Malaysian Journal of Mathematical Sciences 7(S): 1-17 (2013)
Special Issue: The 3rd International Conference on Cryptology & Computer Security 2012 (CRYPTOLOGY2012)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

On the Hastad's Attack to $LUC_{4,6}$ Cryptosystem and Compared with Other RSA-Type Cryptosystem

[1,2*]Wong Tze Jin, [3]Hailiza Kamarulhaili and [2,4]Mohd. Rushdan Md Said

[1]*Department of Basic Science and Engineering, Faculty of Agriculture and Food Sciences, Universiti Putra Malaysia Bintulu Campus, 97008 Bintulu, Sarawak, Malaysia*

[2]*Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*

[3]*School of Mathematical Sciences, Universiti Sains Malaysia, 11800 Pulau Pinang, Penang, Malaysia*

[4]*Department of Mathematics, Faculty of Sciences, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia*

E-mail: sherlock.wong.tj@gmail.com

*Corresponding author

ABSTRACT

The $LUC_{4,6}$ cryptosystem is a system analogy to RSA cryptosystem and extended from LUC and LUC_3 cryptosystems. Therefore, the security problem of the $LUC_{4,6}$ cryptosystem is based on integer factorization which is similar to RSA, LUC and LUC_3 cryptosystems. The Hastad's attack is one of the polynomial attack which relied on the polynomial structure of RSA-type cryptosystem. In this paper, Hastad's Theorem will be used to solve a system of multivariate modular equations and Coppersmith Theorem will be used to find a root of a modular equation. Thus, the number of plaintexts which are required to succeed the attack can be found.

Keywords: Hastad's Theorem, Coppersmith Theorem, Lucas Sequence, Dickson Polynomial.

1. INTRODUCTION

The fourth and sixth order of LUC cryptosystem or $LUC_{4,6}$ cryptosystem (Wong (2007) had been proposed in 2007. This cryptosystem is analogous to the RSA cryptosystem and extended from LUC and LUC_3 cryptosystems. The $LUC_{4,6}$ cryptosystem was derived from the fourth order linear recurrence relation which is related to Quartic polynomial and based on the Lucas function.

The security problem for $LUC_{4,6}$ cryptosystem is based on integer factorization which is similar to RSA (Rivest, Shamir and Adleman (1978)), LUC (Smith and Lennon (1993)) and LUC_3 cryptosystems [Said and John]. The Hastad's attack is one of the polynomial attack which relied on the polynomial structure of RSA-type cryptosystem. Therefore, the Hastad's attack is able to solve the underlying intractable problem which the attack do not factor the RSA- modulus, n for the $LUC_{4,6}$ cryptosystem directly. It used the other solution to recover the plaintext.

In 1986, Hastad showed that using RSA with low public exponent is insecure if the users are sending linearly related plaintexts over a large network (Hastad (1986)). Therefore, Hastad develop a technique to solve a system of univariate modular equations to succeed his attack. Besides that, Coppersmith proposed a new method for finding a root of a modular equation (Coppersmith (1996)), which turned out to be a better way to succeed a successful attack in 1996.

In this paper, the Hastad's attack will be attack on the RSA, LUC and LUC_3 cryptosystems, and extended on the $LUC_{4,6}$ cryptosystem. The cryptosystem will be presented in Section 2. The theorems which are used in the attack will be presented in Section 3. In section 4, the Hastad's attack will be proposed and discussed. Finally, the conclusion had been make in the last section.

2. THE CRYPTOSYSTEM

2.1 RSA Cryptosystem

In the RSA cryptosystem, a plaintext M can use an encryption key (e,n) to encrypt it become a ciphertext C. The encryption process as follows.

First, the user can use any standard representation to represent the plaintext as an integer between 0 and $n-1$. The purpose is getting the plaintext in the numeric form for process encryption used.

Then, the user encrypt the plaintext, M become ciphertext, C. The encryption algorithm defined as

$$E(M) = C \equiv M^e \bmod n \tag{1}$$

When the receiver want to decrypt the ciphertext, the user must has a decryption key denote by $d \equiv e^{-1} \bmod \phi(n)$, where $n = pq$ and Euler function, $\phi(n) = (p-1)(q-1)$. Then, the decryption algorithms defined as

$$D(C) \equiv C^d \bmod n\,. \tag{2}$$

Note that, the encryption key, e must be relative prime to $p-1$ and $q-1$. By the extended Euclidean algorithm, the decryption key, d can be compute as follows.

$$\gcd(d, (p-1)(q-1)) = 1, \tag{3}$$

$$ed \equiv 1 \bmod (p-1)(q-1). \tag{4}$$

where *gcd* is greatest common divisor and d, n are also relatively prime.

2.2 LUC Cryptosystem

Let n be the product of two different odd primes, p and q, and the number e must be relatively primes to $p-1$, $p+1$, $q-1$ and $q+1$. The encryption process of LUC cryptosystem can be defined as

$$E(M) = C \equiv V_e(M,1) \bmod n, \tag{5}$$

where $V_e(M,1)$ is second order Lucas sequence, M is the plaintext and C is the ciphertext.

The corresponding decryption key, d can be generated by

$$ed \equiv 1 \bmod S(n), \tag{6}$$

where $S(n) = (p - (\frac{D}{p}))(q - (\frac{D}{q}))$, $D = C^2 - 4$, and $(\frac{D}{p}))$, $(\frac{D}{q})$ are the Legendre symbols of D with respect to p and q. Therefore, there are four possible decryption keys,

$$d \equiv e^{-1} \bmod \big((p+1)(q+1)\big), \tag{7}$$

$$d \equiv e^{-1} \bmod \left((p+1)(q-1)\right), \tag{8}$$

$$d \equiv e^{-1} \bmod \left((p-1)(q+1)\right), \tag{9}$$

$$d \equiv e^{-1} \bmod \left((p-1)(q-1)\right). \tag{10}$$

The decryption process is similar to the encryption process, with e replaced by d and M replaced by C.

$$M \equiv V_d(C,1) \bmod n. \tag{11}$$

2.3 LUC$_3$ Cryptosystem

As in the RSA and LUC cryptosystems, the Cubic analogue to the RSA cryptosystem or LUC$_3$ cryptosystem has a number n or we called RSA-modulus which is the product of two prime numbers p and q. In the encryption process, the encryption key, e must chosen be relatively prime to the Euler totient function $\Phi(n) = \overline{p}\overline{q}$ because it is necessary to solve the congruence $ed \equiv 1 \bmod \Phi(n)$ to find the decryption key d.

The Euler totient function is defined as

$$\Phi(n) = p_1^{b_1-1}\overline{p_1} \cdot p_2^{b_2-1}\overline{p_2} \cdots p_r^{b_r-1}\overline{p_r}, \tag{12}$$

where

$$\overline{p_i} = \begin{cases} p_i^2 + p_i + 1, & \text{if } f(x) \text{ is of type } t[3] \bmod p_i \\ p_i^2 - 1, & \text{if } f(x) \text{ is of type } t[2,1] \bmod p_i, \\ p_i - 1, & \text{if } f(x) \text{ is of type } t[1] \bmod p_i \end{cases} \tag{13}$$

In practice, since $\Phi(n)$ depends on the type of an auxiliary polynomial, we choose e prime to $p-1, q-1, p+1, q+1, p^2+p+1$ and q^2+q+1 to cover all possible cases.

The LUC$_3$ cryptosystem is set up based on the third order Lucas sequence V_n derived from the cubic polynomial $x^3 - M_1x^2 + M_2x - 1 = 0$, where M_1 M_1 and M_2 constitutes the plaintexts. Then, the encryption function is defined by

$$E(M_1,M_2)=\left(V_e(M_1,M_2,1),V_e(M_2,M_1,1)\right)\equiv(C_1,C_2)\bmod n, \tag{14}$$

where $n=pq$ as above, $V_e(M_1,M_2,1)$ and $V_e(M_2,M_1,1)$ are the e-th term of the third order Lucas sequence defined by

$$V_k(x_1,x_2,1)\equiv x_1V_k(x_1,x_2,1)-x_2V_k(x_1,x_2,1)+V_k(x_1,x_2,1)\bmod n\ , \tag{15}$$

with initial values $V_0=3,\ V_1=x_1$ and $V_2=x_1^2-2x_2$.

The decryption key is (d,n) where d is the inverse of e modulo $\Phi(n)$. To decrypt the plaintext, the receiver must know or be able to compute $\Phi(n)$ and then calculate

$$D(C_1,C_2)=\left(V_d(C_1,C_2,1),V_d(C_2,C_1,1)\right)\equiv(M_1,M_2)\bmod n, \tag{16}$$

which recovers the original plaintext (M_1,M_2).

2.4 LUC$_{4,6}$ Cryptosystem

A fourth order linear recurrence of Lucas function is a sequence of integers V_k defined by

$$V_k=\sum_{i=1}^{4}(-1)^{i+1}a_iV_{k-i}, \tag{17}$$

with initial values $V_0=4,\ V_1=a_1,\ V_2=a_1^2-2a_2$ and $V_3=a_1^3-3a_1,\ a_2+3a_3$, and a_i are coefficients in quartic polynomial,

$$x^4-a_1x^3+a_2x^2-a_3x+a_4=0, \tag{18}$$

Therefore, the encryption function for the LUC4.6 cryptosystem is defined as

$$\begin{aligned}&E(M_1,M_2,M_3)\\&\quad\equiv(V_e(M_1,M_2,M_3,1),\\&\qquad V_e(M_2,M_1M_3-1,M_1^2+M_3^2-2M_2,M_1M_3-1,M_2,1),\\&\qquad V_e(M_3,M_2,M_1,1))\ \text{mod}\ n\\&\quad\equiv(C_1,C_2,C_3)\ \text{mod}\ n,\end{aligned} \tag{19}$$

where $n = pq$, (M_1, M_2, M_3) constitute the plaintexts and the encryption key, e relative prime to $p - 1$, $q - 1$, $p + 1$, $q + 1$, $p^2 + p + 1$, $q^2 + q + 1$, $p^3 + p^2 + p + 1$, and $q^3 + q^2 + q + 1$. Besides that, $V_e(M_1, M_2, M_3, 1)$ and $V_e(M_3, M_2, M_1, 1)$ are the e-th term of the fourth order Lucas sequence and $V_e(M_2, M_1M_3 - 1, M_1^2 + M_3^2 - 2M_2, M_1M_3 - 1, M_2, 1)$ is e-th term of the sixth order Lucas sequence.

To decipher the plaintexts, the receiver must know or be able to compute the Euler totient function $\Phi(n)$ for the purpose to compute the decryption key is (d, n) where d is the inverse of e mod $\Phi(n)$. The Euler totient function $\Phi(n)$ for this case can be defined as

$$\Phi(n) = \overline{p} \cdot \overline{q}, \qquad (20)$$

where

$$\overline{p} = \begin{cases} p^3 + p^2 + p + 1, & \text{if } f(x) \bmod p \text{ is an irreducible quartic polynomial} \\ p^3 - 1, & \text{if } f(x) \bmod p \text{ is an irreducible cubic polynomial times a linear factor} \\ p^2 - 1, & \text{if } f(x) \bmod p \text{ is an irreducible quadratic polynomial times two linear factors} \\ p + 1, & \text{if } f(x) \bmod p \text{ is two irreducible quadratic polynomials} \\ p - 1, & \text{if } f(x) \bmod p \text{ is four linear factors} \end{cases}, \qquad (21)$$

with $f(x) = x^4 - C_1x^3 + C_2x^2 - C_3x + 1$. Similarly for $\overline{q}$.

Thus, the decryption function define as

$$\begin{aligned} & D(C_1, C_2, C_3) \\ & \quad \equiv (V_d(C_1, C_2, C_3, 1), \\ & \qquad V_d(C_2, C_1C_3 - 1, C_1^2 + C_3^2 - 2C_2, C_1C_3 - 1, C_2, 1),, \qquad (22) \\ & \qquad V_d(C_3, C_2, C_1, 1)) \bmod n \\ & \quad \equiv (M_1, M_2, M_3) \bmod n, \end{aligned}$$

which recovers the original plaintexts (m_1, m_2, m_3).

3. METHODOLOGY

The Hastad's attack is used Hastad's Theorem to show that using RSA with low public exponent is insecure if the users are sending linearly related plaintexts over a large network (Hastad (1986)).

Theorem 1 (Hastad's Theorem)

Let $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1 \le i \le k} n_i$. Given a set of k equations $\sum_{j=0}^{\delta} a_{i,j} x^j \equiv 0 \bmod n_i$ where the moduli n_i are pairwise relatively prime and $\gcd\left(\left\langle a_{i,j} \right\rangle_{j=0}^{\delta}, n_i\right) = 1$ for all i. Then it is possible to find $x < n$ in polynomial time if $N > 2^{(\delta+1)(\delta+2)/4} (\delta+1)^{\delta+1} n^{\delta(\delta+1)/2}$.

Proof . See Joye (1997), Corollary 3.2.■

In 1996, Coppersmith extended the result from Hastad's theorem that eventually becomes the Coppersmith's theorem (Coppersmith (1996)). This theorem is specific for a monic integer polynomial of degree δ.

Theorem 2 (Coppersmith's Theorem)

Let a monic integer polynomial $P(x)$ of degree δ and a positive integer N of unknown factorization. In time polynomial in $\log N$ and δ, we can find all integer solutions x_0 to $P(x_0) \equiv 0 \bmod N$ with $|x_0| < N^{1/\delta}$.

Proof: See Coppersmith (1996), Corollary 2.■

Joye (1997) had improved the Hastad's theorem as follows.

Theorem 3. Consider a system of k modular polynomial equations of degree $\le \delta$ with l variables given by

$$\sum_{j_1, j_2, \ldots, j_l = 0}^{j_1 + j_2 + \cdots + j_l \le \delta} a_{i, j_1, j_2, \ldots, j_l} x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \equiv 0 \bmod n_i , \qquad (22)$$

for i = 1, … , k and where x_1, … , $x_l < n$ and $n = \min_{1 \le i \le k} n_i$. Let $N = \prod_{i=1}^{k} n_i$, $f = \sum_{m=1}^{\delta} m \binom{m+l-1}{m}$ and $g = \sum_{m=0}^{\delta} \binom{l+m-1}{m}$, if the moduli n_i are coprime, then $\gcd\left(\left\langle a_{i,j_1,j_2,\ldots,j_l}\right\rangle_{j_1,j_2,\ldots,j_l}^{j_1+j_2+\cdots+j_l\le\delta}, n_i\right)=1$ for $i = 1,\ldots, k$ and if

$$N > 2^{g(g+1)/4} g^g n^f , \quad (23)$$

the result is in polynomial time a real-valued equation which is equivalent to Equation (23).

Proof. See Joye (1997), Theorem 3.1.■

4. HASTAD'S ATTACK

4.1 Attack on the RSA Cryptosystem

Suppose that m is the plaintext of RSA cryptosystem. Let $N = \sum_{i=1}^{k} n_i$, where $(n_i, n_j) = 1$, for $i \neq j$, then the corresponding ciphertexts are $c_i \equiv M^e \bmod n_i$.

We can find $C \equiv M^e \bmod N$ by Chinese remainder theorem.

$$C \equiv \sum_{i=1}^{k} c_i u_i \bmod N , \quad (24)$$

where $u_j \equiv \delta_{ij} \bmod n_i$. However, since $C < N$, it can be recovered.

Corollary 1. In the RSA cryptosystem, a set of k linearly related plaintexts can be recovered if $k > e(e+1)/2$ and $n_i > 2^{(e+1)(e+2)/4}(e+1)^{e+1}$.

Proof. See (Joye 1997), Corollary 3.3. ■

4.2 Attack on the LUC Cryptosystem

In 1995, Pinch extend the Hastad's attack to the LUC cryptosystem (Pinch (1995)). Suppose that $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1\le i\le k} n_i$. Let M is the plaintext of LUC cryptosystem, then $m_i \equiv \alpha_i M + \beta_i \bmod n_i$ and the ciphertext, $c_i \equiv V_{e_i}(\alpha_i M + \beta_i, 1) \bmod n_i$. The Dickson polynomial (Lidl (1993)) and Lucas sequence are equality already proved by Lidl.

Therefore,

$$V_{e_i}(\alpha_i M + \beta_i, 1) \equiv D_{e_i}(\alpha_i M + \beta_i, 1) \bmod n_i, \tag{25}$$

where $D_{e_i}(\alpha_i M + \beta_i, 1)$ is Dickson polynomial, which define as

$$D_{e_i}(\alpha_i M + \beta_i, 1) = \sum_{i=0}^{\lfloor e_i/2 \rfloor} \left(\frac{e_i}{e_i - i} \right) \binom{e_i - i}{i} (-1)^i (\alpha_i M + \beta_i)^{e_i - 2i}, \tag{26}$$

Thus, $c_i \equiv V_{e_i}(\alpha_i M + \beta_i, 1) \bmod n_i$ can be considered as polynomials in M of degree e_i.

Corollary 2. In the LUC cryptosystem, a set of k linearly related plaintexts can be recovered if $k > e(e+1)/2$ and $n_i > 2^{(e+1)(e+2)/4}(e+1)^{e+1}$, where $e = \max_{1 \le i \le k} e_i$.

Proof. See Pinch (1995), Theorem 3. ■

4.3 Attack on the LUC$_3$ Cryptosystem

Suppose that $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1 \le i \le k} n_i$. Let M_1 and M_2 are a set of the plaintexts of LUC$_3$ cryptosystem, then $M_{1,i} \equiv \alpha_i M_1 + \beta_i \bmod n_i$ and $M_{2,i} \equiv \alpha_i M_2 + \beta_i \bmod n_i$.

The ciphertexts are $C_{1,i} \equiv V_{e_i}(\alpha_i M_1 + \beta_i, \alpha_i M_2 + \beta_i, 1) \bmod n_i$ and $C_{2,i} \equiv V_{e_i}(\alpha_i M + \beta_i, \alpha_i M_1 + \beta_i, 1) \bmod n_i$. As we known, the third order of Dickson polynomial (Lidl (1993)) and Lucas sequence are equality. Therefore,

$$\begin{aligned} &V_{e_i}(\alpha_i M_1 + \beta_i, \alpha_i M_2 + \beta_i, 1) \\ &\equiv D_{e_i}(\alpha_i M_1 + \beta_i, \alpha_i M_2 + \beta_i, 1) \bmod n_i, \end{aligned} \tag{27}$$

where $D_{e_i}(\alpha_i M_1 + \beta_i, \alpha_i M_2 + \beta_i, 1)$ is Dickson polynomial, which define as

$$D_{e_i}(x, y, 1) = \sum_{i=0}^{\lfloor e_i/2 \rfloor} \sum_{j=0}^{\lfloor e_i/3 \rfloor} \left(\frac{e_i(-1)^i}{e_i - i - 2j} \right) \binom{e_i - i - 2j}{i + j} \binom{i + j}{i} x^{e_i - 2i - 3j} y^i, \tag{28}$$

where $2i + 3j \le e_i$. Similar for $V_{e_i}(\alpha_i M_2 + \beta_i, \alpha_i M_1 + \beta_i, 1)$.

Thus, $C_{1,i} \equiv V_{e_i}(\alpha_i M_1 + \beta_i, \alpha_i M_2 + \beta_i, 1) \bmod n_i$ and $C_{2,i} \equiv V_{e_i}(\alpha_i M_2 + \beta_i, \alpha_i M_1 + \beta_i, 1) \bmod n_i$ can be considered as polynomials in M_1 and M_2 of degree e_i.

Corollary 3. Let $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1 \le i \le k} n_i$. Given a set of k equations

$$\sum_{j_1, j_2 = 0}^{j_1 + j_2 \le \delta} a_{i, j_1, j_2} x_1^{j_1} x_2^{j_2} \equiv 0 \bmod n_i \,, \tag{29}$$

where the moduli n_i are pairwise relatively prime and $\gcd\left(\left\langle a_{i,j_1,j_2} \right\rangle_{j_1,j_2=0}^{j_1+j_2 \le \delta}, n_i\right) = 1$ for all i. Then it is possible to find $x < n$ in polynomial time if

$$N > 2^{\frac{(\delta+1)(\delta+2)(\delta^2+3\delta+4)}{16}} \left(\tfrac{1}{2}(\delta+1)(\delta+2)\right)^{\frac{1}{2}(\delta+1)(\delta+2)} n^{\frac{1}{3}\delta(\delta+1)(\delta+2)}. \tag{30}$$

Proof. In two variable case for Theorem 1.

$$f = \sum_{m=1}^{\delta} m \binom{m+1}{m} = \tfrac{1}{3}\delta(\delta+1)(\delta+2), \tag{31}$$

$$g = \sum_{m=0}^{\delta} \binom{m+1}{m} = \tfrac{1}{2}(\delta+1)(\delta+2). \tag{32}$$

Then, substitute Equations (32) and (33) into (24) will get Equation (31). ■

Corollary 4. In the LUC$_3$ cryptosystem, a set of k linearly related plaintexts can be recovered if $k > \frac{1}{3}e(e+1)(e+2)$ and $n_i > 2^{\frac{(e+1)(e+2)(e^2+3e+4)}{16}} (\frac{1}{2}(e+1)(e+2))^{\frac{1}{2}(e+1)(e+2)}$, where $e = \max_{1 \le i \le k} e_i$.

Proof. The proving for this corollary is to verify that the conditions of Corollary 4.3 is fulfilled. From the k sets of ciphertexts, there exist k equations

$$P_{1,i}(M_1, M_2) \equiv D_{e_i}(\alpha_i M_1 + \beta_i, \alpha_i M_2 + \beta_i, 1) - C_{1,i} \equiv 0 \bmod n_i, \qquad (33)$$

$$P_{2,i}(M_1, M_2) \equiv D_{e_i}(\alpha_i M_2 + \beta_i, \alpha_i M_1 + \beta_i, 1) - C_{2,i} \equiv 0 \bmod n_i. \qquad (34)$$

Suppose that the moduli n_i are pairwise coprime and also that the coefficients of polynomials $P_{1,i}(M_1, M_2)$ and $P_{2,i}(M_1, M_2)$ are relatively prime to n_i, otherwise the plaintexts can be recovered by factoring n_i.

Since

$k > \frac{1}{3}e(e+1)(e+2)$ and $n_i > 2^{\frac{(e+1)(e+2)(e^2+3e+4)}{16}} (\frac{1}{2}(e+1)(e+2))^{\frac{1}{2}(e+1)(e+2)}$,

it follows

$$\begin{aligned} N = \prod_{i=1}^{k} n_i &\geq n_1 \prod_{i=2}^{\frac{1}{3}e(e+1)(e+2)+1} n_i \\ &> 2^{\frac{(e+1)(e+2)(e^2+3e+4)}{16}} \left(\tfrac{1}{2}(e+1)(e+2)\right)^{\frac{1}{2}(e+1)(e+2)} n^{\frac{1}{3}e(e+1)(e+2)}, \end{aligned} \qquad (35)$$

where $n = \min_{1 \le i \le k} n_1$. ∎

4.4 Attack on the LUC$_{4,6}$ Cryptosystem

Suppose that $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1 \le i \le k} n_i$. Let m_1, m_2 and m_3 are a set of the plaintexts of LUC$_{4,6}$ cryptosystem, then $m_{1,i} \equiv \alpha_i m_1 + \beta_i \bmod n_i$, $m_{2,i} \equiv \alpha_i m_2 + \beta_i \bmod n_i$, and $m_{3,i} \equiv \alpha_i m_3 + \beta_i \bmod n_i$. Therefore, the ciphertexts are

$$c_{1,i} \equiv V_{e_i}(\alpha_i m_1 + \beta_i, \alpha_i m_2 + \beta_i, \alpha_i m_3 + \beta_i, 1) \bmod n_i \ , \qquad (36)$$

$$\begin{aligned} c_{2,i} \equiv V_{e_i}(&\alpha_i m_2 + \beta_i, (\alpha_i m_1 + \beta_i)(\alpha_i m_3 + \beta_i) - 1, \\ &(\alpha_i m_1 + \beta_i)^2 + (\alpha_i m_3 + \beta_i)^2 - 2(\alpha_i m_2 + \beta_i), \\ &(\alpha_i m_1 + \beta_i)(\alpha_i m_3 + \beta_i) - 1, \alpha_i m_2 + \beta_i, 1) \bmod n_i, \end{aligned} \qquad (37)$$

$$c_{3,i} \equiv V_{e_i}(\alpha_i m_3 + \beta_i, \alpha_i m_2 + \beta_i, \alpha_i m_1 + \beta_i, 1) \bmod n_i \ , \qquad (38)$$

Since the Hastad'd attack is relied on the polynomial structure, then the Lucas sequence should be transform to polynomial. In this situation, the Dickson polynomial (Dickson (1987)) is able to transform it. That mean, the fourth order and sixth order of Dickson polynomials and Lucas sequences both are equivalent.

Proposition 1. The fourth order Lucas sequence are equivalent to the three variables of Dickson polynomials, which is defined as

$$V_{e_i}(x,y,z,1) = D_{e_i}(x,y,z,1) = \sum_{i=0}^{\lfloor \frac{e_i}{2} \rfloor} \sum_{j=0}^{\lfloor \frac{e_i}{3} \rfloor} \sum_{k=0}^{\lfloor \frac{e_i}{4} \rfloor} \left(\frac{e_i(-1)^{i+k}}{e_i - i - 2j - 3k} \right) \binom{e_i - i - 2j - 3k}{i+j+k} \binom{i+j+k}{i+j} \times \binom{i+j}{i} x^{e_i - 2i - 3j - 4k} y^i z^j, \tag{39}$$

where $2i + 3j + 4k \le e_i$.

Proof. See Wong (2011), Proposition 3.5. ■

Proposition 2. The sixth order Lucas sequence is equivalent to the five variables of Dickson polynomials, which is define as

$$\begin{aligned} &V_{e_i}(x_1,x_2,x_3,x_4,x_5,1) \\ &= D_{e_i}(x_1,x_2,x_3,x_4,x_5,1) \\ &= \sum_{i_1=0}^{\lfloor \frac{e_i}{2} \rfloor} \sum_{i_2=0}^{\lfloor \frac{e_i}{3} \rfloor} \sum_{i_3=0}^{\lfloor \frac{e_i}{4} \rfloor} \sum_{i_4=0}^{\lfloor \frac{e_i}{5} \rfloor} \sum_{i_5=0}^{\lfloor \frac{e_i}{6} \rfloor} \left(\frac{e_i(-1)^{i_1+i_3+i_5}}{e_i - i_1 - 2i_2 - 3i_3 - 4i_4 - 5i_5} \right) \\ &\times \binom{e_i - i_1 - 2i_2 - 3i_3 - 4i_4 - 5i_5}{i_1+i_2+i_3+i_4+i_5} \binom{i_1+i_2+i_3+i_4+i_5}{i_1+i_2+i_3+i_4} \\ &\times \binom{i_1+i_2+i_3+i_4}{i_1+i_2+i_3} \binom{i_1+i_2+i_3}{i_1+i_2} \binom{i_1+i_2}{i_1} x_1^{e_i-2i_1-3i_2-4i_3-5i_4-6i_5} \\ &\times x_2^{i_1} x_3^{i_2} x_4^{i_3} x_5^{i_4}, \end{aligned} \tag{40}$$

where $2i_1 + 3i_2 + 4i_3 + 5i_4 + 6i_5 \le e_i$.

Proof. See Wong (2011), Proposition 3.6. ■

By Proposition 1 and Proposition 2, Equations (37), (38), and (39) can be considered as polynomials in m_1, m_2 and m_3 of degree e_i.

For Hastad's Theorem, there is a variable to be considered. However, the $LUC_{4,6}$ cryptosystem had three variables. Therefore, there are necessary to modify the Hastad's Theorem.

Corollary 5: Let $N = \prod_{i=1}^{k} n_i$ and $n = \min_{1\le i\le k} n_i$. Given a set of k equations

$$\sum_{j_1,j_2,j_3=0}^{j_1+j_2+j_3\le\delta} a_{i,j_1,j_2,j_3} x_1^{j_1} x_2^{j_2} x_3^{j_3} \equiv 0 \bmod n_i, \tag{41}$$

where the moduli n_i are pairwise relatively prime and $\gcd\left(\left\langle a_{i,j_1,j_2,j_3}\right\rangle_{j_1,j_2,j_3}^{j_1+j_2+j_3\le\delta}, n_i\right) = 1$ for all i. Then it is possible to find $x < n$ in polynomial time if

$$N > 2^{\frac{(\delta+1)(\delta+2)(\delta+3)(\delta+4)(\delta^2+2\delta+3)}{144}} \left(\tfrac{1}{6}(\delta+1)(\delta+2)(\delta+3)\right)^{\frac{1}{6}(\delta+1)(\delta+2)(\delta+3)} \times n^{\frac{1}{8}\delta(\delta+1)(\delta+2)(\delta+3)}, \tag{42}$$

Proof. In three variables case for Theorem 3,

$$f = \sum_{m=1}^{\delta} m \binom{m+2}{m} = \frac{1}{8}\delta(\delta+1)(\delta+2)(\delta+3), \tag{43}$$

and

$$g = \sum_{m=0}^{\delta} m \binom{m+2}{m} = \frac{1}{6}\delta(\delta+1)(\delta+2)(\delta+3), \tag{44}$$

Then, substitute Equations (45) and (46) into Equation (24), get Equation (43). ■

Corollary 6. In the LUC$_{4,6}$ cryptosystem, a set of k linearly related plaintexts can be recovered if

$$k > \tfrac{1}{8} e(e+1)(e+2)(e+3) \quad , \tag{45}$$

and

$$n_i > 2^{\frac{(e+1)(e+2)(e+3)(e+4)(e^2+2e+3)}{144}} \left(\tfrac{1}{6}(e+1)(e+2)(e+3)\right)^{\frac{1}{6}(e+1)(e+2)(e+3)} , \tag{46}$$

where $e = \max_{1\le i\le k} e_i$.

Proof. The proving for this corollary is to verify that the conditions of Corollary 1 are fulfilled. From the k sets of ciphertexts, there exist k equations

$$P_{1,i}(m_1, m_2, m_3) \equiv D_{e_i}(\alpha_i m_1 + \beta_i, \alpha_i m_2 + \beta_i, \alpha_i m_3 + \beta_i, 1) - c_{1,i} \equiv 0 \bmod n_i. \tag{47}$$

$$P_{1,i}(m_1,m_2,m_3) \equiv V_{e_i}(\alpha_i m_2+\beta_i,(\alpha_i m_1+\beta_i)(\alpha_i m_3+\beta_i)-1,$$
$$(\alpha_i m_1+\beta_i)^2+(\alpha_i m_3+\beta_i)^2-2(\alpha_i m_2+\beta_i), \tag{48}$$
$$(\alpha_i m_1+\beta_i)(\alpha_i m_3+\beta_i)-1,\alpha_i m_2+\beta_i,1)-c_{2,i} \bmod n_i$$
$$\equiv 0 \bmod n_i,$$

$$P_{3,i}(m_1,m_2,m_3) \equiv D_{e_i}(\alpha_i m_3+\beta_i,\alpha_i m_2+\beta_i,\alpha_i m_1+\beta_i,1)-c_{3,i} \equiv 0 \bmod n_i \quad , \tag{49}$$

Suppose that the moduli n_i are pairwise coprime and also that the coefficients of polynomials $P_{1,i}(m_1,m_2,m_3)$, $P_{2,i}(m_1,m_2,m_3)$ and $P_{3,i}(m_1,m_2,m_3)$ are relatively prime to n_i; otherwise the plaintexts can be recovered by factoring $n_{i..}$

Since

$$k > \tfrac{1}{8}e(e+1)(e+2)(e+3), \quad , \tag{50}$$

$$n_i > 2^{\frac{(e+1)(e+2)(e+3)(e+4)(e^2+2e+3)}{144}}\left(\tfrac{1}{6}(e+1)(e+2)(e+3)\right)^{\frac{1}{6}(e+1)(e+2)(e+3)}, \tag{51}$$

it follows

$$N=\prod_{i=1}^{k} n_i \geq \prod_{2}^{\frac{1}{8}e(e+1)(e+2)(e+3)+1} n_i$$
$$> 2^{\frac{(e+1)(e+2)(e+3)(e+4)(e^2+2e+3)}{144}}\left(\tfrac{1}{6}(e+1)(e+2)(e+3)\right)^{\frac{1}{6}(e+1)(e+2)(e+3)} \tag{52}$$
$$\times n^{\frac{1}{8}e(e+1)(e+2)(e+3)},$$

where $n=\min_{1\le i\le k} n_i$. ■

Coppersmith based variation method is based on the Coppersmith's theorem which is defined in Theorem 2. With this method, sending more than e linearly related plaintexts that are encrypted via RSA or LUC cryptosystem with encryption key, e and RSA-moduli n_i is dangerous. However, this method cannot be directly applied to $LUC_{4,6}$ cryptosystems. This is because one of the conditions in Coppersmith's theorem is that the polynomial, which is analyzed should be a monic polynomial, but the polynomials in $LUC_{4,6}$ cryptosystems are multivariable polynomials.

Nevertheless, Julta improved the theorem to multivariable polynomials (Julta (1998)). In that article, the author states the following:

"Let $P(x_1,\ldots,x_m)\equiv 0 \bmod N$ be a modular multivariable polynomial equation, in m variables, and total degree k with a root $x_{0,i}$, for $1\le i\le m$. Let $|x_{0,i}|<N^{\alpha_i}$, $\sum \alpha_i < 1/k$ and k linear independent integer polynomial equations (in m variables) of total degree polynomial in $mk\log N$, in polynomial time in $mk\log N$, such that each of the equations has $x_{0,i}$ as a root."

Therefore, all integer solution $x_{0,i}$ to $P(x_1,\ldots,x_m)\equiv 0 \bmod N$ can be found with $|x_{0,i}|<N^{1/k}$.

5. CONCLUSION

For $LUC_{4,6}$ cryptosystem, Dickson polynomial is enabling the Lucas sequence to transform into multivariate polynomial. When the plaintexts transform from the sequence to the polynomial, then the number of plaintexts are required to succeed the Hastad's attack can be found. By Coppersmith based variation and the statement from Julta, we can conclude that the result of sending more than *e* linearly related plaintexts that are encrypted via $LUC_{4,6}$ cryptosystem with encryption key, *e* and RSA-moduli n_i is dangerous.

Based on Corollary 1, 2, 4, and 6, the number of plaintexts are required to succeed the Hastad'd attack for the RSA, LUC, LUC_3, and $LUC_{4,6}$ cryptosystems can be found. Hence, the comparison of the requirement of the number of plaintexts between RSA, LUC, LUC_3 and $LUC_{4,6}$ had been shown in Table 1.

TABLE 1: The number of plaintexts, k required to succeed the Hastad's Attack

e	3	5	7	11	13	17	19
RSA	7	16	29	67	92	154	191
LUC	7	16	29	67	92	154	191
LUC_3	21	71	169	573	911	1939	2661
$LUC_{4,6}$	46	211	631	3004	5461	14536	21946

Table 1 show that the requirement of the number of plaintexts to succeed the Hastad's attack for the $LUC_{4,6}$ cryptosystem is the highest. For $LUC_{4,6}$ cryptosystem, if public key, $e = 19$, at least 21946 plaintexts is required to hack the $LUC_{4,6}$ cryptosystem using Hastad's attack. If the cryptosystem is 128-bit, how many number of plaintext is required? It is almost 504 bits of number. Thus, the $LUC_{4,6}$ cryptosystem is more secure than RSA, LUC and LUC_3 cryptosystems.

REFERENCES

Coppersmith, D. 1996. Finding a Small Root of a Univariate Modular Equation. *Lecture Notes in Computer Science*. **1070**: 155-165.

Dickson, L.E. 1897. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *The Annals of Mathematics.* **11**(1/6): 65–120; 161–183.

Hastad, J. 1986. On using RSA with low exponent in a public key network. *Lecture Notes in Computer Science.* **218**: 404-408.

Joye, M. 1997. *Security Analysis of RSA-type Cryptosystems*. PhD Thesis, Universite Catholique de Louvain, Belgium.

Julta, C.S. 1998. On Finding Small Solutions of Modular Multivariate Polynomial Equations. *Lecture Notes in Computer Science.* **1403**:158-170.

Lidl, R. 1993. Theory and application of Dickson polynomial. *Topics in Polynomials of One and Several Variables and Their Applications*, *World Scientific*, pp. 371-395.

Pinch, R.G.E. 1995. Extending The Hastad Attack to LUC. *Electronics Letter.* **31**(21): 1827-1828.

Said, M.R.M and John L. 2003. A Cubic Analogue of the RSA Cryptosystem. *Bulletin of the Australia Mathematical Society.* **68**: 21-38.

Smith, P.J. and Lennon, M.J.J. 1993. LUC: A New Public Key System. *Proceedings of the Ninth IFIP International Symposium on Computer Security*: 103-117.

Rivest, R., Shamir, A. and Adleman, L. 1978. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communication of the ACM*. **21**: 120-126.

Wong, T. J., Said, M. R. M., Atan, K. A. M. and Ural, B. 2007. The Quartic Analog to the RSA Cryptosystem. *Malaysian Journal of Mathematical Sciences*. **1**(1): 63-81.

Wong, T. J. 2011. *A RSA-type Cryptosystem Based on Quartic Polynomials*. PhD Thesis, Universiti Putra Malaysia.