus ..... \oplus (x, y)}$ k times over $C_p(a, b)$

An isomorphism between $C_p(a, b)$ and $F_p{}^\star$ is defined in [20, 17] for the curve $(y - \alpha x)(y - \beta x) = x^3$ over $F_p{}^\star$, where $\alpha, \beta \in F_p{}^\star$, which is equivalent to equation (1) with $a = -\alpha - \beta mod\, p$ and $b = -\alpha\beta mod\, p$. When $b = 0$ we can put $\alpha = 0$ and $\beta = -a(\neq 0)$.

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

Theorem 2.1. The mapping $\omega : C_p(a, 0) \to F_p{}^\star$ defined by

$$\omega : \bigcirc \to 1 \text{ and } (x, y) \to 1 + \frac{ax}{y} = \frac{x^3}{y^2} \text{ is a group isomorphism.}$$

The group isomorphism mapping $\omega^{-1} : F_p{}^\star \to C_p(a, 0)$ is defined by

$$\omega^{-1} : 1 \to \bigcirc \text{ and } v \to (\frac{a^2 v}{(v-1)^2}, \frac{a^3 v}{(v-1)^3})$$

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

2.2 Singular Cubic Curve Over Z_n

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

$$y^2 + axy = x^3 + bx^2 \text{ over } Z_n \text{ where } a, b \in Z_n. \tag{3}$$

A nonsingular 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 points which are either congruent to $(0, 0) modulo p$ or congruent to $(0, 0) moduloq$, but including a point at infinity $\bigcirc$. 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. Since we are taking $p$and q very large, there fore the addition operation on $C_n(a, b)$ can be defined.

By using Theorem 1 and Chinese Remainder Theorem, the following theorem holds :

Theorem 2.2 : For (x_1, y_1) and (x_i, y_i) satisfying $(x_i, y_i) = i \otimes (x_1, y_1)$ over $E_n(a, 0)$,

we have

$$1 + \frac{ax_i}{y_i} = (1 + \frac{ax_1}{y_1})^i (mod\, n)$$

i.e.

$$\frac{x_i}{y_i} = (\frac{x_1}{y_1})^i (mod\, n) \tag{4}$$

3. DRSA Problem.

The details about the DRSA problem one can refer the papers [6, 13, 4]. Certain definitions and results of those papers used for the construction of a new public key cryptosystem are given below .

Definition 3.1.Computational Dependent -RSA (C-DRSA (n, e)).

To determine the value of $(k+1)^e \mod n$ for given $k^e \mod n$ where k is randomly chosen element of $Z_n{}^\star$ is known as C-DRSA problem.

The success probability of an adversary A is denoted by $Succ(A)$ and defined by,

$Succ(A)$= Pr $[A(k^e \mod n) = (k+1)^e \mod n | k \leftarrow Z_n{}^\star]$.

The decisional version of this problem defined by Decision Dependent RSA problem (D-DRSA).

Definition 3.2. The Decisional Dependent - RSA (D-DRSA(n, e)).

Distinguish the two distributions

$Rand = (\alpha, \gamma) = (k^e \mod n, r^e \mod n) | k, r \leftarrow Z_n{}^*$,

$DRSA = (\alpha, \gamma) = (k^e \mod n, (k+1)^e \mod n) | k \leftarrow Z_n*$.

The advantage of a distinguisher A denoted by $Adv(A)$ and defined by :

$Adv(A) = |Pr_{Rand}[A(\alpha, \gamma) = 1] - Pr_{DRSA}[A(\alpha, \gamma) = 1]|$.

Definition 3.3. Extraction Dependent -RSA (E-DRSA).

A problem to determine the value k for given $k^e \mod n$ and $(k+1)^e \mod n$ is known as Extraction Dependent RSA (E-DRSA) problem.

It can be easily proved that the extraction of e^{th} root is easier to solve than the computational Dependent RSA problem and Extraction Dependent RSA problem together.

Theorem 3.1. Breaking the RSA problem is computationally equivalent to the breaking the C-DRSA and E-DRSA problem together both.

Concerning the Extraction Dependent RSA problem and the theorem 3.1, one can then state the following theorem :

Theorem 3.2. There exists a reduction form the RSA problem to the Computational Dependent RSA problem in $\bigcirc(|n|^2, e \times |e|^2)$ time.

4. Proposed Public Key Cryptosystem.

Now we propose a new D-RSA type scheme over singular cubic curve $E_n(a, 0)$ with the massage dependent variable a similar to that of Koama scheme [14]. The security of the proposed scheme is based on the D-RSA problem, more precisely on the difficulty of factoring n, which is product of two large primes p and q. Let a plaintext (m_x, m_y) be an integer pair, where $m_x, m_y \in {Z_n}^\star$ and $m_x^3 \neq m_y^2 (mod\ n)$. We first transform the plaintext (m_x, m_y) to ${Z_n}^\star$, and then encrypt the isomorphic image of (m_x, m_y) i.e. $\frac{m_x^3}{m_y^2}$.

4.1.Key Generation.

To generate the keys, receiver R chooses two large prime p and q and computes $n = p.q$. Let $N = lcm(p-1, q-1)$. Receiver determines an integer e less then and relatively prime to N. He then computes an integers d_p and d_q such that $d_p \equiv e^{-1} mod\ (p-1)$ and $d_q \equiv e^{-1} mod\ (q-1)$. He made the keys (e, n) publicly available and keep secret to the keys (d_p, d_q, p, q).

4.2.Encryption.

To encrypt the message $(m_x, m_y) \in {Z_n}^* \times {Z_n}^*$ sender S, first chooses a random integer k with $k+1 \in {Z_n}^*$ and sends the ciphertext (C_1, C_2, b) to the receiver R with the receiver's public key (e, n). where

1. $C_1 \equiv k^e mod\ n$,
2. $C_2 = (k+1)^e \frac{{m_x}^3}{{m_y}^2} mod\ n$,
3. $a = \frac{{m_x}^3 - {m_y}^2}{m_x m_y} mod\ n$.
4. $b = (a + k^2) mod\ n$

4.3.Decryption.

The receiver R computes the original plaintext by using his/her secrete after getting the ciphertext (C_1, C_2, a) as follows :

1. R first computes $k_p = C_1^{d_p} mod p$ and $k_q = C_1^{d_q} mod\ q$. By the pair (k_p, k_q) and via Chinese Remainder theorem, R computes the value of k.
2. R then computes $a = (b - k^2) mod\ n$

3. $m = \frac{m_x^3}{m_y^2} mod\ n = \frac{C_2}{(k+1)^e} mod\ n$. Now by using the isomorphism mapping defined above s/he then computes the original plaintext (m_x, m_y) as follows :

$m_x = \frac{a^2 m}{(m-1)^2} mod\ n$ and $m_y = \frac{a^3 m}{(m-1)^3} mod\ n$

5. Efficiency and Security Analysis.

5.1. **Efficiency.** In the scheme given by Koyama, e^{th} power of $\frac{{m_x}^3}{{m_y}^2}$ under modulo n is computed during the encryption process. Where as, in our proposed scheme, the triples like $(k^e mod\ n, (k+1)^e mod\ n, k^2 mod\ n)$ are computed well in advance. Because of this pre-computation, the encryption process requires only one multiplication and one addition. This feature makes the encryption process more efficient than the scheme given by Koyama. Although, our decryption process remains about as efficient as the scheme given by Koyama [14].Following the analysis given by Koyama, let, x and y the coordinates of 2 $logn$-bit plaintext are transformed to a $logn$-bit plaintext by isomorphic mapping. This massage of $logn$ bit length is than encrypted using said encryption process. The obtained ciphertext is then decrypted using decryption key over ${Z_n}^*$ which is the transformed massage. Next, using the inverse transformation, we get the original 2 $logn$ bit length massage. If we exclude the transformation than the number of modulo multiplication is approximately same as the DRSA scheme in decryption process. Hence, the decryption speed of the proposed scheme is 2 times faster than that of D-RSA scheme [6] for a K bit long message if $\lceil \frac{K}{logn} \rceil$ is even.

5.2. **Security Analysis.** The semantic security (indistinguishability of encryption) is defined by Goldwasser & Micali [11]. According to them an attacker is seen as a two-stage ("find and guess") Turing machine, which first chooses two messages, during the "find"-stage. In the second stage, the "guess"-stage, she receives a challenge, which is the encryption of one of the both chosen messages, and has to guess which one is the corresponding plaintext. In other words, if the ciphertext does not leak any useful information about the corresponding plaintext, then the system is called semantically secure.

An intuitive argument that proposed cryptosystem is semantically secure against chosen plaintext attack in the D-DRSA problem is as follows. In order to determine any information about the plaintext m from the ciphertext, attacker need to have some information about $(k+1)^e (mod\ n)$, where k is randomly chosen element in ${Z_n}^*$. The only way to ascertain any information about the value of $(k+1)^e (mod\ n)$ is to first compute k (it is not sufficient to compute some partial information about k; it is necessary to have complete information about k in order to obtain any information about $(k+1)^e (mod\ n)$, as k is randomly chosen). It is not possible without knowing the secret key d or solving the DRSA problem.

Also, in the Koyama scheme, the message dependent variable a gives some information about the plaintext but, in the proposed scheme we keep it secret which is known by the authorized receiver only. Without knowing the value a attacker can neither use the Theorem 2.1 nor the addition operation over the exact singular cubic curve. Thus following the Theorem 9 of David [6] we state and prove the semantic security of proposed scheme as below.

Theorem 5.1 The scheme based on DRSA problem over singular cubic curve is semantically secure against chosen plaintext attack relative to the Decision Dependent RSA problem.

Proof. Let us consider an attacker $A(A_1, A_2)$ who can break the semantic security of this scheme within a time l and an advantage in the "guess" stage, greater than ϵ.

Now we construct a D-DRSA adversary; B, who is able to break the Decisional DRSA problem for the given public key (N, e) with an advantage greater than $\epsilon/2$ and similar running time. (The advantage of B in distinguishing the DRSA and Rand Distribution is $Adv(B) = Adv(A)/2$ and therefore greater than $\epsilon/2$).

$B(\alpha, \gamma)$:
Run $A_1(pk)$
Get m_o, m_1, s
Randomly Choose $b \in 0, 1$
$C_1 = \alpha, C_2 = m_b.\gamma(mod\ n)$
Run $A_2(s, m_o, m_1, (C_1, C_2))$
Get c
If $c = b$ Return 1
else Return o

Note that $m_b = m_{xb}^3/m_{yb}^2$ is isomorphic image of the plaintext pair (m_{xb}, m_{yb}) . Getting either of one is isomorphically equivalent to the other by the *theorem*2.1. Since semantic security $\Rightarrow$ D-DRSA problem is trivially, so we have nothing to prove. On the one hand, we have to study the probability for A_2 to answer $c = b$ when the pair (α, γ) comes from random distribution. But in this case, one can see that the pair $(C_1, C_2) \in (r^e, m_b s^e)|r, s \in {Z_n}^*$ is uniformly distributed in the product space ${Z_n}^* \times {Z_n}^*$ hence independently of b. Then

$Pr_{Rand}[B(\alpha, \gamma) = 1] = Pr_{Rand}[c = b] = \frac{1}{2}$

On the other hand; when the pair (α, γ) comes from the DRSA distribution, one can remark that (C_1, C_2) is valid ciphertext of m_b, following a uniform distribution among the possible ciphertexts. Then

$Pr_{DRSA}[B(\alpha, \gamma) = 1] = Pr_{DRSA}[c = b]Pr_b[A_2(s, m_0, m_1, \varepsilon(B)) = b] \stackrel{def}{=} \frac{1}{2} + \frac{Adv(A)}{2}$

It is well known that Blichenbacher [3] and Seng et al [21] attacks are possible when the ciphertexts belong to the same cubic curve, which contains the corresponding plaintexts. In our proposed scheme, the ciphertext C_2 form (C_1, C_2, a) is not isomorphic image of any point on the elliptic curve.

In other words in our scheme, the ciphertexts does not belong to the same cubic curve which contain corresponding plaintexts. As result, said attacks are not possible in our scheme.

From the analysis discussed in above paras it is clear that proposed public key cryptosystem is more efficient than the David's scheme and the scheme given by Koyama. Also, the partially known plaintext attacks and the linearly related plaintext attacks are not admissible in our scheme.

6. Conclusion

The analysis discussed in above paras are evidence of the fact that proposed public key cryptosystem is more efficient than the David's scheme and the scheme given by Koyama.

References

[1] Bellare M., Desai A., D. Pointcheval and P.Rogaway, relation among notions of security for public key encryption shcemes. Cryto'98 LNCS 1462, pp 26-45, Springer Verlag 1998.

[2] Bellare M. and Rogaway P., Optimal asymmetric encrytion -how to encrytp with RSA. Eurocrypt'94, LNCS 950, pp 92-111 Springer Verlag 1995.

[3] Blichenbacher D. , On the security of KMOV public key cryptosystem. LNCS Crypto'97v.1294, 235-348,1997.

[4] Coppersmith D., Franklin M., Patarin J. and Reiter M., Low exponent RSA with related messages. Eurocrypt'96 LNCS 1070, pp 1-9, Springer Verlag 1996.

[5] Cramer R. and Shoup V. A practical public key cryptosystem provably secure against chosen ciphertext attack. Crypto'98 LNCS 1462,pp. 13-25, Springer Verlag 1998.

[6] David Pointcheval, New public key cryptosystem based on the dependent-RSA problem. Eurocrypt'99 LNCS , 1592, pp.239-254, 1999. Springer Verlag Berlin Hoidelberg 1999.

[7] Don Boneh ,Twenty year attack on RSA cryptosystem. Notice of American Mathematical Society 203-213, 1999.

[8] Dolev D., Dwork C. and Naor M., Non-malleable cryptography.Proc. Of the 23rd STOC . ACM Press 1991.

[9] Diffie Whitfield and Hellmann Martin , New direction in cryptography. IEEE Transaction on Information Theory, v.22, 1976, 644-654.

[10] ElGamal T., A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transaction on Information Theroy C.IT-31, No. 4, pp469-472, July 1985.

[11] Goldwasser S. and Micali M., Probabilistic encryption. Journal of Computer and System Sciences . v.28 pp 270-299, 1984.

[12] Husemaller D. , Elliptic curves, Springer Verlag . 1987.

[13] Hasted J. Solving simultaneous modular equations of low degree. SIAM Journal of Computing v.17,pp336-341. 1988.

[14] Koyama K., Fast RSA -type schemes based on singular cubic curves $y^2 + axy = x^3 mod\ n$. Proceeding in LNCS EUROCYPT '95,Volume - 921 , PP. 329-340. Springer Verlag .

[15] Koyama K. and H. Kuwakado, A new RSA-type scheme based on singular cubic curves $(y - \alpha x)(y - \beta x) \equiv x^3 (mod n)$. IEICE Trans. Fund. E79-A (1996) 49-53.

[16] Kuwakado H., K. Koyama, Y. Tsuruoka, A new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 (mod n)$, IEICE Trans. Fund. E78-A (1995) 27-33.

[17] Menezes A., Elliptic curve public key cryptosystem , Kluwer Acadamic Publisher 1993.

[18] Okamoto T.and Uchiyama S,A new public key cryptosystem as secure as factoring. Eurocrypt'98,1403pp.308-318.Springer Verlag.

[19] Rivest R.L., Shamir A. , Adlemann L. ,A method for obtaining digital signatures and public key cryptosystem , Communication of the ACM 1,2 pp120-126 , (1978).

[20] Silverman J.H. , The arithmetic of elliptic curve , Graduate text in mathematics vol.106 . Springer Berlin 1986.

[21] Seng Kiat Chua, Ka Hin Leung, San Ling, Attack on RSA-type cryptosystem based on singular cubic curves over $Z/nZ*$. Theoretical Computer Science, v.220 19-27.1999.

[22] Tsiounis Y. and Yung M., on the security of ElGamal based encryption. PKC'98 LNCS Springer Verlag 1998.