การปรับปรุงระบบรหัสลับเอ็ลกามอลไลก์ด้วยตัวดำเนินการทีละบิตแบบเป็นคาบ

An Improvement of ElGamal-like Cryptosystem with Periodic Bitwise Operations

Wanchaloem Nadda[1] and Thotsaphon Thongjunthug[1*]

[1]Department of Mathematics, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand

[*]Corresponding Author, Email: thotho@kku.ac.th

Received: 16 February 2018 | Revised: 31 July 2018 | Accepted: 9 August 2018

บทคัดย่อ

Hwang et al. (2002) ได้นำเสนอระบบรหัสลับเอ็ลกามอลไลก์ ซึ่งมีวัตถุประสงค์เพื่อปรับปรุงประสิทธิภาพของระบบรหัสลับเอ็ลกามอลสำหรับการเข้ารหัสลับข้อความขนาดใหญ่ โดยเฉพาะอย่างยิ่งในแง่ของความซับซ้อนในการคำนวณและหน่วยเก็บข้อความรหัสลับ ต่อมา Wang et al. (2006) ได้พิสูจน์ว่าระบบรหัสลับเอ็ลกามอลไลก์มีความปลอดภัยน้อยกว่าระบบรหัสลับเอ็ลกามอล และนำเสนอวิธีการปรับปรุงเพื่อเพิ่มความปลอดภัย ในบทความวิจัยนี้ จะได้แสดงวิธีการปรับปรุงระบบรหัสลับของ Wang et al. (2006) โดยใช้การดำเนินการทีละบิตที่แตกต่างกันในการเข้ารหัสลับแต่ละบล็อกของข้อความปกติ ซึ่งกำหนดโดยอาศัยลำดับเป็นคาบบางลำดับ ผลการศึกษาแสดงให้เห็นว่า ระบบรหัสลับที่ปรับปรุงใหม่นั้นสามารถเพิ่มความยาวคาบของสัมประสิทธิ์สำหรับการเข้ารหัสลับ และยังสามารถป้องกันการโจมตีแบบทราบข้อความรหัสลับเท่านั้น และการโจมตีแบบทราบข้อความปกติ ได้ดีกว่าระบบรหัสลับของ Wang et al. (2006)

ABSTRACT

Hwang et al. (2002) proposed an ElGamal-like cryptosystem which aimed to improve effectiveness of the ElGamal cryptosystem for encrypting large messages, particularly in terms of computational complexity and the storage of ciphertext. Later, Wang et al. (2006) proved that the ElGamal-like cryptosystem is less secure than the ElGamal cryptosystem, and then proposed an improved version to increase the security. In this paper, we improve the scheme of Wang et al. (2006) by using different bitwise operations, which are assigned according to a certain periodic sequence, while encrypting different blocks of plaintext. The results show that our scheme can provide larger period length of the coefficients for encryption and more resistance to a ciphertext-only attack and a known-plaintext attack than the scheme of Wang et al. (2006).

คำสำคัญ: ระบบรหัสลับแบบกุญแจสาธารณะ ลำดับเป็นคาบ ระบบรหัสลับเอ็ลกามอลไลก์

Keywords: Public-key cryptosystem, Periodic sequence, ElGamal-like cryptosystem

1. INTRODUCTION

The concept of public-key cryptosystem was first introduced by Diffie and Hellman (1976), whose scheme, later known as Diffie-Hellman key exchange method, is based on discrete logarithm problem. ElGamal (1985) proposed another public-key cryptosystem, later known as the ElGamal cryptosystem, which is one of many effective public-key cryptosystems used in practice nowadays. Its security still relies on the difficulty of solving discrete logarithm problem. However, when the ElGamal cryptosystem is used to encrypt large message, its security will decrease, for using the same parameters to encrypt different plaintext makes the cipher vulnerable to a known-plaintext attack (Hwang et al., 2002). Moreover, sending a message using the ElGamal cryptosystem has drawbacks in terms of bandwidth because the length of ciphertext is twice as long as the length the plaintext (Wang et al., 2006).

Hwang et al. (2002) proposed an ElGamal-like cryptosystem for encrypting large messages by dividing a message into several blocks. Their proposed cryptosystem sets only two default parameters and other parameters are calculated from both parameters. Nevertheless, Wang et al. (2006) showed that the ElGamal-like cryptosystem is not as secure as the ElGamal cryptosystem since its default parameters cannot generate all the possible parameters. In particular, the period of the function for calculating parameters is less than $p-1$, where p is a prime used as the modulus in the scheme. Wang et al. (2006) then improved the ElGamal-like cryptosystem in order to increase the period of the function for calculating parameters and to decrease probability of fail case for the decryption. Chang et al. (2012) proved that the scheme of Wang et al. (2006) can be attacked by a chosen-plaintext attack, and then a new scheme was proposed.

In this paper, we will improve the scheme of Wang et al. (2006) in order to increase the period length of the coefficients for encryption, which will provide higher security against a ciphertext-only attack and a known-plaintext attack. Our method relies on the use of different bitwise operations, which are assigned according to a certain periodic sequence, while encrypting different blocks of plaintext.

2. RESEARCH METHODOLOGY

2.1 The cryptosystem of Wang et al. (2006)

We shall first give an overview of the cryptosystem of Wang et al. (2006), which consists of three main parts, namely, key generation, encryption algorithm, and decryption algorithm.

2.1.1 Key generation

The scheme of Wang et al. (2006) generates all private keys and public keys in a similar way to the ElGamal cryptosystem (ElGamal, 1985). The key generation consists of the following steps:

1. Choose a prime number p and a primitive root g modulo p.
2. Suppose that there are n recipients. For $i = 1, 2, \dots, n$, the i^{th} recipient choose a private key $d_i \in \{1, 2, \dots, p-1\}$.
3. For $i = 1, 2, \dots, n$, compute $y_i = g^{d_i} \bmod p$.
4. The public key of the i^{th} recipient is (p, g, y_i) and the corresponding private key is d_i.

2.1.2 Encryption algorithm

To send an encrypted message to the i^{th} recipient using the scheme of Wang et al. (2006), a sender needs to complete the following steps:

1. Divide a large message into t blocks of equal length. Then convert each block into its corresponding integer value, say, $M_1, M_2, \dots, M_t$.

2. Choose session keys $r_1, r_2 \in \{1,2,\dots,p-1\}$ and compute

$$\begin{aligned} b_1 &= g^{r_1} \bmod p, \\ b_2 &= g^{r_2} \bmod p. \end{aligned}$$

3. For $j = 1, 2, \dots, t$, compute the j^{th} ciphertext block C_j by

$$C_j = M_j F_j \bmod p,$$

where

$$F_j = \left(\left(y_i^{r_1} \bmod p \right) \oplus \left(\left(y_i^{r_2} \right)^j \bmod p \right) \right) \bmod p \qquad (1)$$

and $\oplus$ is the bitwise exclusive-or of two integers. We call $F_1, F_2, \dots, F_t$ the coefficients for encryption.

4. The ciphertext is $(b_1, b_2, C_1, C_2, \dots, C_t)$.

2.1.3 Decryption algorithm

Once the ciphertext $(b_1, b_2, C_1, C_2, \dots, C_t)$ encrypted using the scheme of Wang et al. (2006) is received, the i^{th} recipient can decrypt it by computing

$$M_j = C_j F_j^{-1} \bmod p,$$

where F_j^{-1} is the multiplicative inverse of F_j modulo p for all $j = 1, 2, \dots, t$. Note that the i^{th} recipient can compute F_j without any knowledge of the session keys r_1, r_2 set by the sender, for

$$\begin{aligned} F_j &= \left(\left(y_i^{r_1} \bmod p \right) \oplus \left(\left(y_i^{r_2} \right)^j \bmod p \right) \right) \bmod p \\ &= \left(\left(g^{d_i r_1} \bmod p \right) \oplus \left((g^{d_i r_2})^j \bmod p \right) \right) \bmod p \\ &= \left(\left(b_1^{d_i} \bmod p \right) \oplus \left(\left(b_2^{d_i} \right)^j \bmod p \right) \right) \bmod p. \end{aligned}$$

Then the i^{th} recipient converts $M_1, M_2, \dots, M_t$ into blocks of letters and combine them to recover the message.

Unfortunately, the coefficients for encryption F_j defined by (1) may not be invertible modulo p for some $j = 1, 2, \dots, t$. This is one of major drawbacks to be mended in our proposed scheme.

2.2 Our modification

Our modification to the scheme of Wang et al. (2006) consists of the following three main steps:

1. Create a number of different bitwise operations to be used for encrypting different blocks of plaintext.

2. Modify the existing encryption algorithm proposed by Wang et al. (2006) so that using different bitwise operations for encrypting different blocks is allowed.

3. Derive the decryption algorithm associated to our modified encryption algorithm.

2.2.1 Defining bitwise operations

For $k = 0, 1, 2, \dots, 15$, we define a bitwise operation $\oplus_k$ as shown in Table 1. In addition, for all $a, b \in \mathbb{N} \cup \{0\}$, we define

$$a \oplus_k b = \sum_{i=0}^{n-1} (a_i \oplus_k b_i) 2^i \,,$$

where $(a_{n-1}a_{n-2} \dots a_1 a_0)_2$ and $(b_{n-1}b_{n-2} \dots b_1 b_0)_2$ are the binary expansions of a and b, respectively, padded with zero if necessary to make their length equal.

Table 1 Bitwise operations $\oplus_k$ for $k = 0, 1, 2, \dots, 15$

a	b	$a \oplus_0 b$	$a \oplus_1 b$	$a \oplus_2 b$	$a \oplus_3 b$	$a \oplus_4 b$	$a \oplus_5 b$	$a \oplus_6 b$	$a \oplus_7 b$
0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1
a	b	$a \oplus_8 b$	$a \oplus_9 b$	$a \oplus_{10} b$	$a \oplus_{11} b$	$a \oplus_{12} b$	$a \oplus_{13} b$	$a \oplus_{14} b$	$a \oplus_{15} b$
0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

Next, we will describe our encryption and decryption algorithms, where all private keys and public keys are generated in a similar way as in the scheme of Wang et al. (2006).

2.2.2 Encryption algorithm

In our modified cryptosystem, a sender can send an encrypted message to the i^{th} recipient, whose public key is (p, g, y_i), via the following steps:

1. Divide a message into t blocks of equal length. Then convert each block into its corresponding integer value, say, $M_1, M_2, \dots, M_t$.

2. Choose session keys $r_1, r_2 \in \{1, 2, \dots, p-1\}$ and compute

$$\begin{aligned} b_1 &= g^{r_1} \bmod p, \\ b_2 &= g^{r_2} \bmod p. \end{aligned}$$

3. Let $c_1 = y_i^{r_1} \bmod p$ and $c_2 = y_i^{r_2} \bmod p$.

4. For $j = 1, 2, \dots, t$, let

$$a_j = \Big(\big(\big((c_2 + j) \bmod c_1 \big) + \big((c_1 j) \bmod c_2 \big) \big) \bmod 15 \Big) + 1. \tag{2}$$

Observe that $a_j \in \{1, 2, \dots, 15\}$.

5. For $j = 1, 2, \dots, t$, compute

$$F_j = \left(c_1 \oplus_{a_j} \left(c_2^j \bmod p \right) \right) \bmod p. \tag{3}$$

6. For $j = 1, 2, \dots, t$, compute the j^{th} ciphertext block C_j by

$$C_j = \begin{cases} (M_j + F_j) \bmod p & \text{if } F_j \text{ is even,} \\ M_j F_j \bmod p & \text{if } F_j \text{ is odd.} \end{cases} \tag{4}$$

7. The ciphertext is $(b_1, b_2, C_1, C_2, \dots, C_t)$.

2.2.3 Decryption algorithm

In our scheme, the ciphertext $(b_1, b_2, C_1, C_2, \dots, C_t)$ can be decrypted by the i^{th} recipient via the following steps:

1. Compute c_1 and c_2 using the fact that

$$c_1 = y_i^{r_1} \bmod p \ = g^{d_i r_1} \bmod p = b_1^{d_i} \bmod p,$$
$$c_2 = y_i^{r_2} \bmod p \ = g^{d_i r_2} \bmod p = b_2^{d_i} \bmod p.$$

2. For $j = 1, 2, \dots, t$, define a_j as in (2).
3. For $j = 1, 2, \dots, t$, compute F_j as in (3).
4. For $j = 1, 2, \dots, t$, compute

$$M_j = \begin{cases} \left(C_j - F_j\right) \bmod p & \text{if } F_j \text{ is even,} \\ \left(C_j F_j^{-1}\right) \bmod p & \text{if } F_j \text{ is odd.} \end{cases} \tag{5}$$

5. Convert all blocks M_j into blocks of letters and combine them to form the message.

One major advantage of our scheme is that every block of ciphertext can be decrypted regardless of the multiplicative invertibility of F_j. To be precise, if F_j is odd, then F_j^{-1} modulo p always exists and so M_j can be obtained. On the other hand, if $F_j = 0$, then both M_j and C_j are identical.

3. RESULTS

In this section, we will prove some number-theoretic results which are essential to the determination of the period length of the coefficients for encryption, and then illustrate some examples of encryption and decryption using our scheme.

Theorem 1. *For $c_1, c_2 \in \mathbb{N}$, let $m = \frac{c_1 c_2}{\gcd(c_1^2, c_2)}$. Then m is the smallest positive integer such that $c_1 \mid m$ and $c_2 \mid c_1 m$.*

Proof. Since $m = \frac{c_1 c_2}{\gcd(c_1^2, c_2)}$ and $\gcd(c_1^2, c_2) \mid c_2$, we have $\frac{c_2}{\gcd(c_1^2, c_2)} \in \mathbb{N}$ and so $c_1 \mid m$. Moreover, since $c_1 m = \frac{c_1^2 c_2}{\gcd(c_1^2, c_2)}$ and $\gcd(c_1^2, c_2) \mid c_1^2$, we have $\frac{c_1^2}{\gcd(c_1^2, c_2)} \in \mathbb{N}$ and so $c_2 \mid c_1 m$.

Let $n \in \mathbb{N}$ such that $c_1 \mid n$ and $c_2 \mid c_1 n$. Then $n = c_1 k$ for some $k \in \mathbb{N}$ and so $c_1 n = c_1^2 k$. Since $c_2 \mid c_1 n$, we have $c_1 n = c_2 k'$ for some $k' \in \mathbb{N}$. Hence,

$$c_1^2 k = c_2 k'. \tag{6}$$

Let $d = \gcd(c_1^2, c_2)$. Then $c_1^2 = dA$ and $c_2 = dB$ for some $A, B \in \mathbb{N}$ with $\gcd(A, B) = 1$. From (6), we have

$$\begin{aligned} dAk &= dBk' \\ Ak &= Bk', \end{aligned}$$

that is, $B \mid Ak$. Since $\gcd(A, B) = 1$, it follows that $B \mid k$. Thus $k = k''B$ for some $k'' \in \mathbb{N}$. This implies that

$$n = c_1 k = c_1(k''B) = k''\left(\frac{c_1 c_2}{d}\right) = k''\left(\frac{c_1 c_2}{\gcd(c_1^2, c_2)}\right) = k''m,$$

and so $m \mid n$. Thus m is the smallest positive integer such that $c_1 \mid m$ and $c_2 \mid c_1 m$. ❑

Theorem 2. *For $b, c_1, c_2, j \in \mathbb{N}$, let*

$$a_j = \Big(\big((c_2 + j) \bmod c_1\big) + \big((c_1 j) \bmod c_2\big)\Big) \bmod b$$

and $m = \frac{c_1 c_2}{\gcd(c_1^2, c_2)}$. Then $a_j = a_{j+m}$ for all $j \in \mathbb{N}$. In other words, the period length of the sequence $\{a_j\}_{j=1}^{\infty}$ is a factor of m.

Proof. For all $j \in \mathbb{N}$, we have

$$a_{j+m} = \left(\left(\left(c_2 + (j+m)\right) \bmod c_1\right) + \left(\left(c_1(j+m)\right) \bmod c_2\right)\right) \bmod b.$$

By Theorem 1, we have $c_1 \mid m$ and $c_2 \mid c_1 m$. Hence,

$$a_{j+m} = \left(\left((c_2 + j) \bmod c_1\right) + \left((c_1 j) \bmod c_2\right)\right) \bmod b = a_j. \qquad ❑$$

The next examples illustrate how encryption and decryption is done using our scheme.

Example 1. To encrypt the message "PASSWORD_IS_AB01" using our scheme with public key $(p, g, y_1) = (16487, 5, 14216)$, the sender must first choose session keys r_1, r_2. Here, we suppose that $r_1 = 11237$ and $r_2 = 8600$.

Suppose that the sender splits the message into eight blocks of two letters and uses the American Standard Code for Information Interchange (ASCII) table (Weiman, 2012) for conversion. Then $M_1, M_2, \ldots, M_8$ can be computed as shown in Table 2.

Table 2 Conversion of blocks of plaintext into integers

j	Letter	ASCII code	M_j
1	"PA"	$(80, 65)$	$80(128) + 65 = 10305$
2	"SS"	$(83, 83)$	$83(128) + 83 = 10707$
3	"WO"	$(87, 79)$	$87(128) + 79 = 11215$
4	"RD"	$(82, 68)$	$82(128) + 68 = 10564$
5	"_I"	$(95, 73)$	$95(128) + 73 = 12233$
6	"S_"	$(83, 95)$	$83(128) + 95 = 10719$
7	"AB"	$(65, 66)$	$65(128) + 66 = 8386$
8	"01"	$(48, 49)$	$48(128) + 49 = 6193$

Next, the sender calculates

$$b_1 = g^{r_1} \bmod p = 434, \quad b_2 = g^{r_2} \bmod p = 6453,$$
$$c_1 = y_1^{r_1} \bmod p = 3251, \quad c_2 = y_1^{r_2} \bmod p = 10298.$$

For $j = 1, 2, \ldots, 8$, the sender computes a_j, F_j, and C_j using (2), (3), and (4), respectively, as shown in Table 3. Thus, the ciphertext is $(434, 6453, 16458, 6684, 7860, 13812, 7143, 15933, 12493, 3563)$.

Table 3 Encryption of $M_1, M_2, \ldots, M_8$ using our scheme

j	M_j	a_j	F_j	C_j
1	10305	3	3251	16458
2	10707	15	8191	6684
3	11215	12	13132	7860
4	10564	1	3248	13812
5	12233	13	15311	7143
6	10719	10	5214	15933
7	8386	14	8013	12493
8	6193	11	3323	3563

Example 2. To decrypt the ciphertext

$$(434, 6453, 16458, 6684, 7860, 13812, 7143, 15933, 12493, 3563)$$

obtained from Example 1 using our scheme, the recipient first computes c_1 and c_2 using b_1, b_2 obtained from the ciphertext and his private key, say, d_1. Here, one can verify that $d_1 = 9253$ and

$$c_1 = b_1^{d_1} \bmod p = 3251, \;\; c_2 = b_2^{d_1} \bmod p = 10298.$$

For $j = 1, 2, \dots, 8$, the recipient computes a_j, F_j, and M_j using (2), (3), and (5), respectively, as shown in Table 4. Converting each M_j to base 128 and using the ASCII table (Weiman, 2012), the recipient obtains blocks of decrypted message as in Table 5. Thus, the message “PASSWORD_IS_AB01” is recovered.

Table 4 Decryption of $C_1, C_2, \dots, C_8$ using our scheme

j	C_j	a_j	F_j	M_j
1	16458	3	3251	10305
2	6684	15	8191	10707
3	7860	12	13132	11215
4	13812	1	3248	10564
5	7143	13	15311	12233
6	15933	10	5214	10719
7	12493	14	8013	8386
8	3563	11	3323	6193

Table 5 Conversion integers into blocks of plaintext

j	M_j	ASCII code	Letters
1	10305	$(80, 65)$	“PA”
2	10707	$(83, 83)$	“SS”
3	11215	$(87, 79)$	“WO”
4	10564	$(82, 68)$	“RD”
5	12233	$(95, 73)$	“_I”
6	10719	$(83, 95)$	“S_”
7	8386	$(65, 66)$	“AB”
8	6193	$(48, 49)$	“01”

4. DISCUSSION

4.1 The period length of coefficients for encryption

For the scheme of Wang et al. (2006), recall from (1) that the j^{th} coefficient for encryption is defined by

$$F_j = \left(\left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^j \bmod p\right)\right) \bmod p.$$

It is obvious that the period of the sequence $\{F_j\}_{j=1}^{\infty}$ is equal to the order of $y_i^{r_2}$ modulo p, that is, the smallest positive integer k such that $\left(y_i^{r_2}\right)^k \equiv 1 \bmod p$ (Burton, 2007). Since $y_i^{r_2} \equiv g^{d_i r_2} \pmod p$ where g is a primitive root modulo p, it follows from elementary number theory that such order equals $\frac{p-1}{\gcd\,(d_i r_2, p-1)}$ (Burton, 2007). This implies that the sequence $\{F_j\}_{j=1}^{\infty}$ cannot generate all elements in $\{1, 2, \dots, p-1\}$ unless $\gcd(d_i r_2,\ p-1) = 1$. In fact, there are only $\phi(p-1)$ elements in $\{1, 2, \dots, p-1\}$ which can be chosen as r_2 and d_i in order to make $\gcd(d_i r_2,\ p-1) = 1$, where $\phi : \mathbb{N} \to \mathbb{N}$ is the Euler's phi-function (Burton, 2007).

In contrast, recall from (2) and (3) that the j^{th} coefficient for encryption of our scheme is

$$F_j = \left(c_1 \oplus_{a_j} \left(c_2^j \bmod p\right)\right) \bmod p,$$

where

$$a_j = \Big(\big((c_2 + j) \bmod c_1\big) + \big((c_1 j) \bmod c_2\big)\Big) \bmod 15 + 1$$

with $c_1 = y_i^{r_1} \bmod p$ and $c_2 = y_i^{r_2} \bmod p$. It is easy to see that the period length of the sequence $\{F_j\}_{j=1}^{\infty}$ is now equal to $\operatorname{lcm}\left(\frac{p-1}{\gcd(d_i r_2, p-1)}, m\right)$, where m is the period length of the sequence $\{a_j\}_{j=1}^{\infty}$. By Theorem 2, we know that $m = \frac{c_1 c_2}{\gcd(c_1^2, c_2)}$ is the best-case scenario. Thus, the sequence of the coefficients for encryption of our scheme can have larger period length than that of the scheme of Wang et al. (2006).

4.2 A ciphertext-only attack

A ciphertext-only attack is an attack where an opponent possesses only the encryption algorithm and a ciphertext (Stallings, 2011). Chang et al. (2012) analyzed the scheme of Wang et al. (2006) using the following theorem on the Legendre symbol.

Theorem 3 (Chang et al., 2012). *There exists a prime number p which satisfies the following conditions for all $a, b \in \{1, 2, \dots, p-1\}$:*

1. *If $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$, then $(a \oplus b) \bmod p$ is either zero or a quadratic non-residue of p.*
2. *If $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -1$, then $(a \oplus b) \bmod p$ is either zero or a quadratic residue of p.*

Since the key (p, g, y_i) is publicly known, an opponent can find $\left(\frac{g}{p}\right)$ and $\left(\frac{y_i}{p}\right)$. Moreover, the opponent can see b_1 and b_2 from the ciphertext and then find $\left(\frac{b_1}{p}\right)$ and $\left(\frac{b_2}{p}\right)$. Since $b_1 = g^{r_1} \bmod p$ and $b_2 = g^{r_2} \bmod p$, the opponent can also determine the parity of the session keys r_1 and r_2, which will lead to successful determination of $\left(\frac{y_i^{r_1} \bmod p}{p}\right)$ and $\left(\frac{y_i^{r_2} \bmod p}{p}\right)$.

In the scheme of Wang et al. (2006), if p satisfies Theorem 3, then the opponent can find $\left(\frac{F_j}{p}\right)$ for all $j = 1, 2, \dots, t$, where F_j is defined as in (1), that is,

$$F_j = \Big(\big(y_i^{r_1} \bmod p\big) \oplus \big((y_i^{r_2})^j \bmod p\big)\Big) \bmod p.$$

Recall that $C_j = M_j F_j$. Since the opponent knows C_j for all $j = 1, 2, \dots, t$, each $\left(\frac{M_j}{p}\right)$ can be found using the multiplicative property of the Legendre symbol (Burton, 2007), that is,

$$\left(\frac{C_j}{p}\right) = \left(\frac{M_j}{p}\right)\left(\frac{F_j}{p}\right).$$

In our scheme, however, even when the public key and the ciphertext are known, the opponent still cannot determine $\left(\frac{M_j}{p}\right)$. This is because we use two operations, namely, addition and multiplication, for encryption (see (4)) and the opponent does not know which operation is used when each block of plaintext is encrypted.

4.3 A known-plaintext attack

A known-plaintext attack is an attack where an opponent possesses one or more plaintext-ciphertext pairs in addition to the encryption algorithm and the ciphertext (Stallings, 2011). Apart from the public key (p, g, y_i), now we suppose that the opponent knows the ciphertext $(b_1, b_2, C_1, C_2, \dots, C_t)$ and two blocks of plaintext, say, M_m and M_n for some $m, n \in \{1, 2, \dots, t\}$ with $m \neq n$.

For $j = 1, 2, \dots, t$, recall that the j^{th} block of ciphertext in the scheme of Wang et al. (2006) is

$$\begin{aligned} C_j &= M_j\left(\left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^j \bmod p\right)\right) \bmod p \\ C_jM_j^{-1} \bmod p &= \left(\left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^j \bmod p\right)\right) \bmod p. \end{aligned}$$

Since $0 \leq \left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^j \bmod p\right) \leq 2p$, we have

$$C_jM_j^{-1} \bmod p = \left(\left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^j \bmod p\right)\right) - k_jp \tag{7}$$

where

$$k_j = \begin{cases} 0 & \text{if } 0 \leq \left(\left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^j \bmod p\right)\right) < p, \\ 1 & \text{if } p \leq \left(\left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^j \bmod p\right)\right) < 2p. \end{cases} \tag{8}$$

For $j = m$, we have

$$\left(C_mM_m^{-1} \bmod p\right) + k_mp = \left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^m \bmod p\right). \tag{9}$$

Similarly, for $j = n$, we have

$$\left(C_nM_n^{-1} \bmod p\right) + k_np = \left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^n \bmod p\right). \tag{10}$$

Computing the exclusive-or of (9) and (10), we have

$$\begin{aligned} &\left(\left(C_mM_m^{-1} \bmod p\right) + k_mp\right) \oplus \left(\left(C_nM_n^{-1} \bmod p\right) + k_np\right) \\ &\quad = \left(\left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^m \bmod p\right)\right) \oplus \left(\left(y_i^{r_1} \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^n \bmod p\right)\right) \\ &\quad = \left(\left(y_i^{r_2}\right)^m \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^n \bmod p\right). \end{aligned}$$

Hence, we can change from solving Diffie-Hellman problem to solving the exclusive-or equation.

Since the exclusive-or operation behaves somewhat similar to addition or subtraction, we can rewrite the exclusive-or operation of integers a, b as $a \oplus b = a + b - 2\Omega(a,b)$ for some $\Omega(a,b) \in \mathbb{Z}$ with $0 \leq \Omega(a,b) \leq \min\,(a,b)$. In the scheme of Wang et al. (2006), if d_i, r_1, r_2 are not well selected, that is,
$\left(\left(y_i^{r_2}\right)^m \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^n \bmod p\right) = \left(\left(y_i^{r_2}\right)^m \bmod p\right) + \left(\left(y_i^{r_2}\right)^n \bmod p\right)$,
then one can find $y_i^{r_2} \bmod p$ by solving the equation

$$A_{m,n} = \left(\left(y_i^{r_2}\right)^m \bmod p\right) + \left(\left(y_i^{r_2}\right)^n \bmod p\right), \tag{11}$$

where

$$A_{m,n} = \left(\left(C_mM_m^{-1} \bmod p\right) + k_mp\right) \oplus \left(\left(C_nM_n^{-1} \bmod p\right) + k_np\right)$$

and k_m, k_n are chosen from the set $\{0,1\}$. If (11) has no solution, then we will choose new $k_m, k_n \in \{0,1\}$ and try again. If (11) has no solution for all $k_m, k_n \in \{0,1\}$, then this implies that
$\left(\left(y_i^{r_2}\right)^m \bmod p\right) \oplus \left(\left(y_i^{r_2}\right)^n \bmod p\right) \neq \left(\left(y_i^{r_2}\right)^m \bmod p\right) + \left(\left(y_i^{r_2}\right)^n \bmod p\right)$.
However, if (11) has a solution, then we will obtain the value of $y_i^{r_2} \bmod p$ and thus the value of $y_i^{r_1} \bmod p$. In particular, if $y_i^{r_1} \bmod p$ and $y_i^{r_2} \bmod p$ satisfy (8) and (7), then they are likely to be used for encryption.

In our scheme, however, even when the public key, the ciphertext, and the plaintext are known, the opponent still cannot find $y_i^{r_1} \bmod p$ and $y_i^{r_2} \bmod p$. Again, this is because we use addition, multiplication, and 15 bitwise operations, namely, $\oplus_1, \oplus_2, \ldots, \oplus_{15}$, for encryption. The opponent also does not know which operation is used when each block of plaintext is encrypted.

5. CONCLUSIONS

In this paper, we propose a modification of the cryptosystem developed by Wang et al. (2006). Our methodology uses the periodic sequence $\{a_j\}_{j=1}^{\infty}$, where a_j is defined by

$$a_j = (((c_2 + j) \bmod c_1 + (c_1 j) \bmod c_2) \bmod 15) + 1,$$

to select the bitwise operation $\bigoplus_{a_j}$ for encrypting the j^{th} block of plaintext. The results show that the period length of the sequence $\{F_j\}_{j=1}^{\infty}$ of our scheme is equal to $\operatorname{lcm}\left(\frac{p-1}{\gcd(d_i r_2, p-1)}, m\right)$, where m is the period length of the sequence $\{a_j\}_{j=1}^{\infty}$. For the best-case scenario, we have $m = \frac{c_1 c_2}{\gcd(c_1^2, c_2)}$. In contrast, the period length of $\{F_j\}_{j=1}^{\infty}$ provided by the scheme of Wang et al. (2006) is merely equal to $\frac{p-1}{\gcd(d_i r_2, p-1)}$. Moreover, we find that our scheme can provide higher security against a ciphertext-only attack and a known-plaintext attack than the scheme of Wang et al. (2006).

6. ACKNOWLEDGEMENTS

The authors would like to thank the Department of Mathematics, Faculty of Science, Khon Kaen University for supporting facilities towards this research. In addition, the first author is indebted to the Development and Promotion of Science and Technology Talents Project (DPST) for sponsoring his scholarship.

7. REFERENCES

Burton, D.M. (2007). Elementary Number Theory. (6th ed.) New York: McGraw-Hill. pp. 131-176.

Chang, T.Y., Hwang, M.S. and Yang, W.P. (2012). Cryptanalysis on an improved version of ElGamal-like public-key encryption scheme for encrypting large message. Informatica (Vilnius) 23(4): 537-562.

Diffie, W. and Hellman, M.E. (1976). New directions in cryptography. IEEE Trans Inform Theory. 22(6): 644-654.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inform Theory. 31(4): 469-472.

Hwang, M.S., Chang, C.C. and Hwang, K.F. (2002). An ElGamal-like cryptosystem for enciphering large messages. IEEE Trans Knowl Data Eng. 14(2): 445-446.

Stallings, W. (2011). Cryptography and Network Security: Principles and Practice. (5th ed.). Upper Saddle River: Pearson Education. p. 36.

Wang, M.N., Yen, S.M., Wu, C.D. and Lin, C.T. (2006). Cryptanalysis on an ElGamal-like cryptosystem for encrypting large messages. In: Proceeding of the 6th WSEAS International Conference on Applied Informatics and Communications (AIC'06), 18-20 August 2006, Elounda, Crete, Greece. Lazakidou A. and Siassiakos, K. (eds.). World Scientific and Engineering Academy and Society, Stevens Point. 418-422.

Weiman, D. (2012). Decimal-Binary-Octal-Hex-ASCII Conversion Chart. The University of Delaware, Source: http://www.eecis.udel.edu/~amer/CISC651/ASCII-Conversion-Chart.pdf. Accessed 20 January 2018.

❑❑❑❑❑