ON SECURITY OF KOYAMA SCHEME

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

Communicated by: B. K. Sharma.

Abstract.

An attack is possible upon all three RSA analogue PKCs based on singular cubic curves given by Koyama. While saying so, Seng et al observed that the scheme become insecure if a linear relation is known between two plaintexts. In this case, attacker has to compute greatest common divisor of two polynomials corresponding to those two plaintexts. However, the computation of greatest common divisor of two polynomials is not efficient. For the reason, the degree e of both polynomials, an encryption exponent, is quite large. In this paper, we propose an algorithm, which makes the attack considerably efficient. Subsequently, we identify isomorphic attack on the Koyama schemes by using the isomorphism between two singular cubic curves.

Key Words :Public Key Cryptosystem, Singular Cubic Curve, Koyama scheme, RSA.
2000 Mathematics Subject Classification. 94A60, 11T17.

1. **Introduction.**

Koyama et al [3, 5, 7]first time constructed RSA type public key cryptosystems based on singular cubic curve where security based on factoring problem. 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 [10] have shown that all three schemes are equivalent to each other by an isomorphism mapping and become insecure if a linear relation is known between two plaintexts. For this attack, attacker has to compute the greatest common divisor (GCD) of two polynomials both of degree e, where e is the encryption exponent. This attack was found less efficient because of its slow speed. Now in this paper, we propose a different algorithm of the same attack, which makes it more efficient than that of the Seng et al. In our attack, the attacker has to compute the GCD of two polynomials of degree six and of degree e. Next, in

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

this article, we identify isomorphic attack. From this, an attacker can forge signature of receiver B without knowing B's secret key. For this attack, a singular cubic curve is needed, isomorphic to the curve corresponding to the plaintext. Historically it was searched by Koyama for the KOMV scheme which was based on nonsingular elliptic curve [6].

2. **Singulaer Cubic Curve.**

Consider the congruence equation

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

$a, b \in Z_p$.

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

Let F_p be a finite field with p elements and $F_p{}^{\star}$ 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 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 [8, 9]. 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 [8, 2]. For any $k \in F_p$ the multiplication operation $\otimes$ is defined as bellow :

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

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 and consider the congruence equation

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

The 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 $(0, 0)$*modulo* q, but including a point at infinity $\bigcirc$. By Chinese Remainder Theorem, $C_n(a, b)$ is isomorphic as a group to $C_p(a, b) \times C_q(a, b)$.

3. **RSA Type Schemes Based on Singular Cubic Curves**

Three RSA type schemes based on singular cubic curve over Zn are proposed as below:

3.1. **Scheme I** [7]**.** This cryptosystem is based on the singular cubic curve of the form

$$C_n(0,b) := y^2 \equiv x^3 + bx^2 (mod\ n) \tag{4}$$

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 $ed \equiv 1 mod\ N$. 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 $b = \frac{m_y^2 - m_x^3}{m_x^2} (\bmod n)$ and then the ciphertext is computed as $C = e \times M$ 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 $d \times (c_x, c_y) = (m_x, m_y)$ over the singular cubic curve $C_n(0, b)$.

3.2. **Scheme II** [3]**.** This cryptosystem is based on the singular cubic curve of the form

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

where $n = pq$ is the product of two large primes. The encryption key e is chosen such that $(e, N) = 1$ where $N = lcm(p-1, q-1)$. The decryption key d is chosen such that $ed \equiv 1 mod\ N$. 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 $C = e \times M$ 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 $d \times (c_x, c_y) = (m_x, m_y)$ over the singular cubic curve $C_n(a, 0)$.

3.3. **Scheme III** [5]**.** This cryptosystem is based on the singular cubic curve of the form

$$C_n(a,b) := (y - \alpha x)(y - \beta x) \equiv x^3 (mod\ n) \tag{6}$$

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 $ed \equiv 1 mod\ N$. The public key is the pair (n, e) and the private keys are d, p and q. To encrypt a plaintext pair $M = (m_x, m_y)$, sender first chooses a randomly and computes . Then the ciphertext is computed as $C = e \times M$ 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 $d \times (c_x, c_y) = (m_x, m_y)$ over the singular cubic curve $C_n(\alpha, \beta)$.

Seng et al [10] have given following two equivalence relation between scheme I, II and III.

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 $b = a^2 4$. 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 the Scheme I.

4. **An Efficient Algorithm For Linearly Related Plaintext Attack.**

In this section, we discuss the situation when two linearly related messages are both encrypted with the same public key. This situation was first time discussed by Coppersmith et al [1] for the RSA scheme and then by Seng et al. [10] for the singular cubic curve based RSA. Now we analyze said situation for singular cubic curve based RSA and propose a more efficient algorithm for the attack then those of Seng et al. In section 3 we have already seen that the scheme II and scheme III are reducible to the scheme I. So, let us consider the scheme I to discuss our attack. Let $M = (m_x, m_y)$ and $M' = (m'_x, m'_y)$ be two plaintexts linearly related by the known relations

$$m'_x \equiv \alpha m_x + \gamma \tag{7}$$

$$m'_y \equiv \beta m_x + \delta \tag{8}$$

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

$$(c_x, c_y) \equiv e \times (m_x, m_y)(mod\ n) \tag{9}$$

$$(c'_x, c'_y) \equiv e \times (m'_x, m'_y)(mod\ n) \tag{10}$$

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

$$m_x^3 + bm_x^2 - m_y^2 \equiv 0 \pmod n$$
$$(\alpha m_x + \gamma)^3 + b'(\alpha m_x + \gamma)^2 - (\beta m_y + \delta)^2 \equiv 0 \pmod n$$

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

$$w(x) = \frac{(\alpha x + \gamma)^3 + b'(\alpha x + \gamma)^2 - \beta^2(x^3 + bx^2)}{2\beta\delta} \tag{11}$$

by equation (4) it is clear that $w(m_x) \equiv m_y(mod\ n)$. Now let $f(x) \equiv x^3 + bx^2 - w(x)^2(mod\ n)$, which is a polynomial of degree 6. From equation (4) we see that $f(mx) \equiv 0(mod\ n)$ on $Z[x]/(n, f(x))$. Next we compute $e \times (x, w(x)) \equiv (h(x), j(x))(mod\ n)$ over $Z[x]/(n, f(x))$. Then we have the following equations

$h(m_x) \equiv c_x(mod\ n)$

$j(m_x) \equiv c_y(mod\ n)$.

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. Knowing this half of the plaintext $(m_x, m_y) = M$, we can compute the other half m_y by $w(m_x) = m_y$. Finally because of the linear relation between M and M' we can compute the plaintext M'.

4.1. Comparison between Seng et al Algorithm (SA)and Proposed Algorithm(PA).

SA- Let two linearly related messages are (x, y) and $(x + \Delta, y + \Delta)$.

1. In SA, attacker has to compute first coordinate of $e \times (x, y)$ and $e \times (x + \Delta, y + \Delta)$ by using the division polynomial. Let it be c_{1x} and c_{2x}.

2. In SA, the attacker has to compute the gcd of two polynomials $G(x)$ and $H(x)$ both of degree e, where $G(x) = x^e - c_{1x}\phi e(x, .)modn$, and $H(x) = (x + \Delta, y + \Delta) - c_{2x}\phi e(x + \Delta, .)modn$.

3. SA depends on e, hence, for higher values of e attack is less applicable.

PA- Let two linearly related messages are $M = (m_x, m_y)$ and $M` = (m_x`, m_y`)$, where $m_x` = \alpha m_x + \gamma$ and $m_y` = \beta m_x + \delta$. 1. In PA, attacker has to compute first coordinates of $e \times (x, w(x))$ where

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

. Let $e \times (x, w(x)) = (h(x), J(x))$ and $f(x) \equiv x^3 + bx^2 - w(x)^2(mod\ n)$.

2. In PA, attacker has to compute the gcd of two polynomials $G(x) = h(x) - c_x$ and $f(x)$. Here, $G(x)$ is a polynomial of degree e and $f(x)$ is a polynomial of degree 6.

3. PA does not depend upon the encryption exponent; hence, it is applicable for each value of e.

4. In PA, since one polynomial is of degree 6 so we may assume that the computational efficiency is faster than SA.

5. Isomorphic Attack

TThe idea behind the proposed attack is based on the isomorphic property of two singular cubic curves. Such type of attack was first time identified by Koyama for the KMOV scheme [6]. We first give definition and the isomorphic property as follows.

Definition 5.1 Let $n = pq$ (p, q are primes), and $C_n(0, b_1)$ and $C_n(0, b_2)$ be singular cubic curves such that

$C_n(0, b_1) : y^2 = x^3 + b_1x^2(mod\ n)$, $C_n(0, b_2) : y^2 = x^3 + b_2x^2(mod\ n)$.

$C_n(0, b_1)$ and $C_n(0, b_2)$ are isomorphic if there exist $u_p \in Z_p^*$ and $u_q \in Z_q^*$ such that,

$b_2 \equiv u_p^2 b_1(mod\ p)$, and $b_2 \equiv u_q^2 b_1(mod\ q)$.

By using the property of singular elliptic curve over field and Chinese Remainder Theorem, the following isomorphic property of singular cubic curve over ring is shown [9]as bellow:

Let $C_n(0, b_1 1) : y^2 = x^3 + b_1 x^2 (mod\ n)$ and $C_n(0, b_2) : y^2 = x^3 + b_2 x^2 (mod\ n)$ be two singular cubic curves. Let $M_1 = (m_{1x}, m_{1y})$, $C_1 = (c_{1x}, c_{1y}) \in C_n(0, b_1)$ and $M_2 = (m_{2x}, m_{2y})$, $C_2 = (c_{2x}, c_{2y}) \in C_n(0, b_2)$, where $C_1 = e \times M_1$ over $C_n(0, b_1)$ and $C_2 = e \times M_2$ over $C_n(0, b_2)$. Then the following statements are equivalent,

1. $C_n(0, b_1)$ and $C_n(0, b_2)$ are isomorphic
2. $b_2 \equiv u^2 b_1 (mod\, n)$ for some $u \in Z_n^*$ (12)
3. $c_{2x} \equiv u^2 c_{1x} (mod\, n)$, $c_{2y} \equiv u^3 c_{2y} (mod\, n)$ for some $u \in Z_n^*$ (13)
4. $m_{2x} \equiv u^2 m_{1x} (mod\, n)$, $m_{2y} \equiv u^3 m_{2y} (mod\, n)$ for some $u \in Z_n^*$ (14)

If C_1, C_2 and M_1 satisfying the congruence (13) are given, then M_2 can be easily obtained by computing the congruence (14). It is not difficult to check whether or not congruence (13) holds.

Suppose, an attacker A wants to victimize B by forge signature on a plaintext $M = (m_x, m_y)$ without B's consent. For this, A generates another message M' with B's public key n_B and random integer u:

$M' = (u^2 m_x (mod\ n_B), u^3 m_y (mod\ n_B))$,

And sends M' to B. B makes a signature $S' = (s'_x, s'_y)$ for M' with his secret key d_B:

$S' = d_B \times M'$ over $C_{n_B}(0, b'_B)$.

Then, A computes the signature

$S = (s_x, s_y) = (u^{-2} s'_x (mod\ n_B), u^{-3} s'_y (mod\ n_B))$. Which is B's signature for the message M.

Note that the curve $C_{n_B}(0, b_B)$ contains points (M, S) and the curve $C_{n_B}(0, b'_B)$ contains points (M', S').

Using this technique A can forge B's signatures without B's secret key.

6. **Conclusion.**

IIn the attack proposed by Seng et al [10] attacker has to compute the GCD of two polynomials both of degree e while in our proposed attack, attacker has to compute the GCD of two polynomials of degree 6 and of degree e. Therefore, the attack proposed by us is more efficient than that of the Seng et al. Next, by using the Isomorphic attack one can forge signature of system generator on any message without using the secret key.

References

[1] D. Coppersmith, M. Franklin, J. Patarin and M. Reiter, Low exponent attack RSA with related messages. Proceeding in EUROCRYPT'96 volume 765, LNCS pp.40-49. Springer- Vrelag, 1996.

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

[3] K.Koyama, Fast RSA type scheme based on singular cubic curve $y^2 + axy = x^3 (mod\ n)$. Proc. Eurocrypt'95, Lecture Notes in Computer Science, vo.921, Springer, Berlin, 1995, pp.329-339.

[4] K.Koyama and H. Kuwakado, Efficient cryptosystems over elliptic curves based on a product of form-free primes. IEICE Trans. Fund. E77-A (1994) 1309-1318.

[5] K. Koyama 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.

[6] K. Koyama, U.M. Maurer, T. Okamoto and S. A. Vanstone, New public key schemes based on elliptic curves over the ring , Proc. Crypto 91 (1991), 252-266.

[7] H. Kuwakado,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.

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

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

[10] Seng Kiat Chua, Ka Hin Leung, San Ling,Attack on RSA-type cryptosystem based on singular cubic curves over Z/nZ^*. Theoretical Computer Science,1999, v.220 19-27. .