

# Attack on RSA-type cryptosystems based on singular cubic curves over $\mathbb{Z}/n\mathbb{Z}$

Chua, Seng Kiat; Leung, Ka Hin; Ling, San

1999

Chua, S. K., Leung, K. H., & Ling, S. (1999). Attack on RSA-type cryptosystems based on singular cubic curves over  $\mathbb{Z}/n\mathbb{Z}$ . *Theoretical Computer Science*, 226(1-2), 19-27.

<https://hdl.handle.net/10356/95880>

[https://doi.org/10.1016/S0304-3975\(99\)00062-6](https://doi.org/10.1016/S0304-3975(99)00062-6)

---

© 1999 Elsevier Science B.V. This is the author created version of a work that has been peer reviewed and accepted for publication by *Theoretical Computer Science*, Elsevier Science B.V. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [DOI: [http://dx.doi.org/10.1016/S0304-3975\(99\)00062-6](http://dx.doi.org/10.1016/S0304-3975(99)00062-6)].

*Downloaded on 20 Mar 2024 20:17:43 SGT*

# Attack on RSA-type cryptosystems based on singular cubic curves over $\mathbb{Z}/n\mathbb{Z}$ <sup>☆</sup>

Seng Kiat Chua, Ka Hin Leung, San Ling <sup>\*</sup>

*Department of Mathematics, National University of Singapore, Lower Kent Ridge Road,  
Singapore 119260, Singapore*

---

## Abstract

Several RSA-type cryptosystems based on singular cubic curves have been proposed in recent years (cf. Koyama, Lecture notes in Computer Science, vol. 921, Springer, Berlin, 1995, pp. 329–339; Kuwakado, IEICE Trans. Fund. E78-A (1995) 27–33; Koyama, IEICE Trans. Fund. E77-A (1994) 1309–1318). We show that these schemes are equivalent and demonstrate that they are insecure if a linear relation is known between two plaintexts.

*Keywords:* Singular cubic curves; RSA-type cryptosystems

---

## 1. Introduction

In recent years, elliptic curves (non-singular cubic curves) have found many applications in public key cryptography. Several RSA-type schemes based on elliptic curves have been proposed (cf. [2, 7, 5]). Instead of elliptic curves, three RSA-types schemes have been proposed which are based on singular cubic curves (cf. [4, 8, 6]). In all these schemes, two plaintext messages  $m_x$  and  $m_y$  are used to form a point  $M = (m_x, m_y)$  on a singular cubic curve of a predetermined type over  $\mathbb{Z}/n\mathbb{Z}$ . The ciphertext is then a point  $C = eM$  on the same curve. In this paper, we show that these three schemes are insecure if a linear relation is known between two plaintexts.

The paper is organised as follows. Section 2 contains general facts about singular cubic curves over finite fields  $\mathbb{F}_p$  and the rings  $\mathbb{Z}/n\mathbb{Z}$ . Section 3 describes the three RSA-type schemes which are based on singular cubic curves modulo  $n$ . In Section 4, we show that the three schemes are equivalent to each other. Section 5 contains the

---

<sup>☆</sup> This work was funded by grant number RP 960668/M.

<sup>\*</sup> Corresponding author.

*E-mail addresses:* matchua@nus.edu.sg (S.K. Chua), matlkh@nus.edu.sg (K.H. Leung), matlings@nus.edu.sg (S. Ling)

main theorem which gives the formula for the division polynomials on singular cubic curves. Finally, we give a detailed description of the attack in Section 6.

## 2. Singular cubic curves

In this section, we discuss some basic facts about singular cubic curves over the finite field  $\mathbf{F}_p$  and the ring  $\mathbf{Z}/n\mathbf{Z}$ , where  $n = pq$  is the product of two distinct odd primes greater than 3.

Consider the congruence

$$y^2 + axy \equiv x^3 + bx^2 \pmod{p}, \quad a, b \in \mathbf{Z}. \quad (1)$$

We use  $C_p(a, b)$  to denote the set of all solutions  $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$  to (1), excluding the point  $(0, 0)$ , but including a “point at infinity”, denoted by  $\mathcal{O}$ . The curve  $C_p(a, b)$  is called a *singular cubic curve* over  $\mathbf{F}_p$ .

It is well known that the same addition laws defined by the chord-and-tangent method in the case of elliptic curves still hold in the case of singular cubic curves [9]. For any point  $P$  on  $C_p(a, b)$ , the sum  $P + \mathcal{O}$  is, by definition, equal to  $P$ , which is also equal to  $\mathcal{O} + P$ . For  $P = (x_0, y_0)$ , we define  $-P$  as the point  $(x_0, -y_0 - ax_0)$ . The sum  $P + (-P)$  is defined to be  $\mathcal{O}$ . 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:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + 2bx_1 - ay_1}{2y_1 + ax_1} & \text{if } P_1 = P_2, \end{cases} \quad \text{and} \quad \mu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{-x_1^3}{2y_1 + ax_1} & \text{if } P_1 = P_2, \end{cases}$$

$$x_3 = \lambda^2 + a\lambda - b - x_1 - x_2 \quad \text{and} \quad y_3 = -(\lambda + a)x_3 - \mu.$$

The existence of such addition laws makes  $C_p(a, b)$  a finite abelian group. In fact, the group structure of  $C_p(a, b)$  is known.

Consider the quadratic congruence

$$T^2 + aT - b \equiv 0 \pmod{p} \quad (2)$$

and let  $\alpha, \beta \in \mathbf{F}_{p^2}$  be the roots of (2). We have that  $\alpha, \beta \in \mathbf{F}_p$  if and only if  $((a^2 + 4b)/p) = 1$ .

For  $a, b$  as in (1), suppose further that  $a^2 + 4b \not\equiv 0 \pmod{p}$ . Let  $L_p(a, b)$  be defined as follows:

$$L_p(a, b) = \begin{cases} \mathbf{F}_p^\times & \text{if } \left(\frac{a^2 + 4b}{p}\right) = 1 \\ \{x \in \mathbf{F}_{p^2} \mid x^{p+1} = 1\} & \text{if } \left(\frac{a^2 + 4b}{p}\right) = -1. \end{cases}$$

Then it is well known that  $L_p(a, b)$  is a cyclic group and that there is an isomorphism (cf. [9])

$$\begin{aligned} C_p(a, b) &\xrightarrow{\sim} L_p(a, b), \\ (x, y) &\mapsto \frac{y - \beta x}{y - \alpha x} = \left(1 + \frac{a^2 + 4b}{2x}\right) + \left(-\frac{ax + 2y}{x^2}\right) \gamma, \\ \emptyset &\mapsto 1, \end{aligned} \quad (3)$$

where  $\gamma = \beta + a/2$  so that  $\gamma^2 = (a^2 + 4b)/4 \pmod p$ .

The inverse of the map (3) can be described as follows. An element of  $L_p(a, b)$  may be written in the form of  $f + g\gamma$  with  $\gamma$  as above,  $f, g \in \mathbf{F}_p$  and  $f^2 - \gamma^2 g^2 = 1$ . This element is sent by the inverse map to the point  $(x, -\frac{1}{2}(gx^2 + ax))$  of  $C_p(a, b)$ , where  $x \equiv 2\gamma^2/(f - 1) \equiv (a^2 + 4b)/(2(f - 1)) \pmod p$ .

When  $n = pq$  is the product of two distinct primes greater than 3, we consider similarly the congruence

$$y^2 + axy \equiv x^3 + bx^2 \pmod n. \quad (4)$$

We denote by  $C_n(a, b)$  the set of solutions to (4) in  $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ , excluding those points which are either congruent to  $(0, 0)$  modulo  $p$  or congruent to  $(0, 0)$  modulo  $q$ , but including a “point at infinity”. By the Chinese Remainder Theorem,  $C_n(a, b)$  is isomorphic as a group to  $C_p(a, b) \times C_q(a, b)$ . The curve  $C_n(a, b)$  is called a *singular cubic curve* over  $\mathbf{Z}/n\mathbf{Z}$ .

### 3. RSA-type schemes based on singular cubic curves

Three RSA-type schemes have been proposed which are based on singular cubic curves modulo  $n$ .

#### 3.1. Scheme 1 [8]

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

$$C_n(0, b): \quad y^2 \equiv x^3 + bx^2 \pmod n, \quad (5)$$

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

$$N_n = \text{lcm}(p - 1, p + 1, q - 1, q + 1).$$

*Encryption:* Given a plaintext  $M = (m_x, m_y)$ , the sender first computes

$$b \equiv \frac{m_y^2 - m_x^3}{m_x^2} \pmod n$$

then the ciphertext is computed as  $C = eM$  on the singular cubic curve  $C_n(0, b)$ .

### 3.2. Scheme 2 [4]

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

$$C_n(a, 0): y^2 + axy \equiv x^3 \pmod{n}, \quad (6)$$

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

$$N_n = \text{lcm}(p-1, q-1).$$

*Encryption:* Given a plaintext  $M = (m_x, m_y)$ , the sender first computes

$$a \equiv \frac{m_x^3 - m_y^2}{m_x m_y} \pmod{n}$$

then the ciphertext is computed as  $C = eM$  on the singular cubic curve  $C_n(a, 0)$ .

### 3.3. Scheme 3 [6]

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

$$(y - \alpha x)(y - \beta x) = x^3 \pmod{n}, \quad (7)$$

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

$$N_n = \text{lcm}(p-1, q-1).$$

*Encryption:* Given a plaintext  $M = (m_x, m_y)$ , the sender chooses  $\alpha \in (\mathbf{Z}/n\mathbf{Z})^*$  randomly, and computes

$$\beta \equiv \frac{m_x^3 - m_y^2 + \alpha m_x m_y}{m_x(\alpha m_x - m_y)} \pmod{n}$$

then the ciphertext is computed as  $C = eM$  on the singular cubic curve defined in Eq. (7).

## 4. Equivalence of the three schemes

In this section, we will show that all the three schemes described above can be reduced to one scheme, namely, Scheme 1.

### 4.1. Reduction of Scheme 2 to Scheme 1

The following change of variables

$$(x, y) \mapsto \left(x, y + \frac{a}{2}x\right)$$

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 2 to Scheme 1.

#### 4.2. Reduction of Scheme 3 to Scheme 1

The following change of variables

$$(x, y) \mapsto \left( x, y - \frac{\alpha + \beta}{2}x \right)$$

will transform the curve

$$(y - \alpha x)(y - \beta) = x^3$$

to the curve  $C_n(0, b)$  with  $b = ((\alpha - \beta)/2)^2$ . Using this transformation, one can reduce Scheme 3 to Scheme 1.

#### 5. Division polynomials on singular cubic curves

To carry out the attack on RSA-type schemes based on singular cubic curves, we need to introduce the notion of division polynomials on singular cubic curves, similar to the notion of division polynomials on elliptic curves (see [9]). They allow us to compute the multiple of a point in terms of the first coordinate. Since we have shown that both Schemes 2 and 3 can be reduced to Scheme 1, we will only describe the division polynomials for the singular cubic curves of the form  $C_n(0, b)$ .

**Definition 1.** The division polynomials  $\Psi_m(x, y)$  for the singular cubic curve  $C_n(0, b)$  are defined inductively by

$$\Psi_1 = 1,$$

$$\Psi_2 = 2y,$$

$$\Psi_3 = 3x^4 + 4bx^3,$$

$$\Psi_4 = 4y(x^6 + 2bx^5),$$

$$\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, \quad (m \geq 2),$$

$$2y\Psi_{2m} = \Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) \quad (m \geq 3).$$

**Theorem 2.** Let  $C_n(0, b)$  be a singular cubic curve defined over the ring  $\mathbf{Z}/n\mathbf{Z}$ . If  $P = (x, y) \in C_n(0, b)$ , then the first coordinate of  $mP$  is given by

$$x(mP) = \frac{x^{m^2}}{\Psi_m(x, y)^2} = \frac{x^m}{\Phi_m(x, y)},$$

where  $\Psi_m(x, y)$  is the  $m$ th division polynomial for  $C_n(0, b)$  and  $\Phi_m(x, y)$  is the polynomial defined by

$$\Phi_m(x, y) = \frac{\Psi_m(x, y)^2}{x^{m^2-m}}.$$

**Proof.** To prove this formula, we first note that the rational function  $x(mP)$  has poles at those points  $T$  such that  $mT = \mathcal{O}$ , with multiplicity 1. Since  $(0, 0)$  is not a point on the curve  $C_n(0, b)$ ,  $x(mP)$  is never equal to zero. Hence the rational function  $x(mP)$  must be of the form

$$x(mP) = \frac{k_m x^m}{m^2 \prod_{\substack{mT=\mathcal{O} \\ T \neq \mathcal{O}}} (x - x(T))} = \frac{k_m x^{m^2}}{F_m(x)},$$

where  $k_m$  is a constant independent of  $x$  and  $F_m(x)$  is the polynomial defined by

$$F_m(x) = m^2 x^{m^2-m} \prod_{\substack{mT=\mathcal{O} \\ T \neq \mathcal{O}}} (x - x(T)).$$

We first claim that  $k_m = 1$ . By a straightforward computation, it is not difficult to see that  $x(mP)$  can be expressed in the form

$$x(mP) = \frac{\phi_m(x)}{\Psi_m(x, y)^2},$$

where  $\phi_m(x) = x^{m^2} + \text{lower order terms}$ , and  $\Psi_m(x, y)^2 = m^2 x^{m^2-1} + \text{lower order terms}$ . (Note that the formula obtained above is similar to that given in [9, Exercise 3.7].) By comparing the coefficients of the leading terms in the equation

$$k_m x^{m^2} \psi_m(x)^2 = \phi_m(x) F_m(x)$$

we easily deduce  $k_m = 1$ . Note that even though the degree of  $\phi_m(x)$  is  $m^2$ , it is not clear that  $\phi_m(x) = x^{m^2}$ .

Observe that for any point  $T \neq \mathcal{O}$  with  $mT = \mathcal{O}$ , we have  $m(-T) = \mathcal{O}$ . Moreover,  $T = -T$  if and only if  $2T = \mathcal{O}$ . In conclusion, we have

- for  $m$  odd, all factors in the product occur with multiplicity 2;
- for  $m$  even, all factors in the product occur with multiplicity 2 except those  $T$  for which  $2T = \mathcal{O}$ .

However, note that

$$x^2 \prod_{\substack{2T=\mathcal{O} \\ T \neq \mathcal{O}}} (x - x(T)) = y^2.$$

Hence  $F_m$  is a perfect square as a polynomial in  $x, y$ . In other words, there exists a polynomial  $\varphi_m(x, y)$  satisfying  $F_m(x) = \varphi_m(x, y)^2$  for each  $m$ . We shall prove that  $\varphi_m(x, y)$  is the  $m$ th division polynomial for  $C_n(0, b)$ . For  $m = 1, 2, 3, 4$ , we can easily verify that

$$\begin{aligned} F_1(x) &= 1 = \Psi_1(x, y)^2, \\ F_2(x) &= (2y)^2 = \Psi_2(x, y)^2, \\ F_3(x) &= x^6(3x + 4b)^2 = \Psi_3(x, y)^2, \\ F_4(x) &= x^{10}(4y(x + 2b))^2 = \Psi_4(x, y)^2. \end{aligned}$$

So far, we have proved that  $\Psi_m(x, y) = \varphi_m(x, y)$  if  $m \leq 4$ . We shall now prove by induction on  $m$  that indeed  $\Psi_m(x, y) = \varphi_m(x, y)$  for  $m \geq 1$ . Suppose we have proved that  $\Psi_m(x, y) = \varphi_m(x, y)$  for  $m \leq m_0$ .

Let  $m$  be an integer with  $m + 2 \leq m_0$ . Consider the rational function  $x - x(mP)$ .

- It has poles exactly at the zeros of  $\Psi_m^2$ , with the same multiplicity 2.
- It has zeros at those points  $T$  such that

$$mT = \pm T \quad \text{i.e., } (m \pm 1)T = \mathcal{O}.$$

These points have multiplicity 1.

By comparing the coefficients of the leading terms, we conclude that

$$x - x(mP) = \frac{\Psi_{m+1}\Psi_{m-1}}{\Psi_m^2} \quad \text{and} \quad x - x((m+1)P) = \frac{\Psi_{m+2}\Psi_m}{\Psi_{m+1}^2}.$$

By the above formula and induction, we then get

$$x(mP) - x((m+1)P) = \frac{\Psi_{m+2}\Psi_m^3 - \Psi_{m+1}^3\Psi_{m-1}}{\Psi_{m+1}^2\Psi_m^2} = \frac{x^{m^2}}{F_m(x)} - \frac{x^{(m+1)^2}}{F_{m+1}(x)}.$$

Note that  $\Psi_{m+2}\Psi_m^3 - \Psi_{m+1}^3\Psi_{m-1} = \Psi_{2m+1}$  and

$$\frac{x^{m^2}}{F_m(x)} - \frac{x^{(m+1)^2}}{F_{m+1}(x)} = \frac{x^m p(x)}{q(x)},$$

where  $p(x), q(x)$  are polynomials in  $x$  and  $x$  does not divide  $q(x)$ . Clearly,  $\Psi_{2m+1}(x) = x^m p(x) \Psi_{m+1}^2 \Psi_m^2$ . Observe that by induction,  $x^{(m+1)^2 - (m+1)}$  and  $x^{m^2 - m}$  divide  $\Psi_{m+1}^2$  and  $\Psi_m^2$ , respectively. Since  $x$  does not divide  $q(x)$ , it follows that  $x^{2m^2 + m}$  divides  $\Psi_{2m+1}$ . On the other hand, the rational function  $x(mP) - x((m+1)P)$  has zeros at those points  $T$  such that

$$(m+1)T = \pm mT, \quad \text{i.e., } ((m+1) \pm m)T = \mathcal{O}.$$

Hence these points are the zeros of  $\Psi_{2m+1}$ . Combining with the earlier observation that  $x^{2m^2 + m}$  divides  $\Psi_{2m+1}$ , we conclude that  $F_{2m+1}$  divides  $\Psi_{2m+1}^2$ . Finally, by comparing the degrees and their leading coefficients, we see that  $F_{2m+1} = \Psi_{2m+1}^2$  and hence  $\varphi_{2m+1} = \Psi_{2m+1}$ .

By using a similar argument on the rational function  $x((m+1)P) - x((m-1)P)$ , it is straightforward to prove that  $\Psi_{2m} = \varphi_{2m}$ . This completes the proof of our theorem.  $\square$

## 6. Detailed description of the attack

To illustrate the attack, we shall only focus on the first coordinate. Let  $x(M_1) = m_x$  and  $x(M_2) = m_x + \Delta$  be the  $x$ -coordinates of two plaintexts  $M_1$  and  $M_2$ , and let  $c_{1,x}$  and  $c_{2,x}$  be the  $x$ -coordinates of the two corresponding ciphertexts  $C_1 = eM_1$  and  $C_2 = eM_2$ ,

respectively. Recall that  $\Delta$  is a known constant. By the previous theorem, we have

$$\begin{aligned} m_x^e - c_{1,x} \Phi_e(m_x, \cdot) &\equiv 0 \pmod{n}, \\ (m_x + \Delta)^e - c_{2,x} \Phi'_e(m_x + \Delta, \cdot) &\equiv 0 \pmod{n}, \end{aligned}$$

where  $\Phi_m$  is defined by

$$\Phi_m(x, y) = \frac{\Psi_m(x, y)^2}{x^{m^2-m}}$$

for the curve  $C_n(0, b)$  on which  $M_1$  and  $C_1$  lie. The function  $\Phi'_m$  is defined analogously for the curve on which  $M_2$  and  $C_2$  lie. This relation allows us to construct the following attack.

(1) Let  $F(x)$  and  $G(x)$  be polynomial over the ring  $\mathbf{Z}/n\mathbf{Z}$ , defined by

$$\begin{aligned} F(x) &= x^e - c_{1,x} \Phi_e(x, \cdot), \\ G(x) &= (x + \Delta)^e - c_{2,x} \Phi'_e(x + \Delta, \cdot). \end{aligned}$$

(2) We compute  $H(x) = \gcd(F(x), G(x))$ , the gcd of  $F(x)$  and  $G(x)$  over the ring  $\mathbf{Z}/n\mathbf{Z}$ , which is with a very high probability, a polynomial of degree 1. Solving the polynomial  $H(x)$  in  $x$  will give the value of  $m_x$ .

Although this attack is similar to that proposed in [3], it should be noted that, unlike the elliptic curve case where the polynomials  $F(x)$  and  $G(x)$  are of degree  $e^2$ , our attack involves only polynomials of degree  $e$  and is therefore much more efficient.

**Example.** Suppose we set

$$\text{keys: } p = 1237, \quad q = 5683, \quad e = 11,$$

$$\text{plaintext: } M_1 = (54321, 67890), \quad M_2 = (54411, 67980), \quad \text{i.e., } \Delta = 90$$

$$\text{ciphertext: } C_1 = (2687388, 3712394), \quad C_2 = (2387261, 3231021).$$

Let  $F(x) = x^{11} + 5229989x^{10} + 3440216x^9 + 1918724x^8 + 833716x^7 + 4214133x^6 + 5288492x^5 + 658705x^4 + 5018141x^3 + 2203074x^2 + 3786039x + 3314999$  and  $G(x) = x^{11} + 6396991x^{10} + 4606503x^9 + 6789657x^8 + 6778159x^7 + 6520626x^6 + 6319754x^5 + 806279x^4 + 3985603x^3 + 4360013x^2 + 4835444x + 1937673$ . Then  $\text{GCD}(F(x), G(x)) = 6975550 + x$ . Solving, we get  $x = 54321$ .

## 7. Conclusion

We have shown that the RSA-type schemes in [4,6] are special cases of that in [8]. Moreover, we have described an attack on the scheme in [8] (and hence those in [4,6]) when the  $x$ -coordinates of the plaintexts are related by a known linear relation. Our attack uses polynomials of degree  $e$  (which is the same as in the case of the classical RSA (cf. [1])) as compared to the elliptic curve case which needs polynomials of degree  $e^2$ .

In [1], the following generalizations were discussed: (i) when the number of messages involved could be more than 2; and (ii) when the messages are known to be related in some ways more complicated than a linear relation. It is easy to see that our above attack could be modified to accommodate these generalizations. In all cases, as a result of the Theorem above, the complexity of the algorithms for the attacks on the singular cubic curve schemes is the same as those for the classical RSA schemes, which is in turn more efficient than the corresponding attacks on the RSA-type schemes based on elliptic curves.

## References

- [1] D. Coppersmith, M. Franklin, J. Patarin, M. Reiter, Low-exponent RSA with related messages, *Advances in Cryptology – Proc. Eurocrypt’96*, Lecture Notes in Computer Science, vol. 1070, Springer, Berlin, 1996, pp. 1–9.
- [2] N. Demytko, A new elliptic curve based analogue of RSA, *Advances in Cryptology – Proc. Eurocrypt’93*, Lecture Notes in Computer Science, vol. 765, Springer, Berlin, 1993, pp. 40–49.
- [3] M. Joye, J.-J. Quisquater, Protocols Failures for RSA-like Functions using Lucas Sequences and Elliptic Curves, Technical Report CG-1995/4, Université Catholique de Louvain Crypto Group, 1995.
- [4] K. Koyama, Fast RSA-type schemes based on singular cubic curves  $y^2 + axy \equiv x^3 \pmod{n}$ , *Advances in Cryptology – Proc. Eurocrypt’95*, Lecture Notes in Computer Science, vol. 921, Springer, Berlin, 1995, pp. 329–339.
- [5] K. Koyama, H. Kuwakado, Efficient cryptosystems over elliptic curves based on a product of form-free primes, *IEICE Trans. Fund. E77-A* (1994) 1309–1318.
- [6] K. Koyama, H. Kuwakado, A new RSA-type scheme based on singular cubic curves  $(y - \alpha x)(y - \beta x) \equiv x^3 \pmod{n}$ , *IEICE Trans. Fund. E79-A* (1996) 49–53.
- [7] K. Koyama, U.M. Maurer, T. Okamoto, S.A. Vanstone, New public-key schemes based on elliptic curves over the ring  $Z_n$ , *Advances in Cryptology – Proc. Crypto’91*, Lecture Notes in Computer Science, vol. 576, Springer, Berlin, 1992, pp. 252–266.
- [8] H. Kuwakado, K. Koyama, Y. Tsuruoka, A new RSA-type scheme based on singular cubic curves  $y^2 \equiv x^3 + bx^2 \pmod{n}$ , *IEICE Trans. Fund. E78-A* (1995) 27–33.
- [9] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer, Berlin, 1986.