

An Improvement on Shimada's Public-Key Cryptosystem

Chin-Chen Chang and Sun-Min Tsu

Department of Computer Science and Information Engineering,
National Chung Cheng University, Chiayi, Taiwan, R. O. C

Abstract

The difficulty of breaking Rabin's cryptosystem is the same as that of factoring its public key. So far, this has been proven to be very difficult. However the disadvantage of Rabin's cryptosystem is that the deciphering function cannot produce a unique plaintext. Many modified Rabin's cryptosystems have been proposed. Recently, an excellent scheme modified from Rabin's cryptosystem has been proposed by Shimada. Using Shimada's scheme, we can obtain the desired plaintext without any information additional to the ciphertext itself. Here we propose an improvement to this scheme to simplify the decryption process. Our effort makes the implementation of Shimada's public key cryptosystem more efficient.

Key Words: Rabin cryptosystem, ciphertext, plaintext, enciphering function, deciphering function

1. Introduction

Shimada [4] proposed a new cryptosystem based on Rabin's cryptosystem [3], which can restrict the domain of Rabin's enciphering function. More significantly, it can obtain the plaintext from the ciphertext C alone (i.e. without expanding the block size). The plaintext is one of the solutions for $x^2 = C \pmod{n}$, and it can be determined according to the information generated from the ciphertext C itself. The computation of finding solutions, however, is a very time-consuming process. Thus, how to simplify this time-consuming process is our major concern in this paper.

2. A Brief Review of Shimada's Scheme

Here, some definitions must be stated to understand Shimada's cryptosystem.

Definition 2.1 Generalized Legendre Symbol

Let p be an odd prime number and a be an integer. The generalized Legendre symbol $L(\frac{a}{p})$ is defined as follows:

$$L\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a^{(p-1)/2} = 1 \pmod{p}, \\ -1 & \text{if } a^{(p-1)/2} = -1 \pmod{p}. \end{cases}$$

Definition 2.2 Generalized Jacobi Symbol

Let $n = pq$ be a positive integer for odd primes p and q , and let i be any integer. Then the generalized Jacobi symbol $J(\frac{i}{n})$ is defined below:

$$J\left(\frac{i}{n}\right) = L\left(\frac{i}{p}\right) \times L\left(\frac{i}{q}\right),$$

where $L(\frac{i}{p})$ and $L(\frac{i}{q})$ are generalized Legendre symbols.

Shimada's encryption scheme is briefly described in the following steps. If the user U_j wants to send the plaintext M to the user U_i secretly, he/she has to attach the user U_i 's public key N , where N is the product of two odd primes p and q , with the form of $p = 7 \pmod{8}$ and $q = 3 \pmod{8}$. Besides, two public encryption functions, t_e and u_e , are used in the enciphering algorithm.

Enciphering: For a given plaintext $M \in \{0, 1, \dots, N-1\}$, a ciphertext C can be obtained as follows :

Step 1: Calculate $t_e(M)$

$$t_e(M) = \begin{cases} 1 & \text{if } 0 < M \leq (N-1)/2, \\ -1 & \text{if } (N-1)/2 < M \leq (N-1). \end{cases}$$

Step 2: Calculate $u_e(M)$

$$u_e(M) = \begin{cases} 1 & \text{if } J\left(\frac{M}{N}\right) = 1 \text{ or } 0, \\ 2 & \text{if } J\left(\frac{M}{N}\right) = -1. \end{cases}$$

Step 3: Evaluate θ

$$\theta = M^2 \pmod{N}.$$

Step 4: Generate the ciphertext C

$$C = t_e(M) u_e(M) \theta \pmod{N}.$$

The ciphertext C is transmitted to the user U_i .

When the user U_i receives the ciphertext C, he/she can obtain the plaintext M by using the following deciphering algorithm with the secret key pair (p, q), and two decryption function t_d and u_d .

Deciphering: For a given ciphertext $C \in 0, 1, \dots, N-1$, a plaintext M can be obtained as follows:

Step 1: Calculate $t_d(C)$

$$t_d(C) = \begin{cases} 1 & \text{if } L\left(\frac{C}{p}\right) = L\left(\frac{C}{q}\right) = 0, \\ L\left(\frac{C}{p}\right) & \text{if } L\left(\frac{C}{p}\right) = 0 \text{ and } L\left(\frac{C}{q}\right) \neq 0, \\ L\left(\frac{C}{q}\right) & \text{if } L\left(\frac{C}{p}\right) \neq 0. \end{cases}$$

Step 2: Calculate $U_d(C)$

$$u_d(C) = \begin{cases} 1 & \text{if } L\left(\frac{C}{p}\right)L\left(\frac{C}{q}\right) = 0 \text{ or } 1, \\ 2 & \text{if } L\left(\frac{C}{p}\right)L\left(\frac{C}{q}\right) = -1. \end{cases}$$

Table 1: Relation between solutions of $x^2 = \theta \pmod{N}$ and the corresponding ciphertext C

Range	$J\left(\frac{x}{N}\right)$	$t_e(x)$	$u_e(x)$	$L\left(\frac{C}{p}\right)$	$L\left(\frac{C}{q}\right)$
$0 < X \leq 1$ (N-1/2)	1	1	1	1	1
$0 < X \leq -1$ (N-1/2)	-1	1	2	1	-1
$(N/2) < X \leq -1$ (N-1)	-1	-1	2	-1	-1
$(N/2) < X \leq 1$ (N-1)	1	-1	1	-1	1

Step 3: Calculate θ

$$\theta = C[t_d(C)]^{-1}[u_d(C)]^{-1} \pmod{N},$$

where $[t_d(C)]^{-1}$ is the inverse of $t_d(C)$ modulo N such that $[t_d(C)]^{-1} [t_d(C)] \equiv 1 \pmod{N}$, and $[u_d(C)]^{-1}$ is the inverse of $u_d(C)$ modulo N such that $[u_d(C)]^{-1} [u_d(C)] \equiv 1 \pmod{N}$.

Step 4: Recover the plaintext M

Find the solution of $x^2 = \theta \pmod{N}$ for which

$$t_e(x) = t_d(C) \quad (1)$$

$$\text{and } u_e(x) = u_d(C). \quad (2)$$

Then the specified solution x is the plaintext M corresponding to the ciphertext C.

For more clearness, the following table displays the relation between the solutions of $x^2 = \theta \pmod{N}$ and the corresponding ciphertext C.

3. Our Improvement to Shimada's Scheme

Shimada's scheme can restrict the domain of Rabin's enciphering function. Besides, the specified solution can be found according to the ciphertext itself, without any additional indication information. However, Step 4 in Section 2, the cost of computing Equation(2) is similar to that of computing exponentiation. It is a time-consuming process. To reduce this cost of deciphering, we will propose a solution. First, a method described in [3] is used to solve the congruence $\theta = M^2 \pmod{N}$. This method is briefly introduced in the following. The solutions are obtained by first solving the two equations

$$x^2 \pmod{p} = \theta \pmod{p} = a, \quad (3)$$

$$x^2 \pmod{q} = \theta \pmod{q} = b. \quad (4)$$

The solutions x_p and $(p-x_p)$ are obtained from Equation(3), where $x_p = a^{(p+1)/4} \pmod{p}$. Similarly, x_q and $(q-x_q)$ are obtained from Equation(4), where $x_q = b^{(q+1)/4} \pmod{q}$. The pairs (x_p, x_q) , $(x_p, q-x_q)$, $(p-x_p, x_q)$ and $(p-x_p, q-x_q)$ are successively substituted for (x_p, x_q) in the following system of equations:

$$x = x_p \pmod{p},$$

$$x = x_q \pmod{q}.$$

The four solutions $root_1$, $root_2$, $root_3$ and $root_4$ can be computed by Chinese remainder theorem.

Theorem 3.1 Chinese Remainder Theorem [1]

Let p_1, p_2, \dots, p_t be pairwise relatively primes, and let $n = p_1 p_2 \dots p_t$. Then the system of equations

$$x = x_i \pmod{p_i}, \quad (i=1, 2, \dots, t)$$

has a solution x in the range $[0, n-1]$, $x =$

$$\left[\sum_{i=1}^t \left(\frac{n}{p_i} \right) y_i x_i \right] \pmod{n}, \text{ where } y_i \text{ is the inverse}$$

of $\left(\frac{n}{p_i} \right)$ modulo p_i such that $y_i \left(\frac{n}{p_i} \right) = 1 \pmod{p_i}$.

Let CRT be the implementation of Chinese remainder theorem; that is, $\text{CRT}(n, p_1, p_2, \dots, p_t, x_1, x_2, \dots, x_t) = x$.

According to the above, we have

$$\text{root}_1 = \text{CRT}(N, p, q, x_p, x_q),$$

$$\text{root}_2 = \text{CRT}(N, p, q, x_p, q - x_q),$$

$$\text{root}_3 = \text{CRT}(N, p, q, p - x_p, x_q),$$

$$\text{root}_4 = \text{CRT}(N, p, q, p - x_p, q - x_q).$$

In fact, $\text{root}_4 = N - \text{root}_1$ and $\text{root}_3 = N - \text{root}_2$.

Theorem 3.2

Let t_d and u_d be two decryption functions, the root of $M^2 = \theta \pmod{N}$ can be determined by the following rules:

$$M = \begin{cases} \text{root}_1 \text{ or } \text{root}_4 & \text{if } t_d(C) = 1 \text{ and } u_d(C) = 1, \\ \text{root}_2 \text{ or } \text{root}_3 & \text{if } t_d(C) = 1 \text{ and } u_d(C) = 2, \\ \text{root}_2 \text{ or } \text{root}_3 & \text{if } t_d(C) = -1 \text{ and } u_d(C) = 2, \\ \text{root}_1 \text{ or } \text{root}_4 & \text{if } t_d(C) = -1 \text{ and } u_d(C) = 1, \end{cases}$$

Where $x_p \in \text{QR}_p$ and $x_q \in \text{QR}_q$, $C = t_e(M)u_e(M) \theta \pmod{N}$, $\theta = M^2 \pmod{N}$ and $N = pq$. Here p and q are two large primes with forms $p = 7 \pmod{8}$ and $q = 3 \pmod{8}$, respectively.

Proof:

Assume that $t_d(C) = 1$ and $u_d(C) = 1$, then the root of $M^2 = \theta \pmod{N}$ satisfying that $t_e(M) = 1$ and $u_e(M) = 1$ is the specified solution. Now, we want to prove that, in this case, $M = \text{root}_1$ or root_4 . Namely, we are going to prove this by the known fact that $J\left(\frac{M}{N}\right) = 1$ according to Table 1.

Since M is the root of $M^2 = \theta \pmod{N}$, so we have the following four cases.

Case 1: $M = \text{root}_1$

Since $x_p \in \text{QR}_p$, then

$$L\left(\frac{M}{p}\right) = M^{(p-1)/2} \pmod{p} = (x_p)^{(p-1)/2} \pmod{p} = 1.$$

Similarly, Since $x_q \in \text{QR}_q$, then

$$L\left(\frac{M}{q}\right) = M^{(q-1)/2} \pmod{q} = (x_q)^{(q-1)/2} \pmod{q} = 1.$$

We have $J\left(\frac{M}{N}\right) = 1$.

Case 2: $M = \text{root}_2$

Since $x_p \in \text{QR}_p$, then

$$L\left(\frac{M}{p}\right) = M^{(p-1)/2} \pmod{p} = (x_p)^{(p-1)/2} \pmod{p} = 1.$$

Since $q - x_q \in \text{QNR}_q$, then

$$L\left(\frac{M}{q}\right) = M^{(q-1)/2} \pmod{q} = (x_q)^{(q-1)/2} \pmod{q} = -1.$$

We have $J\left(\frac{M}{N}\right) = -1$. It contradicts to $J\left(\frac{M}{N}\right) = 1$.

Case 3: $M = \text{root}_3$

Since $p - x_p \in \text{QNR}_p$, then

$$L\left(\frac{M}{p}\right) = M^{(p-1)/2} \pmod{p} = (x_p)^{(p-1)/2} \pmod{p} = -1.$$

Since $x_q \in \text{QR}_q$, then

$$L\left(\frac{M}{q}\right) = M^{(q-1)/2} \pmod{q} = (x_q)^{(q-1)/2} \pmod{q} = 1.$$

We have $J\left(\frac{M}{N}\right) = -1$. It contradicts to $J\left(\frac{M}{N}\right) = 1$.

Case 4: $M = \text{root}_4$

Since $p - x_p \in \text{QNR}_p$, then

$$L\left(\frac{M}{p}\right) = M^{(p-1)/2} \pmod{p} = (x_p)^{(p-1)/2} \pmod{p} = -1$$

Similarly, Since $q - x_q \in \text{QNR}_q$, then

$$L\left(\frac{M}{q}\right) = M^{(q-1)/2} \pmod{q} = (x_q)^{(q-1)/2} \pmod{q} = -1$$

We have $J\left(\frac{M}{N}\right) = 1$.

Then we conclude that if $t_d(C) = 1$ and $u_d(C) = 1$, the specified solution of $M^2 = \theta \pmod{N}$ is root_1 or root_4 . Similarly, the other three conditions can be proved in the same way. **Q.E.D.**

From Step 4 of Shimada's deciphering procedure, we must check Equations (1) and (2) for all possible solutions. It is doubtless that the process is very time-consuming. According to Theorem 3.3, the specified solution of $M^2 = \theta \pmod N$ can be determined by checking the values of $t_d(C)$ and $u_d(C)$. Because we show that the specified solution can be easily determined by the known $t_d(C)$ and $u_d(C)$, thus the cost of computing Equations (1) and (2) can be eliminated. In the following, a more efficient, in term of computation cost, deciphering scheme is proposed.

Deciphering : For a given ciphertext $C \in \{0, 1, \dots, N-1\}$, a plaintext M can be obtained as follows:

Step 1: Calculate $t_d(C)$

$$t_d(C) = \begin{cases} 1 & \text{if } L\left(\frac{C}{p}\right) = L\left(\frac{C}{q}\right) = 0, \\ L\left(\frac{C}{p}\right) & \text{if } L\left(\frac{C}{p}\right) = 0 \text{ and } L\left(\frac{C}{q}\right) \neq 0, \\ L\left(\frac{C}{q}\right) & \text{if } L\left(\frac{C}{p}\right) \neq 0. \end{cases}$$

Step 2: Calculate $u_d(C)$

$$u_d(C) = \begin{cases} 1 & \text{if } L\left(\frac{C}{p}\right)L\left(\frac{C}{q}\right) = 0 \text{ or } 1, \\ 2 & \text{if } L\left(\frac{C}{p}\right)L\left(\frac{C}{q}\right) = -1. \end{cases}$$

Step 3: Calculate θ

$$\theta = C[t_d(C)]^{-1}[u_d(C)]^{-1} \pmod N,$$

where $[t_d(C)]^{-1}$ is the inverse of $t_d(C)$ modulo N such that $[t_d(C)]^{-1} [t_d(C)] \equiv 1 \pmod N$, and $[u_d(C)]^{-1}$ is the inverse of $u_d(C)$ modulo N such that $[u_d(C)]^{-1} [u_d(C)] \equiv 1 \pmod N$.

Step 4: Find the four pairs (x_p, x_q) , $(x_p, q-x_q)$, $(p-x_p, x_q)$ and $(p-x_p, q-x_q)$

Compute

$$M^2 \pmod p = \theta \pmod p = a,$$

$$M^2 \pmod q = \theta \pmod q = b.$$

Compute $x_p = a^{(p+1)/4} \pmod p$, and $x_q = b^{(q+1)/4} \pmod q$.

Compute the four pairs (x_p, x_q) , $(x_p, q-x_q)$,

$(p-x_p, x_q)$ and $(p-x_p, q-x_q)$.

Step 5: Recover the plaintext M according to $t_d(C)$ and $u_d(C)$

Compute $t_d(C)$ and $u_d(C)$.

Case 1: $t_d(C) = 1$ and $u_d(C) = 1$

Compute $M = \text{CRT}(N, p, q, x_p, x_q)$.

Table 2: Relation among the (α, β) pair, the range,

$$J\left(\frac{M}{N}\right), t_e(M), u_e(M)$$

Range	$J\left(\frac{M}{N}\right)$	$t_e(M)$	$u_e(M)$	(α, β)
$0 < X \leq 1$ ($N-1/2$)	1	1	1	(x_p, x_q) or $(p-x_p, q-x_q)$
$0 < X \leq -1$ ($N-1/2$)	-1	1	2	$(x_p, q-x_q)$ or $(p-x_p, x_q)$
$(N/2) < X \leq (N-1)$	-1	-1	2	$(x_p, q-x_q)$ or $(p-x_p, x_q)$
$(N/2) < X \leq (N-1)$	1	-1	1	(x_p, x_q) or $(p-x_p, q-x_q)$

If M is in $(0, N/2)$, then output M ; else compute $M = N - M$ and output M .

Case 2: $t_d(C) = 1$ and $u_d(C) = 2$.

Compute $M = \text{CRT}(N, p, q, x_p, q-x_q)$.

If M is in $(0, N/2)$, then output M ; else compute $M = N - M$ and output M .

Case 3: $t_d(C) = -1$ and $u_d(C) = 2$.

Compute $M = \text{CRT}(N, p, q, x_p, q-x_q)$.

If M is in $(N/2, N)$, then output M ; else compute $M = N - M$ and output M .

Case 4: $t_d(C) = -1$ and $u_d(C) = 1$.

Compute $M = \text{CRT}(N, p, q, x_p, q-x_q)$.

If M is in $(N/2, N)$, then output M ; else compute $M = N - M$ and output M .

Table 2 lists the conditions to show how to select the appropriate pair (α, β) from four pairs (x_p, x_q) , $(x_p, q-x_q)$, $(p-x_p, x_q)$ and $(p-x_p, q-x_q)$ to evaluate the specified solution of $M^2 = \theta \pmod N$.

Example 3.1

The secret keys for Bob are $p=23$ and $q=19$. The public key N is therefore 437. Suppose Alice wants to send $M=59$ to Bob.

Enciphering: Since $59 \in [0, (N-1)/2]$ and $J(\frac{M}{N}) = -1$, then $t_e(M) = 1$ and $u_e(M) = 2$. $\theta = 59^2 \bmod 437 = 422$. Thus, Alice has $C = 1 \times 2 \times 422 \bmod 437 = 407$. The ciphertext is then transmitted to Bob by Alice.

Deciphering: Bob receives the ciphertext $C = 407$.

Step 1: Calculate $t_d(C)$

$$t_d(C) = t_d(407) = 1.$$

Step 2: Calculate $u_d(C)$

$$u_d(C) = u_d(407) = 2.$$

Step 3: Calculate θ

$$\theta = C[t_d(C)]^{-1}[u_d(C)]^{-1} \bmod N = 422.$$

Step 4: Find the four pairs (x_p, x_q) , $(x_p, q-x_q)$, $(p-x_p, x_q)$ and $(p-x_p, q-x_q)$

Compute

$$M^2 \bmod p = \theta \bmod p = 8,$$

$$M^2 \bmod q = \theta \bmod q = 4.$$

Compute $x_p = a^{(p+1)/4} \bmod p = 13$, and $x_q = b^{(q+1)/4} \bmod q = 17$.

Compute the four pairs $(x_p, x_q) = (13, 17)$, $(x_p, q-x_q) = (13, 2)$, $(p-x_p, x_q) = (10, 17)$ and $(p-x_p, q-x_q) = (10, 2)$.

Step 5: Recover the plaintext M according to $t_d(C)$ and $u_d(C)$

Because $t_d(C) = 1$ and $u_d(C) = 2$, the pair $(13, 2)$ is selected.

Compute $M = \text{CRT}(437, 23, 19, 13, 2) = 59$. Since 59 is in the range $(0, 218)$, so 59 is the desired message.

4. Conclusion

Here an improvement on Shimada's public-key cryptosystem is proposed. It can speed up the deciphering process by directly checking $t_d(C)$ and $u_d(C)$. We eliminate the need to compute Equations (1) and (2). This improvement makes Shimada's scheme very efficient and practical.

Reference

- [1] Denning, D. E. "Cryptography and Data Security," Addison-Wesley, Reading, Massachusetts, (1982).
- [2] Rosen, K. H. "Elementary Number Theory and Its Applications," Addison-Wesley, Reading, Massachusetts, (1982).

- [3] Rabin, M. O. "Digital Signatures and Public Key Functions as Intractable as Factorization," MIT/LCS/TR-212, January (1979).
- [4] Shimada, M. "Another Practical Public-Key Cryptosystem," *Electronics Letters*, Vol. 28, No.23, pp. 2146-2147, Nov. (1992).

Accepted: Sep. 20, 2000