PUBLIC KEY CRYPTOSYSTEM USING A RECIPROCAL NUMBER WITH THE SAME INTRACTABILITY AS FACTORING A LARGE NUMBER

Kaoru KUROSAWA Toshiya Itoh Masashi Takeuchi

Department of Electrical and Electronic Engineering,
Faculty of Engineering,
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152, Japan
kurosawa@ss.titech.ac.jp

Abstract This paper proposes a public key cryptosystem using a reciprocal number. Breaking the proposed cryptosystem is proven to be as difficult as factoring a large number. Encryption requires $O(n^2)$ bit operations and decryption requires $O(n^3)$ bit operations. (n is the bit length of a plaintext.)

1 Introduction

A public key cryptosystem proposed by Rabin [1] is excellent because it has been proven that breaking the cryptosystem is as hard as factoring a large number. However, a ciphertext cannot be uniquely deciphered because four different plaintexts produce the same cipher. Williams [2] showed that this disadvantage can be overcome if the secret two prime numbers, p and q, are chosen such that $p = q = 3 \bmod 4$.

RSA cryptosystem [3] is the most well-known public key cryptosystem. However, it is not known whether breaking RSA cryptosystem is as hard as factoring a lagre number. Recently, Williams [4] proposed a modified RSA cryptosystem which utilizes quadratic irrational numbers. He showed that the cryptosystem is as difficult to break as it is to factor a large number.

Such RSA schemes require $O(n^3)$ bit operations for both encryption and decryption (where n is the bit length of a plaintext).

This paper proposes a public key cryptosystem using a reciprocal number. Breaking the proposed cryptosystem is proven to be as difficult as factoring a large number. Encryption requires only $O(n^2)$ bit operations and decryption requires $O(n^3)$ bit operatinos. The secret two prime numbers, p and q, are arbitrary, which is a great advantage over Williams' version [2] of Rabin's cryptosystem.

2 Preliminaries

2.1 Legendre's symbol and Jacobi's symbol

The following symbol is called Legendre's symbol.

$$(a/p) \overset{\triangle}{=} \begin{cases} 1 & \text{if ``}x^2 = a \bmod p\text{'' has a solution;} \\ -1 & \text{otherwise,} \end{cases}$$

where p is a prime number other than 2. Half of the integers "a" such that $0 < a < p$ satisfy $(a/p) = 1$ and the other half satisfy $(a/p) = -1$.

The following symbol is called Jacobi's symbol.

$$(a/R) \overset{\triangle}{=} (a/p)(a/q),$$

where $R = pq$. The value of (a/R) is computed efficiently by applying a method like Euclidean algorithm to "a" and R.

2.2 Rabin's cryptosystem

Rabin proposed the following public key cryptosystem [1].

(Secret key) two lagre prime numbers, p and q.

(Public key) $R(= pq)$ and c.

(Plaintext) M, where $0 < M < R$.

(Ciphertext) $E = M(M + c) \bmod R$.

(Decryption) Solve the following quadratic equations.

$$M^2 + cM - E = 0 \bmod p \quad (1)$$

$$M^2 + cM - E = 0 \bmod q \quad (2)$$

He has proved that breaking the crytosystem is as hard as factoring pq. However, the ciphertexts cannot be uniquely deciphered because four different plaintexts produce the same cipher.

Williams showed that the following special form of Rabin's cryptosystem can overcome the above disadbantage [2].

(Secret key) two lagre prime numbers, p and q, where $p = q = 3 \bmod 4$.

(Public key) $R(= pq)$.

(Plaintext) M, where $0 < M < R/2$ and $(M/R) = 1$.

(Ciphertext) $E = M^2 \bmod R$.

We call the above cryptosystem "restricted Rabin's cryptosystem" because p and q are restricted such that $p = q = 3 \bmod 4$.

3 Public key cryptosystem using a reciprocal numbner

We present a public key cryptosystem that utilizes the reciprocal number of a plaintext modulo $R(= p \cdot q)$. Breaking our cryptosystem is proven to be as hard as factoring R. The encryption procedure requires $O(n^2)$ bit operateions and decryption requires $O(n^3)$ bit operations, where n is the bit length of a plaintext. The secret two prime numbers, p and q, are arbitrary, which is a great advantage over restricted Rabin's cryptosystem.

(Secret key) two lagre prime numbers, p and q.

(Public key) $R(= pq)$ and c such that

$$(c/p) = (c/q) = -1 \tag{3}$$

(Plaintext) M, where $0 < M < R$ and $\gcd(M, R) = 1$.

> (When p and q are 250 bits long, the probability that $\gcd(M, R) = p$ or q is $(p+q)/R \approx 2^{-250}$, which is negligibly small. RSA cryptosystem is also broken if $\gcd(M, R) = p$ or q.)

(Ciphertext) (E, s, t), where

$$\begin{aligned} E &= M + (c/M) \bmod R & (4) \\ s &= \begin{cases} 0 & \text{if } (M/R) = 1; \\ 1 & \text{if } (M/R) = -1. \end{cases} & (5) \\ t &= \begin{cases} 0 & \text{if } (c/M \bmod R) > M; \\ 1 & \text{if } (c/M \bmod R) < M, \end{cases} & (6) \end{aligned}$$

(Decryption) From (4), we obtain

$$M^2 - EM + c = 0 \qquad (7)$$

Let a_1 and a_2 be the roots of (7) $\bmod p$ and b_1 and b_2 be the roots of (7) $\bmod q$. (Solving (7) $\bmod p$ or $\bmod q$ will be shown in Sec. 5.) Then, (7) $\bmod R$ has the following four roots:

$$\begin{aligned} M_1 &= [a_1, b_1], \qquad & M_2 &= [a_2, b_2] \\ M_3 &= [a_1, b_2], \qquad & M_4 &= [a_2, b_1] \end{aligned}$$

where $M_1 = [a_1, b_1]$ means $M_1 = a_1 \bmod p$ and $M_1 = b_1 \bmod q$. (Chinese remainder theorem gives M_i from a_j and b_k.)

The plaintext M is one of the four roots. s and t tell the receiver which root the plaintext M is. From (3) and the relationship between the roots and the coefficients of (7), we obtain

$$(a_1/p)(a_2/p) = (c/p) = -1.$$

We set

$$(a_1/p) = 1, \qquad (a_2/p) = -1. \qquad (8)$$

Similarly, we set

$$(b_1/q) = 1, \qquad (b_2/q) = -1. \qquad (9)$$

Then, we obtain

$$(M_1/R) = (M_1/p)(M_1/q) = (a_1/p)(b_1/q) = 1.$$

Similarly, we get

$$\begin{aligned} (M_2/R) &= 1 \\ (M_3/R) &= (M_4/R) = -1. \end{aligned}$$

Therefore, the receiver sees that

$$M = \begin{cases} M_1 \text{ or } M_2 & \text{if } s = 0; \\ M_3 \text{ or } M_4 & \text{if } s = 1. \end{cases}$$

Now, suppose that $s = 0$. The relationship between the roots and the coefficients of (7) gives us

$$M_1 M_2 = [a_1 a_2, b_1 b_2] = [c, c] = c \bmod R.$$

Hence,

$$M_2 = c/M_1 \bmod R.$$

Therefore, the receiver sees that

$$M = \begin{cases} \min(M_1, M_2) & \text{if } t = 0; \\ \max(M_1, M_2) & \text{if } t = 1. \end{cases}$$

When $s = 1$,

$$M = \begin{cases} \min(M_3, M_4) & \text{if } t = 0; \\ \max(M_3, M_4) & \text{if } t = 1. \end{cases}$$

Thus, a ciphertext is uniquely deciphered.

(Digital signature) Let

$$E_j = E + j.$$

Increase j $(j = 0, 1, 2, ...)$ until the following equation holds.

$$((E_j^2 - 4c)/p) = ((E_j^2 - 4c)/q) = 1 \tag{10}$$

Let j satisfying (10) be J and let M_J be any one of the plaintexts obtained from E_J. The signed message is (M_J, J).

4 Intractability of breaking the proposed cryptosystem

It will now be shown that breaking the proposed cryptosystem is as difficult as factoring a large number. It is clear that the proposed cryptosystem is broken if one can factor $R = pq$. We will prove the converse. That is, one can factor $R = pq$ if the proposed cryptosystem is broken.

THEOREM 1 *Neither " (7) mod p " nor " (7) mod q " has a multiple root.*

(Proof)

From (8) and (9), we get

$$a_1 \neq a_2 \bmod p, \qquad b_1 \neq b_2 \bmod q$$

Q.E.D.

THEOREM 2 *Suppose that there exists a polynomial time algorithm finding the plaintext from any ciphertext of the proposed cryptosystem. Then, there exists a polynomial time algorithm factoring $R = pq$ with probability $1/4$.*

(Proof)

Choose at random a number $0 < c < R$. c satisfies (3) with 1/4 probability. Let (R, c) be a public key of the proposed cryptosystem.

Pick any plaintext M. Compute M' as follows:

$$\begin{aligned} M &\rightarrow (E, s, t) \text{ (Encryption)} \\ &\rightarrow (E, \bar{s}, t) \\ &\rightarrow M' \text{ (Decryption)}, \end{aligned}$$

where $\bar{s} = s + 1 \bmod 2$.

Let $M = [f_1, g_1]$. Since $\bar{s} = s + 1 \bmod 2$,

$$M' = [f_1, g_2] \text{ or } M' = [f_2, g_1].$$

Let's consider the case of $M' = [f_1, g_2]$. Then,

$$M - M' = [f_1, g_1] - [f_1, g_2] = [0, g_1 - g_2].$$

From Theorem 1, $g_1 - g_2 \neq 0 \bmod q$. That is, $M - M' = 0 \bmod p$ and $M - M' \neq 0 \bmod q$. Therefore, $\gcd(M - M', R) = p$.

The number of bit operations required by the above procedure is clearly polynomial of n (n is the bit length of R). The proof in the case of $M' = [f_2, g_1]$ is the same.

Q.E.D.

The probability that the above probabilistic algorithm fails after 100 trials is $(3/4)^{100} = 10^{-13}$, which is negligibly small.

The next theorem strengthens Theorem 2.

THEOREM 3 *Suppose that there exists a polynomial time algorithm finding the plaintext from $1/K$ of all the ciphertexts of the proposed cryptosystem. Then, there exists a polynomial time algorithm factoring $R = pq$ with probability $1/4K$.*

(Proof)

Let X be the set of the ciphertexts which are broken by the supposed algorithm. Choose at randam a number $0 < M < R$. The ciphertext of M belongs to X with $1/K$ probability. We can apply the same algorithm in the proof of Theorem 2 to the M. It is clear that the total algorithm succeds with probability $1/4K$.

Q.E.D.

5 A quadratic equation $\bmod p$ in the proposed cryptosystem

This chapter shows how to solve "(7) $\bmod p$ " or "(7) $\bmod q$ ". (We use the same notation as in Sec. 3.) The following theorem is attained by modifying Rabin's method [5] to the proposed cryptosystem.

THEOREM 4 *(i) Over $GF(p)$,*

$$\gcd(x^{(p-1)/2} - 1, x^2 - Ex + c) = x - a_1$$

(ii) Over $GF(q)$,

$$\gcd(x^{(q-1)/2} - 1, x^2 - Ex + c) = x - b_1$$

(Proof)

(i) (8) and Euler's criterion give us

$$a_1^{(p-1)/2} = 1, \quad a_2^{(p-1)/2} = -1$$

Therefore, a_1 is a root of $x^{(p-1)/2} - 1$ and a_2 isn't. This shows that (i) holds.

(ii) The proof is the same as (i).

Q.E.D.

a_2 and b_2 are obtained from the relationship between the roots and the coefficients of (7) as follows:

$$a_2 = E - a_1 \bmod p$$
$$b_2 = E - b_1 \bmod q.$$

Note that $\gcd(x^{(p-1)/2} - 1, x^2 - Ex + c)$ can be obtained by computing

$$x^{(p-1)/2} \bmod (x^2 - Ex + c).$$

6 Computational complexity

Let a plaintext M be n bits long.

(Encryption) $1/M \bmod R$ is computed by applying Enclidean algorithm to M and R. (M/R) is computed in a similar way. Euclidean algorithm requires $O(n^2)$ bit operations. The multiplication of $c \cdot (1/M) \bmod R$ also requires $O(n^2)$ bit operations. Therefore, encryption of the proposed cryptosystem requires $O(n^2)$ bit operations.

(Decryption) Note that the method shown in Sec. 5 is equivalent to computing

$$x^{(p-1)/2} \bmod x^2 - Ex + c$$
$$x^{(q-1)/2} \bmod x^2 - Ex + c.$$

The above equations are computed by $O(n^3)$ bit operaionts. Therefore, the complexity of decryption is $O(n^3)$.

Table 1 shows the comparison of computational complexity.

Table 1. Comparison of computational complexity (bit operations)

	Proposed	Rabin	RSA
(Encryption)	$O(n^2)$	$O(n^2)$	$O(n^2)$(e is small.) $O(n^3)$(e is large.)
(Decryption)	$O(n^3)$	$O(n^3)$	$O(n^3)$

7 Discussion

The decryption procedure for Rabin's cryptosystem is to solve

$$M^2 + cM - E = 0.$$

On the other hand,

$$M^2 - EM + c = 0,$$

must be solved in the proposed cryptosystem. The quadratic equation of the proposed cryptosystem is given only by exchanging the constant term and the linear term of Rabin's quadratic equation. This exchange overcomes the disadvantages of Rabin's cryptosystem and restricted Rabin's cryptosystem. That is,

1. A ciphertext is uniquely deciphered.
2. The two secret prime numbers, p and q, are arbitrary.

8 Example

(Secret key) $p = 11, q = 13$

(Public key) $R(= pq) = 143, c = 2$

(Plaintext) $M = 24$

(Encryption)

$$E = 24 + (2/24) = 36 \bmod 143,$$

$s = 0$ because $(24/R) = 1$. $t = 1$ because

$$c/M = 2/24 = 12 \bmod 143 \text{ and } 12 < 24(= M).$$

(Ciphertext) $(36, 0, 1)$

(Decryption) Solving $M^2 - 36M + 2 = 0 \bmod 11$ yields

$$a_1 = 1, \quad a_2 = 2.$$

Solving $M^2 - 36M + 2 = 0 \bmod 13$ yields

$$b_1 = 12, \quad b_2 = 11$$

Since $s = 0$, the plaintext is

$$M_1 = [1, 12] = 12 \text{ or } M_2 = [2, 11] = 24$$

Since $t = 1$ and $M_1 < M_2$, the receiver sees that $M = 24$.

9 Summary

The authors propose a Public Key Cryptosystem using a reciprocal number. It has been proved that breaking the proposed cryptosystem is as hard as factoring a large number. Encryption requires $O(n^2)$ bit operations and decryption requires $O(n^3)$ bit operations. The proposed cryptosystem has no disadvantage of Rabin's cryptosystem.

It will take further work to develop a more efficient method that solves a quadratic equation mod$p$.

References

[1] M.O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization ", *Technical Report LCS/TR212, Cambridge MA:MIT,* 1979.

[2] H.C. Williams, "A modification of the RSA public-key encryption procedure ", *IEEE Trans. Information Theory.* 26: 726-729, 1980.

[3] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems ", *Comm. ACM.*21: 120-126, 1978.

[4] H.C. Williams, "Some public-key cryptofunctions as intractable as factorization ", *Cryptologia.* 9: 223-237, 1985.

[5] M.O. Rabin, "Probabilistic algorithms in finite fields ", *SIAM J. Comput.* 9: 273-280, 1980.