Joint Conference of 1996 International Computer Symposium
December 19~21, Kaohsiung, Taiwan, R.O.C.

Fast RSA-type Schemes Based on Pell Equations over Z_N^*

Chien-Yuan Chen
Department of Information Engineering,
Kaohsiung Polytechnic Institute, Tahsu, Kaohsiung, Taiwan 840, R.O.C.
E-mail: cyChen@csa500.kpi.edu.tw
Chin-Chen Chang
Institute of Computer Science and Information Engineering,
National Chung Cheng University, Chiayi, Taiwan 621, R.O.C.
E-mail: ccc@cs.ccu.edu.tw
Wei-Pang Yang
Department of Computer and Information Science,
National Chiao Tung University, Hsinchu, Taiwan 300, R.O.C.

Abstract

In this paper, we propose two new fast RSA-type schemes based on Pell equations over the ring Z_N^*. The decryption speed of the proposed schemes is about two times as fast as that of the RSA scheme for a 2 logN-bit long message. The encryption speed of our schemes is about 1.5 times slower than that of the RSA scheme. So, our schemes can be used in communications between a smart card and a larger computer. In addition, we also prove that the proposed schemes are as secure as the RSA scheme against the ciphertext attack.

Keywords: Public-key system, Pell equations, the RSA scheme,

1. Introduction

An analogue of the RSA scheme based on the use of elliptic curves was first proposed by Koyama et al. in 1991. The scheme, called the KMOV scheme, seems to be more secure than the RSA scheme from the viewpoint of the Hastad attack [3]. However, the decryption speed of the KMOV scheme is about 5.8 times as slow as that of the RSA scheme. Later, Demytko presented another RSA-type scheme based on elliptic curves [2] such that most of the limitations of the KMOV scheme are overcome. When the decryption speed is considered, however, Demytko's scheme is slower than the KMOV scheme. In 1995, Koyama presented fast RSA-type schemes based on singular cubic curves [5]. The decryption speed of the schemes is about two times as fast as that of the RSA scheme. But the encryption speed of Koyama's scheme 1 in [5] is roughly (5 + d)/2 times slower than that of the RSA scheme, where d means the ratio of the computation amount of division to that of multiplication. In fact , these RSA-type schemes based on elliptic curves are less efficient in encryption. Obviously, it is attractive to develop a more efficient RSA-type scheme.

In this paper, we describe a cyclic group G_P over the Pell equation

$x^2 - Dy^2 \equiv 1 \pmod P$,

where P is an odd prime. Some properties of the group G_P are then deduced. These properties are also found in the group G_N over the Pell equation $x^2 - Dy^2 \equiv 1 \pmod N$, where N is a product of two primes. This group G_N is then developed to be a public key cryptoscheme based on Pell equations over the ring Z_N^*. From the group G_N, we find a group isomorphism mapping f: $G_N \rightarrow Z_N^*$ such that a solution (x, y) of the Pell equation $x^2 - Dy^2 \equiv 1 \pmod N$ can easily be transformed to a unique element $u \in Z_N^*$. This implies that the plaintexts/ciphertexts in the group G_N can easily be transformed to the corresponding plaintexts/ciphertexts in the RSA scheme. So, we present new RSA-type schemes such that the ciphertexts can be deciphered by the isomorphic mapping and the RSA scheme. These new schemes decrypt the ciphertexts about two times faster than the RSA scheme for a 2 *log*N-bit message. Furthermore, the encryption speed of the proposed schemes is only 1.5 times as slow as that

of the RSA scheme. Comparing to Koyama's scheme 1, our schemes are more efficient.

In Section 2, we introduce Pell equations over the ring Z_N^*. Section 3 presents our schemes. In Section 4, performance analysis is given. Securities of our schemes are analyzed in Section 5. The last section concludes this paper.

2. Pell equations over the ring Z_N^*

Let P be an odd prime and D be a non-zero quadratic residue element in F_P. G_P denotes the set of solutions $(x, y) \in F_P \times F_P$ to the Pell equation

$$x^2 - Dy^2 \equiv 1 \pmod P. \qquad (2.1)$$

We then define an addition operation "⊕" on G_P as follows. If two pairs $(x_1, y_1), (x_2, y_2) \in G_P$, then the third pair (x_3, y_3) can be computed by

$$(x_3, y_3) \equiv (x_1, y_1) \oplus (x_2, y_2)$$
$$\equiv (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1) \pmod P. \quad (2.2)$$

If we define the identity element by (1, 0) and the inverse of the element (x, y) by (x, -y), then it is easy to verify that the addition operation is closed, associative and communicative. That is to say, G_P together with the operation "⊕" is an abelian group. We further give the following theorem according to [7].

Theorem 2.1: G_P together with the operation "⊕" is a cyclic group of order P - 1.

Now we want to prove that the group G_P is isomorphic to F_P^*, where F_P^* denotes a multiplicative group of F_P.

Theorem 2.2: Two groups G_P and F_P^* are isomorphic.

Proof. (sketch)

Let $f : G_P \to F_P^*$ be a mapping from G_P to F_P^* such that

$$f((1, 0)) \equiv 1 \pmod P,$$
$$f((x, y)) \equiv x - ay \pmod P,$$

where $(x, y) \in G_P$ and $a^2 \equiv D \pmod P$.

If $A = (x_1, y_1)$, $B = (x_2, y_2) \in G_P$, then we have

$$f(A \oplus B) = f((x_1, y_1) \oplus (x_2, y_2)) = f((x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1))$$
$$\equiv x_1x_2 + Dy_1y_2 - a(x_1y_2 + x_2y_1) \pmod P$$
$$\equiv x_1x_2 - ax_1y_2 - ax_2y_1 + a^2y_1y_2 \pmod P$$
$$\equiv (x_1 - ay_1)(x_2 - ay_2) \pmod P$$
$$\equiv f(A)f(B).$$

This implies that f is a homomorphism of G_P into F_P^*.

Next we will claim that f is a one-to-one homomorphism of G_P onto F_P^*.

For each $u \in F_P^*$, we assume that there exists an element $(x, y) \in G_P$ such that

$$u \equiv x - ay \pmod P. \qquad (2.3)$$

Because $(x, y) \in G_P$, we have

$$x^2 - a^2y^2 \equiv 1 \pmod P,$$
$$(x - ay)(x + ay) \equiv 1 \pmod P,$$
$$u(x + ay) \equiv 1 \pmod P, \text{ and}$$
$$x + ay \equiv u^{-1} \pmod P, \qquad (2.4)$$

where u^{-1} means the inverse of u modulo P. From Equations (2.3) and (2.4), we have

$$x \equiv (u + u^{-1})/2 \pmod P \text{ and}$$
$$y \equiv (u^{-1} - u)/2a \pmod P. \qquad (2.5)$$

So, f is an onto mapping. From Equation (2.5) for each $u \in F_P^*$, there exists a unique element (x, y) satisfying $f((x, y)) \equiv u$. Therefore, f is a one-to-one homomorphism of G_P onto F_P^*.

This concludes that G_P is isomorphic to F_P^*.■

Now we define another operation "⊗" as follows:

$$i \otimes (x, y) = \underbrace{(x, y) \oplus (x, y) \oplus \cdots \oplus (x, y)}_{i \text{ times}} \text{ over } G_P.$$

If $(x_i, y_i) = i \otimes (x, y)$, we expand the above expression and have

$$x_i = \sum_{\substack{0 \le k \le i \\ k \text{ is even}}} \binom{i}{k} D^{\lfloor \frac{k}{2} \rfloor} x^{i-k} y^k,$$

$$y_i = \sum_{\substack{0 \le k \le i \\ k \text{ is odd}}} \binom{i}{k} D^{\lfloor \frac{k}{2} \rfloor} x^{i-k} y^k \qquad (2.6)$$

According to the definition of the mapping f, we have

$$f((x_i, y_i)) \equiv x_i - ay_i$$

$$\equiv \sum_{\substack{0\le k\le i \\ k \text{ is even}}} \binom{i}{k} D^{\lfloor \frac{k}{2} \rfloor} x^{i-k} y^k - a \sum_{\substack{0\le k\le i \\ k \text{ is odd}}} \binom{i}{k} D^{\lfloor \frac{k}{2} \rfloor} x^{i-k} y^k$$

$$\equiv \sum_{\substack{0\le k\le i \\ k \text{ is even}}} \binom{i}{k} x^{i-k} (ay)^k + \sum_{\substack{0\le k\le i \\ k \text{ is odd}}} \binom{i}{k} x^{i-k} (-ay)^k$$

$\equiv (x - ay)^i$. (2.7)

Because G_P is a cyclic group of order P -1, we have that if $k \equiv 1 \pmod{P - 1}$, then

$(x, y) = k \otimes (x, y)$, for all $(x, y) \in G_P$. (2.8)

Let N be a product of two large primes p and q. Z_N^* denotes a multiplicative group of Z_N. From Theorem 2.2, it is easy to develop the following theorem.

Theorem 2.3: The mapping $f : G_N \to Z_N^*$ satisfying

$f((1, 0)) \equiv 1 \pmod N$,

$f((x, y)) \equiv x - ay \pmod N$,

where $(x, y) \in G_N$ and $a^2 \equiv D \pmod N$, is a group isomorphism. Its inverse mapping $f^{-1} : Z_N^* \to G_N$ is defined by

$f^{-1}(1) \equiv (1, 0) \pmod N$,

$f^{-1}(u) \equiv ((u + u^{-1})/2, (u^{-1} - u)/2a) \pmod N$,

where $u \in Z_N^*$.

Considering Equations (2.7) and (2.8), we have the following results over the ring Z_N^*.

Theorem 2.4: If $(x_i, y_i) = i \otimes (x, y)$ over G_N, we have $x_i - ay_i \equiv (x - ay)^i \pmod N$.

Theorem 2.5: If $k \equiv 1 \bmod (l.c.m.(p -1, q -1))$, we have $(x, y) = k \otimes (x, y)$, for all $(x, y) \in G_N$.

3. New-type RSA schemes based on Pell equations

In this section, two RSA-type schemes based on Pell equations are presented. The main difference between these two schemes is the way of encryption. One uses Formula (2.2), while the other uses exponentiation. These two schemes have the same key generation procedure as follows.

Assume that the recipient R selects two large primes p and q. He then chooses an integer e such that *g.c.d.*(e, *l.c.m.*(p-1, q-1))=1. Using the Euclidean theorem he determines the secret key d satisfying $ed \equiv 1 \pmod{l.c.m.\ (p -1, q -1)}$. Finally, the recipient R publishes (e, N=pq) as his public key and keeps the keys p, q, d secret. To simplify notation, we often omit, in the rest of this paper, the mod N.

3.1 Scheme 1

Assume that the sender S wants to send the messages m_1 and m_2 to the recipient R.

Encryption:

The sender S first changes the messages m_1 and m_2 into values $z_1 \equiv m_1 + m_2$ and $z_2 \equiv m_1 - m_2$. He solves the equations

$x - az_2 \equiv z_1$, and (3.1)

$x + az_2 \equiv z_1^{-1}$,

and gets $x \equiv (z_1 + z_1^{-1})/2$ and $a \equiv (z_1^{-1} - x)/z_2$. Let $y \equiv z_2$ and $D \equiv a^2$. Then, (x, y) is a solution of the Pell equation $x^2 - Dy^2 \equiv 1$. Next, he iteratively uses Formula (2.2) to compute

$e \otimes (x, y) = (x_c, y_c)$, (3.2)

where e is the public key of the recipient. Then, the sender S sends the ciphertext (x_c, y_c, a) to the recipient R.

Decryption:

After receiving the ciphertext (x_c, y_c, a), the recipient R checks that

$x_c^2 - a^2 y_c^2 \equiv 1$. (3.3)

If yes, he continues to compute

$C = f((x_c, y_c)) \equiv x_c - ay_c$. (3.4)

Then, he uses the secret key d to compute

$M \equiv C^d$. (3.5)

The solution (x, y) can be obtained by evaluating $x \equiv (M + M^{-1})/2$ and $y \equiv (M^{-1} - x)/a$. This implies $z_1 \equiv M$ and $z_2 \equiv y$. Therefore, the recipient R can get the original messages $m_1 \equiv (z_1 + z_2)/2$ and $m_2 \equiv (z_1 - z_2)/2$.

3.2 Scheme 2

Assume that the sender S wants to send the messages m_1 and m_2 to the recipient R.

Encryption:

The sender S first changes the messages m_1 and m_2 into values $z_1 \equiv m_1 + m_2$ and $z_2 \equiv m_1 - m_2$. He solves the equations

$x - az_2 \equiv z_1$, and

$x + az_2 \equiv z_1^{-1}$,

and gets $x \equiv (z_1 + z_1^{-1})/2$ and $a \equiv (z_1^{-1} - x)/z_2$. Let $y \equiv z_2$ and $D \equiv a^2$. Then, (x, y) is a solution of the Pell equation $x^2 - Dy^2 \equiv 1$. Then he uses Theorem 2.3 to compute

$M = f((x, y)) \equiv x - ay \equiv z_2$.

Then, he uses the public key e to compute

$C \equiv M^e$. (3.6)

The ciphertext (C, a) is sent to the recipient R.

Decryption:

After receiving the ciphertext (C, a), the recipient R uses his secret key d to compute

$M \equiv C^d$. (3.7)

Using Theorem 2.3, he can obtain (x, y) by $x \equiv (M + M^{-1})/2$ and $y \equiv (M^{-1} - M)/2a$. This implies $z_1 \equiv M$ and $z_2 \equiv y$. So, the original messages $m_1 \equiv (z_1 + z_2)/2$ and $m_2 \equiv (z_1 - z_2)/2$ are discovered.

4. Performance analyses

4.1 Comparison of our schemes and the RSA scheme

Here, we focus on the decryption procedure to evaluate the average number of modular multiplications. In general, $M \equiv C^d$ requires $1.5 log d$ multiplications modulo N on average. Our proposed schemes, i.e., Scheme 1 and Scheme 2, involve Equations (3.5) and (3.6). So, the decryption of each scheme requires at least $1.5 log d$ multiplications modulo N on average. Besides, the cost of isomorphic mapping requires two modular inverses and one modular multiplication. According to [1, 4], one modular inverse requires six modular multiplications. So, the decryption of each scheme requires $1.5 log d + 13$ modular multiplications on average. If we neglect the cost of isomorphic mapping, our proposed schemes almost have the same decryption time as the RSA scheme. Because the block size for each one of our proposed schemes is two times as large as that for the RSA scheme, the decryption speed of the former is about two times faster than that of the latter.

4.2 Comparison of Scheme 1 and Koyama's Scheme 1

In [5], Koyama evaluated the average number of modular multiplications for decryption excluding the cost of isomorphic mapping. Here we focus on the cost of isomorphic mapping of Koyama's scheme 1. It requires seven modular multiplications and three modular inverses. However, Scheme 1 in this paper only requires one modular multiplication and two modular inverses, to perform isomorphic mapping. Obviously, the decryption speed of Scheme 1 is somewhat faster than that of Koyama's scheme 1 if the cost of isomorphic mapping is considered.

4.3 Comparison of Scheme 1 and Scheme 2

From Subsection 4.1, we know that Scheme 1 and Scheme 2 have the same decryption speed. Here we focus on the encryption procedures without considering the cost of the isomorphic mapping. Scheme 1, involving Equation (3.2), requires $4.5 log e$ multiplications modulo N on average by using the right-to-left binary method. This result is deduced by $0.5*(2) + 0.5*(2+5) = 4.5\ log e$ modular multiplications because the equation

$2 \otimes (x, y) \equiv (x^2 + Dy^2, 2xy) \equiv (2x^2 - 1, 2xy)$

and Equation (2.2) require 2 and 5 modular multiplications, respectively. Scheme 2, however, only requires $1.5 log e$ multiplications modulo N on average. Considering the block size, we find that the encryption speed of Scheme 2 is about two times faster than that of the RSA scheme. Similarly, the encryption speed of Scheme 1 is about 1.5 times slower than that of the RSA scheme. According to [5], the encryption speed of Koyama's scheme 1 is roughly $(5 + d)/2$ times slower than that of the RSA scheme. Therefore, the speed of Scheme 1 is faster than that of Koyama's scheme 1.

In addition, the length of ciphertext in Scheme 1 is 1.5 times as large as that in Scheme 2. Although Scheme 1 requires additional space, it can check the ciphertext against accidental corruption.

5. Security

Under the ciphertext attack, we claim that our proposed schemes are as secure as the RSA scheme.

Theorem 5.1: The ciphertext attack in the RSA scheme is polynomially reduced to that in Scheme 1.

Proof (sketch):

Let (x_c, y_c, a) be the ciphertext of Scheme 1. Assume that there exists an algorithm A which can output the solution (x, y) given the input (x_c, y_c, a). Now given the ciphertext C in the RSA scheme, one can discover the corresponding message by using Algorithm A as follows.

Firstly let us randomly select a pair (x_c, y_c). Then compute $a \equiv (x_c - C)/y_c$. Now input (x_c, y_c, a) to Algorithm A. According to the assumption of Algorithm A, the solution (x, y) will be output. By Theorem 2.3, the message $M \equiv x - ay$ is discovered.

This concludes the proof. ■

Similarly, we can easily show that the ciphertext attack in Scheme 1 is polynomially reduced to that in the RSA scheme. So, our proposed schemes are as secure as the RSA scheme under the ciphertext attack.

Now, we consider the known-plaintext attacks. Assume the attacker knows one of the messages m_1 and m_2, say m_1, and the corresponding ciphertext (x_c, y_c, a). According to Equation (3.1), he can get the following equation

$$x - a(m_1 - m_2) \equiv m_1 + m_2.$$

But he cannot solve the above equation to get x and another message m_2.

6. Conclusions

We have proposed fast RSA-type schemes based on Pell equations over the ring Z_N^*. The decryption speed of the proposed schemes is about two times faster than that of the RSA scheme for a 2 *log*N-bit long message. Furthermore, the decryption speed of the proposed schemes is somewhat faster than that of Koyama's schemes if the cost of the isomorphic mapping is considered. In addition to the decryption speed, we have shown that the encryption speed of our proposed schemes are even more efficient than that of Koyama's scheme 1. We also prove that the proposed schemes are as secure as the RSA scheme against the ciphertext attack.

References

1. Chiou, C. W. and Yang, T. C. (1994): "Iterative Modular Multiplication Algorithm without Magnitude Comparison," Electronics Letters, Vol.30, No. 24, Nov. 1994, pp. 2017-2018.
2. Demytko, N (1993): "A New Elliptic Curve Based Analogue of RSA," Advances in Cryptology-EUROCRYPT'93 Proceedings, Berlin: Springer-Verlag, 1993, pp. 39-48.
3. Hastad, J.(1985): "On Using RSA with Low Exponent in a Public Key Network," Proc. of CRYPTO'85, springer-verlag, New York, 1986, pp. 403-408.
4. Kaliski Jr. B. S. (1995): "The Montgomery Inverse and Its Applications," IEEE Transactions on Computers, Vol. 44, No. 8, Aug. 1995, pp. 1064-1065.
5. Koyama, K, Maurer, U. M, Okamoto, T., and Vanstone, S. A. (1992): "New Public-Key Schemes Based on Elliptic Curves Over the Ring Z_n," Advances in Cryptology-CRYPTO'91 Proceedings, Berlin: Springer-Verlag, 1992, pp. 252-266.
6. Koyama, K. (1995): "Fast RSA-type Schemes Based on Singular Cubic Curves $y^2 + axy \equiv x^3 \pmod n$," Advances in Cryptology-EUROCRYPT'95 Proceedings, 1995, pp. 329-340.
7. Menezes, A. (1993): Elliptic Curve Public Key Cryptosystems, Boston Kluwer Academic 1993, pp. 57-58.
8. Rivest, R. L., Shamir, A., and Adleman, L.(1978): "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. of the ACM, Vol. 21(2), 1978, pp. 120-126.