A Fast Semantically Secure Public Key Cryptosystem Based on Factoring

Sahdeo Padhye and Birendra Kumar Sharma
(Corresponding author: Sahdeo Padhye)

School of Studies in Mathematics, Pt. Ravishankar Shukla University
Paipur (C.G.), India (Email: sahadeo_mathrsu@yahoo.com & sharmabk_nib@sancharnet.in)

(Received Aug. 21, 2005; revised and accepted Oct. 1, 2005)

Abstract

The cryptosystem proposed by Koyama is not semantically secure. Also, it is not secure against partial known plaintext attack, linearly related plaintext attack and low exponent attack. In this paper we propose a cryptosystem over singular cubic curve using the idea of Koyama and Kouichi et al. Our proposed cryptosystem is approximately two times faster than the cryptosystem given by Kouichi et al. with the same security label and more efficient than the Koyama scheme at higher security label. 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.

Keywords: Public key cryptosystem, RSA, semantic security, singular cubic curve

1 Introduction

The efficiency and security are two important demands of any cryptosystem. The details about different type of security notions we refer the reader to the paper by Bellare et al. [1]. In 1984, Goldwasser and Micalli [10] introduced a security notion, named semantic security. This means that the ciphertext should not leave any useful information about the plaintext. Adopting the condition of semantic security, ElGamal [9] proposed an encryption scheme based on the Diffie-Hellman [7] problem. However, such semantic security was related to the Decisional Deffie-Hellmann problem [7, 24] and couldn't gain popularity because of the computational load. On the other hand, the standard RSA [22] was not semantically secure. Later, in 1994, Bellare and Rogaway [2] presented some variants of RSA, which were semantically secure against chosen ciphertext attack in the random oracle model [2]. The cryptosystems given by Pointcheval [21] and S-Paillier [5] are also semantically secure. The scheme given by Pointcheval is 6 times faster than the ElGamal encryption scheme. In the Pointcheval scheme, small exponent e cannot be used for the security point of view because of the related message attack. Later, Kouichi et al. [14] generalized the scheme given by Pointcheval and S-Paillier cryptosystem. It is known as G-RSA cryptosystem at present. In this scheme, a small exponent e can be used. This scheme was more efficient than the scheme given by Pointcheval.

The singular cubic curve is an important object in number theory because of its wide range of applications. The quality of singular cubic curve is that it forms an abelian group over finite field. This attracted cryptographers to propose the analogue of some existing public key cryptosystems. The singular cubic curve was first time used by Koyama [15] and Koyama et al. [13, 17] for the construction of RSA type cryptosystem. However, the cryptosystem proposed by Koyama is two times faster than that of the standard RSA [22] scheme. But the scheme is not semantically secure and also not secure against low exponent attack [16], related message attack [6, 19] and partially known plaintext attack [3, 20]. It is therefore natural to curb said above three security weakness within Koyama schemes [13, 15, 17]. With this purpose we use "one way function" of Kouichi et al. [14] to redesign the Koyama scheme and construct a more secure cryptosystem. This new design is not only semantically secure but also prevents said three attacks.

The object of this paper is to propose a variant of RSA scheme based on singular cubic curve applying the ”one way function” used in Kouichi et al. [14] scheme. In our opinion, apart from semantic security it rules out the possibility of said three attacks. Our scheme is approximately 2 times faster than Kouichi et al. [14] scheme and more secure than Koyama scheme [15].

2 Singulaer 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:

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

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 over F_p.

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

A nonsingular 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 $\bigcirc$.

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 [18, 23]. For any point $P \in C_p(a, b)$. For the sum $P \oplus \bigcirc$, by definition, is equal to P, which is also equal to $\bigcirc \oplus P$. For $P = (x_0, y_0)$, we define $\ominus P$ the additive inverse of P as the point $(x_0, -y_0 - ax_0)$. The sum of $P \oplus (\ominus P)$ 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 $P_1 \oplus P_2 = (x_3, y_3)$ is calculated as follows:

$$\begin{aligned} x_3 &= \gamma^2 + a\gamma - b - x_1 - x_2 \\ y_3 &= \gamma(x_1 - x_3) - y_1, \end{aligned} \tag{2}$$

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

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

An isomorphism between $C_p(a, b)$ and ${F_p}^\star$ is defined in [18] 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 $a = -\alpha - \beta \bmod p$ and $b = -\alpha\beta \bmod p$. 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 theorems:

Theorem 1 *[18] The mapping* $\omega : C_p(a, 0) \to {F_p}^\star$ *defined by* $\omega : \bigcirc \to 1$ *and* $(x, y) \to 1 + \frac{ax}{y} = \frac{x^3}{y^2}$ *is a group isomorphism. The group isomorphism mapping* $\omega^{-1} : {F_p}^\star \to C_p(a, 0)$ *is defined by* $\omega^{-1} : 1 \to \bigcirc$ *and* $v \to (\frac{a^2 v}{(v-1)^2}, \frac{a^3 v}{(v-1)^3})$.

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

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

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 $(0, 0) \bmod p$ or congruent to $(0, 0) \bmod q$, 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 *[12] 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*

$$\begin{aligned} 1 + \frac{ax_i}{y_i} &= (1 + \frac{ax_1}{y_1})^i (\text{mod} n), \quad \textit{i.e.} \\ \frac{x_i}{y_i} &= (\frac{x_1}{y_1})^i (\text{mod} n) \end{aligned} \tag{4}$$

3 RSA Type Schemes Based on Singular Cubic Curves

Three RSA type schemes based on singular cubic curve over Z_n are proposed as follows.

3.1 Scheme I [17]

This cryptosystem is based on the singular cubic curve of the form:

$$C_n(0, b) := y^2 \equiv x^3 + bx^2 (\text{mod} n), \tag{5}$$

where $n = pq$ is the product of two large primes. The encryption key e is chosen such that $(e, N) = 1$ where $N = lcm(p - 1, p + 1, q - 1, q + 1)$.The decryption key d is chosen such that $ed \equiv 1 \bmod N$. The public key is the pair (n, e) and the private keys are d, p and q. To encrypt a plaintext pair $M = (m_x, m_y)$, the sender first computes $b = \frac{{m_y}^2 - {m_x}^3}{{m_x}^2} (\text{mod} n)$ and then the ciphertext is computed as $C = e \otimes M$ on the singular cubic curve $C_n(0, b)$. The complete ciphertext is (C, b). The Receiver, who knows the decryption key d can get the plaintext (m_x, m_y) by computing $d \otimes (c_x, c_y) = (m_x, m_y)$ over the singular cubic curve $C_n(0, b)$.

3.2 Scheme II [15]

This cryptosystem is based on the singular cubic curve of the form:

$$C_n(a, 0) := y^2 + axy \equiv x^3 (\text{mod} n), \tag{6}$$

where $n = pq$ is the product of two large primes. The encryption key e is chosen such that $(e, N) = 1$ where

$N = lcm(p-1, q-1)$.The decryption key d is chosen such that $ed \equiv 1 \bmod N$. The public key is the pair (n, e) and the private keys are d, p and q. To encrypt a plaintext pair $M = (m_x, m_y)$, the sender first computes $a = \frac{{m_x}^3 - {m_y}^2}{m_x m_y}(\bmod n)$and then the ciphertext is computed as $C = e \otimes M$ on the singular cubic curve $C_n(a, 0)$.The complete ciphertext is (C, a). The Receiver, who knows the decryption key d can get the plaintext (m_x, m_y) by computing $d \otimes (c_x, c_y) = (m_x, m_y)$ over the singular cubic curve $C_n(a, 0)$.

3.3 Scheme III [13]

This cryptosystem is based on the singular cubic curve of the form:

$$C_n(\alpha, \beta) := (y - \alpha x)(y - \beta x) \equiv x^3 (\bmod n), \qquad (7)$$

where $n = pq$ is the product of two large primes. The encryption key e is chosen such that $(e, N) = 1$ where $N = lcm(p-1, q-1)$.The decryption key d is chosen such that $ed \equiv 1 \bmod N$. The public key is the pair (n, e) and the private keys are d, p and q. To encrypt a plaintext pair $M = (m_x, m_y)$, the sender first chooses α randomly and computes $\beta = \frac{{m_x}^3 - {m_y}^2 + \alpha m_x m_y}{m_x(a m_x - m_y)}(\bmod n)$.Then the ciphertext is computed as $C = e \otimes M$ on the singular cubic curve $C_n(\alpha, \beta)$.The complete ciphertext is (C, α, β). The Receiver, who knows the decryption key d can get the plaintext (m_x, m_y) by computing $d \otimes (c_x, c_y) = (m_x, m_y)$ over the singular cubic curve $C_n(\alpha, \beta)$.

Seng et al. [6] have given following two equivalence relations for the schemes I, II and III mentioned above.

Reduction of Scheme II to Scheme I: The transformation $(x, y) \rightarrow (x, y + \frac{a}{2}x)$ will transform the curve $C_n(a, 0)$ to the curve $C_n(0, b)$ with $b = 4a^2$. Using this transformation one can reduce Scheme II to Scheme I.

Reduction of Scheme III to Scheme I: The transformation $(x, y) \rightarrow (x, y - \frac{\alpha - \beta}{2}x)$ will transform the curve $C_n(\alpha, \beta)$ to the curve $C_n(0, b)$ with $b = (\frac{\alpha - \beta}{2})^2$. Using this transformation, one can reduce Scheme III to Scheme I.

4 G-RSA Cryptosystem

Kouichi et al. generalized the S-Paillier [5] and D-RSA [21] cryptosystem which enhanced the RSA cryptosystem to be semantically secure using one way function f, where f is a function $Z_n \rightarrow Z_n$. This is known as G-RSA cryptosystem. In this cryptosystem, A message m is encrypted by $(c_0 = r^e (\bmod n)$, $c_1 = f(r) + m c_0 (\bmod n))$, where r is randomly chosen element of ${Z_n}^*$. The ciphertext is decrypted by computing $r = {c_0}^d (\bmod n)$ first and then plaintext is obtained by computing $m = ((c_1 - f(r)){c_0}^{-1})(\bmod n)$.

Let OW be a class of one way function $f : Z_n \rightarrow Z_n$. The one way-ness assumption of G-RSA cryptosystem is that, for any probabilistic polynomial time algorithm A^{OW}_{G-RSA}, the probability

$$\begin{aligned} &\Pr{}_{r \in_R Z_n}[(n, e) \leftarrow RSA_{Public}, f \leftarrow OW,\ r \leftarrow_R Z_n^*, \\ &c_0 = r^e \bmod n, \\ &c_1 = f(r) + m c_0 \bmod n : A^{OW}_{G-RSA}(c_0, c_1) = 1] \end{aligned}$$

is negligible in *log n*.

A semantic security adversary A^{SS}_{G-RSA} against the G-RSA cryptosystem consists of the find stage $A^{SS_1}_{G-RSA}$and the guess stage $A^{SS_2}_{G-RSA}$. The semantic security of G-RSA cryptosystem is that, for any probabilistic polynomial time algorithm A^{SS}_{G-RSA} the probability

$$\begin{aligned} &2\Pr[(n, e) \leftarrow RSA_{public}, f \leftarrow OW, \\ &(m_0, m_1, st) \leftarrow A^{SS_1}_{G-RSA}(e, n), b \leftarrow \{0, 1\}, \\ &r \leftarrow_R Z_n^*,\ c_0 = r^e \bmod n, c_1 = f(r) + m_b c_0 \bmod n\,; \\ &A^{SS_2}_{G-RSA}((c_0, c_1), m_0, m_1, st) = b] - 1 \end{aligned}$$

is negligible in *logn*.

Kouichi et al. defined two problems called C-RSA+OW problem and D-RSA+OW problem, in order to investigate the security of G-RSA cryptosystem based on a one way function $f : Z_n \rightarrow Z_n$. The computational $C - RSA + OW$ problem is to compute the value $f(r)$ for given RSA public key (e, n) and the random ciphertext $c_0 = r^e (\bmod n)$.

4.1 C-RSA+OW Assumption

For any probabilistic polynomial time algorithm $A_{C-RSA+OW}$, the probability

$$\begin{aligned} &\Pr{}_{r \in_R Z_n^*}[\ (n, e) \leftarrow RSA_{public},\ f \leftarrow OW, c = r^e \bmod n; \\ &A_{C-RSA+OW}(c) = f(r)\ ] \end{aligned}$$

is negligible in *log n*.

The decisional version of $C - RSA + OW$ problem is to distinguish whether an element $(x, y) \in Z_n \times Z_n$ comes from the distribution $(r^e mod\ n, f(r))$ for $r \in {Z_n}^*$.

4.2 D-RSA+OW Assumption

For any probabilistic polynomial time algorithm $A_{D-RSA+OW}$, the probability of distinguishing the two distribution

$$\begin{aligned} &|\Pr[\,(x, y) \leftarrow Z_n \times Z_n : A_{D-RSA+OW}(x, y) = 1] - \\ &\Pr[\,r \leftarrow Z_n^*,\ x = r^e \bmod n, \\ &\quad f \leftarrow OW, y = f(r) : A_{D-RSA+OW}(x, y) = 1]| \end{aligned}$$

is negligible in *log n*.

Following two theorems proves the one way-ness and semantic security of G-RSA cryptosystem.

Theorem 3 *The encryption function of G-RSA cryptosystem is one-way if and only if the C-RSA+OW assumption holds.*

Theorem 4 *The G-RSA cryptosystem is semantically secure if and only if the D-RSA+OW assumption holds.*

Kouchi et al. proposed a novel one way function, most significant bits zeroes ($MSBZ$) function. Let r be a k-bit random integer in ${Z_n}^*$. The binary representation of r is $r = r_0 2^0 + r_1 2^1 + r_2 2^2 + . + r_l 2^l + r_{l+1} 2^{l+1} + ... + r_{k-1} 2^{k-1}$. The proposed one way function was $f^{e,n}_{MSBZ}(r) = (r - MSBZ_{(l)}(r))^e \underline{m}od\ n$ where l is large enough. Here, $r - MSBZ_l(r)$ denotes the l most significant bits of r equal to zero, i.e. $r - MSBZ_l(r) = r_0 2^0 + r_1 2^1 + r_2 2^2 + . + r_l 2^l$. This one way function was named after most significant bits zeroes function ($MSBZ$).

The equivalence between RSA and G-RSA cryptosystem was based on the following theorems.

Theorem 5 *The C-RSA+MSBZ assumptions holds iff RSA assumption holds.*

Theorem 6 *Let $(n, e) \in RSA_{public}$ and $c = r^e(\text{mod} n)$ be the input of the computational $RSA+MSBZ$ problem. An adversary, who breaks the $D-RSA+MSBZ$ problem, can computes the least significant bit of r. If the least significant bits of r are zero, the next bit after the zeroes can be computed by the adversary.*

5 Proposed Cryptosystem

Now we propose a new semantically secure encryption scheme over the singular cubic curve $C_n(a, 0)$ with the massage dependent variable a similar to that of Koyama scheme [15]. The security of the proposed scheme is based on the 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 $m_x, m_y \in {Z_n}^*$ and ${m_x}^3 \neq {m_y}^2(\text{mod} n)$. We first transform the plaintext (m_x, m_y) to ${Z_n}^*$, and then encrypt the isomorphic image of (m_x, m_y), i.e. $\frac{{m_x}^3}{{m_y}^2}$.

5.1 Key Generation

To generate keys, receiver R chooses two large primes p,q and computes $n = pq$. Receiver determines an integer e less than and relatively prime to $\phi(n)$. He then computes 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 makes the keys (e, n) publicly available and keeps secret to the keys (d_p, d_q, p, q). Moreover a one way function $f : {Z_n}^* \rightarrow {Z_n}^*$ is used as a system parameter.

5.2 Encryption

To encrypt the message pair (m_x, m_y), sender S, first chooses a random integer $r \in {Z_n}^*$ and sends the ciphertext (c_0, c_1, c) to the receiver R with the receiver's public key (e, n). Where

1) $c_0 = r^e mod\ n$.

2) $c_1 = f(r) + (\frac{{m_x}^3}{{m_y}^2})c_0 mod\ n$.

3) $a = \frac{{m_x}^3 - {m_y}^2}{m_x m_y} mod\ n$.

4) $c = (a + r^2) mod\ n$.

The complete ciphertext is (c_0, c_1, c). It is clear that the ciphertext does not belongs to any corresponding point on the singular cubic curve $C_n(a, 0)$. Also the ciphertext c does not leak any information about the plaintext.

5.3 Decryption

The receiver R computes the original plaintext by using his/her secrete keys after getting the ciphertext (c_0, c_1, c) as below:

1) $r_p = {c_0}^{d_p} mod\ p$ and $r_q = {c_0}^{d_q} mod\ q$. By the pair (r_p, r_q) and via Chinese Remainder theorem, compute the value of r.

2) $a = (c - r^2) mod\ n$.

3) $m = \frac{{m_x}^3}{{m_y}^2} mod\ n = (c_1 - f(r))c_0^{-1} mod\ n$. Now by using the isomorphism mapping for singular cubic curve defined above he/she then computes the original plaintext (m_x, m_y) by $m_x = \frac{a^2 m}{(m-1)^2} mod\ n$ and $m_y = \frac{a^3 m}{(m-1)^3} mod\ n$.

Example: Following is a very simple example to understand our proposed cryptosystem:

Let $p = 5$ and $q = 11$, $n = 55$, $\phi(n) = 40$, then $Z^\star_n =$ 1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 17, 18, 19, 21, 23, 24, 26, 27, 28, 29, 31, 32, 34, 36, 37, 38, 39, 41, 42, 43, 46, 47, 48, 49, 51, 52, 53, 54.

Key Generation: Let $e = 3$, $d_p \equiv \frac{1}{3}(\text{mod} 4) \equiv 3$, $d_q \equiv \frac{1}{3}(\text{mod} 10) \equiv 7$.

Let the Plaintext pair = (2, 3), i.e. $m_x = 2$ and $m_y = 3$

Encryption: To encrypt the message pair (2, 3), the sender chooses the parameter $r = 7$, he then proceeds as follows:

1) $c_0 = 7^3 mod\ 55 \equiv 13$.

2) $c_1 = f(7) + (\frac{2^3}{3^2}) \times 13 mod\ 55 \equiv f(7) + 7 \times 13 \equiv f(7) + 36$.

3) $a = \frac{2^3 - 3^2}{6} mod\ 55 \equiv 9$.

4) $c = (9 + 7^2) mod\ 55 \equiv 3$.

Sender sends the complete ciphertext $(13, f(r) + 36, 3)$ to the receiver R.

Decryption: To get the plaintext after having the ciphertext, R proceeds as follows:

1) $r_p = 13^3 mod\ 55 \equiv 2$ and $r_q = 13^7 mod\ 11 \equiv 7$. By the pair (r_p, r_q) and via Chinese Remainder theorem, R computes the value of $r = 7$.

2) $a = (3 - 7^2) mod\ 55 \equiv 3 - 49 \equiv 9$.

3) $m = \frac{{m_x}^3}{{m_y}^2} mod\ n \equiv (f(7) + 36 - f(7))13^{-1} mod\ n \equiv \frac{36}{13} mod\ 55 \equiv 7$. He/she then computes the original plaintext (m_x, m_y) by $m_x = \frac{9^2 \times 7}{(7-1)^2} mod\ 55 \equiv 2$ and $m_y = \frac{9^3 \times 7}{(7-1)^3} mod\ 55 \equiv 3$.

6 Efficiency and Security

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 $(r^e \bmod n, f(r) \bmod n, r^e \bmod n)$ are computed well in advance. Because of this pre-computation, the encryption process requires only two multiplications and one addition modulo n. This feature makes the encryption process more efficient than the scheme given by Koyama, although, our decryption process remains approximately as efficient as the scheme given by Koyama.Following the analysis given by Koyama [15], let, x and y the coordinates of $2 \log\ n$-bit plaintext are transformed to a $\log n$-bit plaintext by isomorphic mapping. This massage of $\log n$ bit length is than encrypted by using encryption process. The obtained ciphertext is decrypted by using decryption key over ${Z_n}^*$ which is the transformed massage. By using the inverse transformation, we get the original $2 \log n$ bit length massage. If we exclude the transformation than the number of modulo multiplication is approximately same as for the G-RSA scheme in decryption process. Hence, the decryption speed of the proposed scheme is 2 times faster than that of G-RSA scheme for a K bit long message if $\lceil \frac{K}{log\ n} \rceil$ is even.

An intuitive argument that cryptosystem proposed is semantically secure against chosen plaintext attack in the Decisional GRSA problem is as follows. In order to determine any information about the plaintext m from the ciphertext, attacker need to have some information about $f(r) \bmod n$ where r is randomly chosen element in Z_n^*. The only way to ascertain any information about the value of $f(r)(\bmod n)$ is to first compute r (it is not sufficient to compute some partial information about r; it is necessary to have complete information about r in order to obtain any information about $f(r)(\text{mod} n)$, as r is randomly chosen). It is not possible without knowing the secret key d or solving the GRSA 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 neither use Theorem 1 nor the addition operation over the exact singular cubic curve. Next, following Theorems 3 and 4 the proposed scheme is semantically secure against the chosen ciphertext attack.

We have mentioned that the schemes proposed by Koyama [15] and Koyama et al. [13, 17] are not secure against partially known plaintext attack [3, 20] linearly related message attack [6] and low exponent attack [3, 16]. Also, all three schemes [13, 15, 17] are equivalent to each other [6] and the transformation $(x, y) \to (x, y + \frac{a}{2}x)$ with $b = a^2 4$, transforms the curve $C_n(a, 0)$ to the curve $C_n(0, b)$. Using this transformation one can reduce the scheme [15] to the scheme [17]. Here, we consider the scheme [17] over the curve $C_n(0, b)$ to compare with our scheme for the security analysis and show that the said above attacks not admissible in our proposed scheme as below.

Secure Against Partially Known Plaintext Attack. In the Koyama scheme, knowing one ordinate m_x or m_y in a plaintext pair (m_x, m_y) one can compute the whole plaintext under with the help of corresponding ciphertext. In brief, this attack is as below:

Let n, e be a public key for scheme [17] and $C = (c_x, c_y)$ be the encryption of the plaintext $M = (m_x, m_y)$, i.e. $e \otimes (m_x, m_y) = (c_x, c_y)$. Assume that m_x is known and m_y is unknown. Let $m_y = y$. Then we compute $e \otimes M$ over $Z[y]/(y^2 - {m_x}^3 - bm_x, n)$by using the addition law of singular cubic curve. For the Koyama scheme, by induction technique, it can be shown that for any k in Z_n, $k \otimes (m_x, y) \equiv (u_k, v_k y)$ where u_k and v_k are two positive integers. Finally, for $k = e$, we get the relation $(u_e, v_e y) = (c_x, c_y)$, which can be solved for $y = c_y {v_e}^{-1}(\text{mod} n)$ if $v_e \neq 0(\text{mod} n)$. However, if $v_e = 0(\text{mod} n)$ then the ciphertext C is a point of order 2 in $C_n(0, b)$ which means that $d \otimes C = M$, i.e. $C = M$, hence M is always computable.

In our scheme we hide the parameter a and the ciphertext is not a permutation of the plaintext pair (m_x, m_y) on the same curve. Also, with the help of ciphertext, none but the receiver can compute the addition parameter a. And hence he cannot use the addition operation. So, the attacker neither can use the said above transformation nor Theorem 1. Thus we conclude that the partially known plaintext attack is not admissible in our scheme.

Secure Against Linearly Related Plaintext Attack. We have mentioned that the Koyama schemes [13, 15, 17] become insecure if two linearly related plaintexts are encrypted with the same public key [3, 6, 19]. In brief, the attack is as below.

Let $M = (m_x, m_y)$ and $M' = (m'_x, m'_y)$ be two plaintexts linearly related by the known relations:

$$\begin{aligned} m'_x &\equiv \alpha m_x + \gamma \\ m'_y &\equiv \beta m_x + \delta, \end{aligned}$$

where α, γ, β and δ are integers in ${Z_n}^*$. Assume that the encryption of the plaintexts (m_x, m_y) and (m'_x, m'_y) are given by

$$\begin{aligned} (c_x, c_y) &\equiv e \times (m_x, m_y)(\text{mod} n) \\ (c'_x, c'_y) &\equiv e \times (m'_x, m'_y)(\text{mod} n). \end{aligned}$$

From the above ciphertext we can derive the curves $C_n(0, b)$ and $C_n(0, b')$ upon which the point must lie.

Thus we have

$$\begin{aligned} m_x^3 + bm_x^2 - m_y^2 &\equiv 0(\text{mod}n) \\ (\alpha m_x + \gamma)^3 + b'(\alpha m_x + \gamma)^2 - (\beta m_y + \delta)^2 &\equiv 0(\text{mod}n). \end{aligned}$$

By above two equations we can write my as a polynomial w in m_x with

$$w(x) = \frac{(\alpha x + \gamma)^3 + b'(\alpha x + \gamma)^2 - \beta^2(x^3 + bx^2)}{2\beta\delta}.$$

By using the addition formula on singular cubic curve, it is clear that $w(m_x) \equiv m_y(\text{mod}n)$. Now let $f(x) \equiv x^3 + bx^2 - w(x)^2(\text{mod}n)$, which is a polynomial of degree 6. Thus $f(mx) \equiv 0(\text{mod}n)$ on $Z[x]/(n, f(x))$. Next we compute $e \times (x, w(x)) \equiv (h(x), j(x))(\text{mod}n)$ over $Z[x]/(n, f(x))$. Then we have the following equations:

$$\begin{aligned} h(m_x) &\equiv c_x(\text{mod}n) \\ j(m_x) &\equiv c_y(\text{mod}n). \end{aligned}$$

Finally, we compute $gcd(h(x) - cx, f(x))$ which is a linear polynomial of the form $k(x - m_x)$. This gives us the plaintext m_x. After knowing the half of the plaintext $(m_x, m_y) = M$, we can compute the other half m_y by $w(m_x) = m_y$. Again by the linear relation between M and M' we can compute the plaintext M'.

Again to apply such type of attack, the knowledge of parameter b (or a) is necessary. In the proposed scheme, we hide the parameter a, so that no one can apply above attack in our scheme. It is therefore, secure against linearly related plaintext attack.

Finally, as the GRSA scheme [14] is secure against low exponent attack, we assert that the proposed scheme is also secure against low exponent attack.

Acknowledgements

This work is support under CSIR, JRF (INDIA) 2002 scheme.

References

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

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

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

[4] D. Boneh, "Twenty-year attack on RSA cryptosystem," *Notice of American Mathematical Society*, vol. 46, no. 2, pp. 203-213, 1999.

[5] D. Catalano, R. Gennaro, N. Howgraw-Crahan, and P. Nguyen, "Paillier's cryptosystem revisited," in *ACM Conference on Computer and Communication Security*, pp. 206-214, 2001.

[6] S. K. Chua, K. H. Leung, S. Ling, "Attack on RSA-type cryptosystem based on singular cubic curves over Z/nZ^*," *Theoretical Computer Science*, vol. 220, pp. 19-27, 1999.

[7] W. Diffie and M. Hellmann, "New direction in cryptography," *IEEE Transaction on Information Theory*, vol. 22, pp. 644-654, 1976.

[8] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography,", in *Proceedings of the 23rd STO*, ACM Press, pp. 542-552, 1991.

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transaction on Information Theroy*, vol. 31, no. 4, pp. 469-472, 1985.

[10] S. Goldwasser and M. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, pp 270-299, 1984.

[11] J. Hasted, "Solving simultaneous modular equations of low degree," *SIAM Journal of Computing*, vol. 17, pp. 336-341, 1988.

[12] D. Husemaller, "Elliptic curves," *Graduate Text in Mathematics*, Springer Verlag, 1987.

[13] K. Koyama and H. Kuwakado, "A new RSA-type scheme based on singular cubic curves $(y - ax)(y - bx) \equiv x^3(modn)$," *IEICE Transactions on Fundamental*, vol. E79-A, pp. 49-53, 1996.

[14] S. Kouichi and T. Takagi, "New semantically secure public key crytosystems from RSA-Primitive," in *PKC'2002*, LNCS 2274, pp. 1-16, 2002.

[15] K. Koyama, "Fast RSA -type schemes based on singular cubic curves $y^2 + axy = x^3 mod\ n$," in *EUROCYPT'95*, LNCS 921, pp. 329-340, Springer Verlag, 1995.

[16] K. Kurosawa, K. Kada, S. Tsuji, "Low exponent attack against elliptic curve RSA," *Information Processing Letters*, vol. 53, pp. 77-83, 1995.

[17] H. Kuwakado, K. Koyama, Y. Tsuruoka, "A new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2(\bmod n)$," *IEICE Transactions on Fundamental*, vol. E78-A, pp. 27-33, 1995.

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

[19] S. Padhye, *On Security of Koyama Scheme*, Eprint Archive-2005/153, http://eprint.iacr.org/2005/153.pdf.

[20] S. Padhye, "Partial known plaintext attack on Koyama scheme," *Information Processing Letters*, vol. 96, no. 3, pp. 96-100, 2005.

[21] D. Pointcheval, "New public key cryptosystem based on the dependent-RSA problem," in em Eurocrypt'99, LNCS 1592, pp. 239-254, 1999.

[22] R. L. Rivest, A. Shamir, L. Adlemann, "A method for obtaining digital signatures and public key cryptosystem," *Communication of the ACM*, vol. 1, no. 2, pp120-126, 1978.

[23] J. H. Silverman, "The arithmetic of elliptic curve," *Graduate Text in Mathematics*, vol. 106, Springer Berlin, 1986.

[24] Y. Tsiounis and M. Yung, "On the security of ElGamal based encryption," in *PKC'98*, LNCS 1431, pp. 117-134, Springer Verlag, 1998.

Sahadeo Padhye received the B.Sc. and M.Sc. degree in Mathematics form Pt. Ravishankar Shukla University, Raipur. Chhattisgarh, India in 1999 and 2001. Council of Scientific and Industrial Research (CSIR), India has granted him Junior Research Fellowship (2002-2004). He then joined School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, India for his research work. He is a life member of Cryptology Research Society of India (CRSI). His area of interest is Public Key Cryptography based on elliptic curve.

Birendra Kumar Sharma Prof. & Head, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur, (C. G.) India has been working in the field of Non Linear Operator Theory for a long time. !5 scholars have got their Ph.D. degree under his guidance in the field of fixed point theory. Since last three years he moved to work in the applied field such as Cryptography. He is a life member of Indian Mathematical society and the Ramanujan Mathematical Society.