World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:13, No:4, 2019

Cryptographic Attack on Lucas Based Cryptosystems Using Chinese Remainder Theorem

Tze Jin Wong, Lee Feng Koo, Pang Hung Yiu

***Abstract*—**Lenstra's attack uses Chinese remainder theorem as a tool and requires a faulty signature to be successful. This paper reports on the security responses of fourth and sixth order Lucas based ($LUC_{4,6}$) cryptosystem under the Lenstra's attack as compared to the other two Lucas based cryptosystems such as LUC and LUC_3 cryptosystems. All the Lucas based cryptosystems were exposed mathematically to the Lenstra's attack using Chinese Remainder Theorem and Dickson polynomial. Result shows that the possibility for successful Lenstra's attack is less against $LUC_{4,6}$ cryptosystem than LUC_3 and LUC cryptosystems. Current study concludes that $LUC_{4,6}$ cryptosystem is more secure than LUC and LUC_3 cryptosystems in sustaining against Lenstra's attack.

***Keywords*—**Lucas sequence, Dickson Polynomial, faulty signature, corresponding signature, congruence.

I. Introduction

PUBLIC key Cryptography is an encryption technique for secret writing involving a public key and a private key. Public key is used to encrypt the plaintexts, whilst private key is used to decrypt the ciphertexts. This concept was introduced by Diffie and Hellman [2] in 1976. In 1978, Rivest, Shamir, and Adleman [5] discovered the first practical public-key encryption and signature scheme, which now is referred as RSA. The RSA scheme is based on hard mathematical problem and the intractability of factoring large integers.

Smith and Lennon [8] proposed a cryptosystem which is analogous to the RSA scheme and based on Lucas function [9]. It was referred as LUC cryptosystem. LUC cryptosystem used the second order of Lucas sequence to generate the ciphertext or to recover the original plaintext through the process of encryption and decryption respectively. Subsequently, Said and John [6], [7] extended the LUC cryptosystem with a cubic equation and referred it as LUC_3 cryptosystem. Similarly, LUC_3 cryptosystem used third order Lucas sequence to develop further the cryptosystem. Wong used the fourth and sixth order Lucas sequence to develop their $LUC_{4,6}$ cryptosystem [10], [11] which was extended from LUC and LUC_3 cryptosystem, based on the characteristics of quartic equation. The security of $LUC_{4,6}$ cryptosystem [10], [11] had been verified using Hastad's attack [12], GCD attack [13], and garbage-man-in-the-middle (type 1) attack [14], respectively.

At Bellcore press release, September 25th 1996, Boneh, Demilli and Lipton reported that they successfully identified the attack against RSA based on Chinese Remainder Theorem. However, they did not provide any further technical detail. The attack was able to recover the secret factors, p and q of the public modulus n from two signatures of the same plaintext, i.e. a real plaintext and a faulty plaintext. After that, Lenstra [1] wrote a memo to show that only the faulty signature was required for the attack. In this paper, these Lenstra's attacks [3], [4] will be further extended to test on the LUC, LUC_3, and $LUC_{4,6}$ cryptosystems.

II. The LUC-Type Cryptosystem

A N-th order linear recurrence of Lucas sequence is a sequence of integers T_k defined by

$$T_k = \sum_{i=1}^{N} (-1)^{i+1} a_i T_{k-1} \tag{1}$$

with initial values of $T_0, T_1, \cdots, T_{N-1}$, where $a_i$are coefficients in N-th order polynomial,

$$x^N + \sum_{i=1}^{N-1} (-1)^i a_i x^{N-i} + a_N = 0\,. \tag{2}$$

Therefore, all the cryptosystems were developed based on Lucas sequence called LUC-type cryptosystems. In this manner, this study focused on the reaction of LUC, LUC_3, and $LUC_{4,6}$ cryptosystems under Lenstra's attack.

A. LUC Cruptosystem

Suppose that n be the product of two different odd primes, p and q, and the public key, e must be relatively primes to $(p-1)(q-1)(p+1)(q+1)$. Then, the encryption process of LUC cryptosystem can be defined as

$$E(M) = C \equiv V_e(M,1) \bmod n, \tag{3}$$

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

$$ed \equiv 1 \bmod \phi(n) \tag{4}$$

Tze Jin Wong is with Department of Basic Science and Engineering, Universiti Putra Malaysia, Bintulu, Sarawak, 97008 Malaysia. He also is an associate research with Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor 43400 Malaysia (corresponding author, e-mail: w.tzejin@upm.edu.my).

Lee Feng Koo is with Department of Basic Science and Engineering, Universiti Putra Malaysia, Bintulu, Sarawak, 97008 Malaysia. She also is an associate research with Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor 43400 Malaysia (e-mail: leefeng@upm.edu.my).

Pang Hung Yiu is with Department of Basic Science and Engineering, Universiti Putra Malaysia, Bintulu, Sarawak, 97008 Malaysia (e-mail: yiuph@upm.edu.my).

where $\phi(n)$ is Euler function. The Euler totient function defined as

$$\phi(n)=\left(p-\left(\frac{C^2-4}{p}\right)\right)\left(q-\left(\frac{C^2-4}{q}\right)\right) \tag{5}$$

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

$$\begin{aligned} d &\equiv e^{-1} \bmod (p+1)(q+1),\\ d &\equiv e^{-1} \bmod (p+1)(q-1),\\ d &\equiv e^{-1} \bmod (p-1)(q+1),\\ d &\equiv e^{-1} \bmod (p-1)(q-1). \end{aligned} \tag{6}$$

Similarly, the decryption process can be obtained by substituting e and M with d and C respectively into (3).

$$D(C)=M\equiv V_d(C,1) \bmod n. \tag{7}$$

B. LUC_3 Cryptosystem

As in the LUC cryptosystems, LUC_3 cryptosystem has a number n which is the product of two prime numbers p and q. In the encryption process, the encryption key, e must be chosen relatively prime to the Euler function $\phi(n)=\overline{p}\cdot\overline{q}$, in order to solve the congruence $ed\equiv 1 \bmod \phi(n)$, and hence to find the decryption key d.

In the LUC_3 cryptosystem, $\overline{p}$ and $\overline{q}$ are defined as

$$\overline{p}=\begin{cases} p^2+p+1, & \text{if } f(x) \text{ is of type } t[3] \bmod p;\\ p^2-1, & \text{if } f(x) \text{ is of type } t[2,1] \bmod p;\\ p-1, & \text{if } f(x) \text{ is of type } t[1] \bmod p. \end{cases} \tag{8}$$

and

$$\overline{q}=\begin{cases} q^2+q+1, & \text{if } f(x) \text{ is of type } t[3] \bmod q;\\ q^2-1, & \text{if } f(x) \text{ is of type } t[2,1] \bmod q;\\ q-1, & \text{if } f(x) \text{ is of type } t[1] \bmod q. \end{cases} \tag{9}$$

where $f(x)=x^3-Px^2+Qx-1$ with P and Q are plaintexts. Note that type $t[3]$ means $f(x)$ is an irreducible cubic polynomial, type $t[2,1]$ means $f(x)$ is product of an irreducible quadratic polynomial and a linear polynomial, and type $t[1]$ means that $f(x)$ is product of three linear polynomials.

In practice, since $\phi(n)$ depends on the type of an auxiliary polynomial, then the public key, e must be relatively prime to $p-1, q-1, p+1, q+1, p^2+p+1$, and q^2+q+1.

The LUC_3 cryptosystem is set up based on the third order Lucas sequence, V_n which is derived from the cubic polynomial $x^3-Px^2+Qx-1=0$, where P and Q constitute the plaintexts.

The encryption function is defined by

$$E(P,Q)=(V_e(P,Q,1),V_e(Q,P,1))\equiv(C_1,C_2) \bmod n \tag{10}$$

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

$$V_{k+3}=PV_{k+2}-QV_{k+1}+V_k \bmod n \tag{11}$$

with initial values $V_0(P,Q,1)=3$, $V_1(P,Q,1)=P$ and $V_2(P,Q,1)=P^2-2Q$, or $V_0(Q,P,1)=3$, $V_1(Q,P,1)=Q$ and $V_2(Q,P,1)=Q^2-2P$. P and Q are coefficients for cubic polynomial.

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 follow by calculating

$$\begin{aligned} D(C_1,C_2) &= (V_d(C_1,C_2,1),V_d(C_2,C_1,1))\\ &\equiv (C_1,C_2) \bmod n \end{aligned} \tag{12}$$

which would finally recover the original plaintext (P,Q).

C. $LUC_{4,6}$ Cryptosystem

As in the LUC and LUC_3 cryptosystems, the Lucas sequence was used to generate the chipertext from the plaintext or recover the plaintext from the chipertext. In the $LUC_{4,6}$ cryptosystem, the fourth and sixth order Lucas sequence had been selected to generate the ciphertext and recover the plaintext, where the fourth order Lucas sequence was used for the first and third plaintext or ciphertext and the sixth order Lucas sequence was used for the second plaintext or ciphertext. Therefore, there are three sets of plaintexts or ciphertexts. However, there is only one set of plaintext or ciphertext in LUC cryptosystems, whereas LUC_3 is 2.

The encryption key, (e,n) can be made public, whilst (m_1,m_2,m_3) is the set of plaintext. The prime number e must be relatively prime to the Euler totient function $\phi(n)=\overline{p}\cdot\overline{q}$ in order to solve the congruence $ed\equiv 1 \bmod \phi(n)$ and, hence find the decryption key d.

In the $LUC_{4,6}$ cryptosystem, $\overline{p}$ and $\overline{q}$ are defined as

$$\overline{p}=\begin{cases} p^3+p^2+p+1, & \text{if } f(x) \text{ is of type } t[4] \bmod p;\\ p^3-1, & \text{if } f(x) \text{ is of type } t[3,1] \bmod p;\\ p^2-1, & \text{if } f(x) \text{ is of type } t[2,1] \bmod p;\\ p+1, & \text{if } f(x) \text{ is of type } t[2] \bmod p\\ p-1, & \text{if } f(x) \text{ is of type } t[1] \bmod p. \end{cases} \tag{13}$$

and

$$\bar{q} = \begin{cases} q^3+q^2+q+1, & \text{if } f(x) \text{ is of type } t[4] \bmod p; \\ q^3-1, & \text{if } f(x) \text{ is of type } t[3,1] \bmod p; \\ q^2-1, & \text{if } f(x) \text{ is of type } t[2,1] \bmod p; \\ q+1, & \text{if } f(x) \text{ is of type } t[2] \bmod p \\ q-1, & \text{if } f(x) \text{ is of type } t[1] \bmod p. \end{cases} \quad (14)$$

where $f(x) = x^4 - m_1x^3 + m_2x^2 - m_3x + 1$. Note that type $t[4,1]$ means $f(x)$ is an irreducible quartic polynomial, type $t[3,1]$ means $f(x)$ is product of an irreducible cubic polynomial and a linear polynomial, type $t[2,1]$ means $f(x)$ is product of an irreducible quadratic polynomial and two linear polynomials, type $t[2]$ means $f(x)$ is product of two irreducible quadratic polynomials, and type $t[1]$ means $f(x)$ is product of four linear polynomials. In fact, the receiver receives the ciphertext, (c_1, c_2, c_3) but not the plaintext, (m_1, m_2, m_3). Therefore, it is necessary to make sure $g(x) = x^4 - c_1x^3 + c_2x^2 - c_3x + 1$ must in the same type as $f(x)$. In practice, the encryption key e must be relatively 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 in order to cover all possible cases since $\phi(n)$ depends on the type of an auxiliary polynomial. Thus, a public-key cryptosystem will be set, based on the Lucas sequence, V_k which is derived from the quartic polynomial, $x^4 - m_1x^3 + m_2x^2 - m_3x + 1 = 0$.

The encryption function is defined by

$$\begin{aligned} &E(m_1, m_2, m_3) \\ &= (V_e(m_1, m_2, m_3, 1), \\ &\quad V_e(m_2, m_1m_3 - 1, {m_1}^2 + {m_3}^2 - 2m_2, m_1m_3 - 1, m_2, 1) \\ &\quad V_e(m_3, m_2, m_1, 1)) \\ &\equiv (c_1, c_2, c_3) \bmod n \end{aligned} \quad (15)$$

where $n = pq$, (m_1, m_2, m_3) constitute the plaintexts and the coefficients of quartic polynomial and the encryption key,(e, n). $V_e(m_1, m_2, m_3, 1)$ and $V_e(m_3, m_2, m_1, 1)$ are the e-th term of the fourth order Lucas sequence. $V_e(m_2, m_1m_3 - 1, {m_1}^2 + {m_3}^2 - 2m_2, m_1m_3 - 1, m_2, 1)$ is e-th term of the sixth order Lucas sequence which can easily be obtained by using (1).

To decrypt the ciphertexts, the receiver calculates

$$\begin{aligned} &D(c_1, c_2, c_3) \\ &= (V_e(c_1, c_2, c_3, 1), \\ &\quad V_e(c_2, c_1c_3 - 1, {c_1}^2 + {c_3}^2 - 2c_2, c_1c_3 - 1, c_2, 1) \\ &\quad V_e(c_3, c_2, c_1, 1)) \\ &\equiv (m_1, m_2, m_3) \bmod n \end{aligned} \quad (16)$$

which will recover the original message (m_1, m_2, m_3).

III. The Attack

Lenstra's attack is an attack performed using the Chinese Remainder Therorem. It enables the cryptanalyst to get the secret factors of modulus. On the other hand, a greater common divisor (GCD) is used to get the secret factors during the final stage of calculation.

The second of Dickson Polynomial is defined as

$$D_k(x, a) = \sum_{i=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \frac{k}{k-i} \binom{k-i}{i} (-a)^i x^{n-2i} \quad (17)$$

where $\left\lfloor \frac{k}{2} \right\rfloor$ is the largest integer less than $\frac{k}{2}$. It is easy to extend it to the third, fourth and sixth order of Dickson Polynomial. In the Lenstra's attack, Dickson Polynomial is used to transform the Lucas sequence into polynomial to indicate that the secret factors of the modulus can be obtain by GCD method.

A. Attack on LUC Cryptosystem

In the LUC cryptosystem, let p and q be two primes, $n = pq$ denotes the modulus, e is the encryption key, d is the decryption key, m is the plaintext, s is the corresponding signature, and $\hat{s}$ is the faulty signature.

Theorem 1. If the faulty signature, $\hat{s}$ is not in congruence with corresponding signature s modulus p, but in congruence with corresponding signature s modulus q, then

$$\gcd(V_e(\hat{s}, 1) - m \bmod n, n) = q.$$

Proof. Since $\hat{s} \equiv s \bmod q = s + kq$, where k is an any integer, then $V_e(\hat{s}, 1) = V_e(s + kq, 1)$. By using second order of Dickson polynomial,

$$\begin{aligned} V_e(s+kq,1) &\equiv \sum_{i=0}^{\left\lfloor \frac{e}{2} \right\rfloor} \frac{e(-1)^i}{e-i} \binom{e-i}{i} (s+kq)^{e-2i} \bmod n \\ &\equiv V_e(s,1) + q \sum_{i=0}^{\left\lfloor \frac{e}{2} \right\rfloor} \sum_{j=1}^{e-2i} \frac{e(-1)^i}{e-i} \binom{e-i}{i} \binom{e-2i}{j} \times k^j q^{j-1} s^{e-2i-j} \bmod n \\ &\equiv m + q \sum_{i=0}^{\left\lfloor \frac{e}{2} \right\rfloor} \sum_{j=1}^{e-2i} \frac{e(-1)^i}{e-i} \binom{e-i}{i} \binom{e-2i}{j} \times k^j q^{j-1} s^{e-2i-j} \bmod n. \end{aligned}$$

Therefore,

$$V_e(\hat{s}, 1) - m \equiv q \sum_{i=0}^{\left\lfloor \frac{e}{2} \right\rfloor} \sum_{j=1}^{e-2i} \frac{e(-1)^i}{e-i} \binom{e-i}{i} \binom{e-2i}{j} \times k^j q^{j-1} s^{e-2i-j} \bmod n.$$

Since

$$\sum_{i=0}^{\left\lfloor \frac{e}{2} \right\rfloor} \sum_{j=1}^{e-2i} \frac{e(-1)^i}{e-i} \binom{e-i}{i} \binom{e-2i}{j} k^j q^{j-1} s^{e-2i-j}$$

is an irreducible quadratic polynomial, then

$$\gcd(V_e(\hat{s},1) - m \bmod n, n) = q \,. \qquad \square$$

B. Attack on LUC$_3$ Cryptosystem

Same as LUC cryptosystem, let p and q be two primes, $n = pq$ denotes the modulus, e is encryption key, d is decryption key, (m_1, m_2) are plaintexts, (s_1, s_2) are corresponding signatures, and $(\widehat{s_1}, \widehat{s_2})$ are faulty signatures.

Theorem 2. If the faulty signature, $\widehat{s_1}$ is not in congruence with corresponding signature s_1 modulus p, while in congruence with corresponding signature s_1 modulus q, and the faulty signature, $\widehat{s_2}$ is not in congruence with corresponding signature s_2 modulus p, while in congruence with corresponding signature s_2 modulus q, then

$$\gcd(V_e(\widehat{s_1}, \widehat{s_2}, 1) - m_1 \bmod n, n) = q \text{ , and}$$
$$\gcd(V_e(\widehat{s_2}, \widehat{s_1}, 1) - m_2 \bmod n, n) = q \,.$$

Proof: Since

$$\widehat{s_1} \equiv s_1 \bmod q = s_1 + k_1 q \text{ , and } \widehat{s_2} \equiv s_2 \bmod q = s_2 + k_2 q$$

where k_1 and k_2 are an any integer, then

$$V_e(\widehat{s_1}, \widehat{s_2}, 1) = V_e(s_1 + k_1 q, s_2 + k_2 q, 1) \text{ and}$$
$$V_e(\widehat{s_2}, \widehat{s_1}, 1) = V_e(s_2 + k_2 q, s_1 + k_1 q, 1) \,.$$

By using third order of Dickson polynomial,

$$\begin{aligned}
&V_e(s_1 + k_1 q, s_2 + k_2 q, 1) \\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2} \rfloor} \sum_{j=0}^{\lfloor \frac{e}{3} \rfloor} \frac{e(-1)^i}{e-i-2j} \binom{e-i-2j}{i+j} \binom{i+j}{i} (s_1 + k_1 q)^{e-2i-3j} \times (s_2 + k_2 q)^i \bmod n \\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2} \rfloor} \sum_{j=0}^{\lfloor \frac{e}{3} \rfloor} \frac{e(-1)^i}{e-i-2j} \binom{e-i-2j}{i+j} \binom{i+j}{i} \times \sum_{h=0}^{e-2i-3j} \binom{e-2i-3j}{h} k_1{}^h q^h s_1{}^{e-2i-3j-h} \\
&\times \sum_{l=0}^{i} \binom{i}{l} s_2{}^{i-l} (k_2 q)^{i-l} \bmod n \\
&\equiv m_1 + q \sum_{i=0}^{\lfloor \frac{e}{2} \rfloor} \sum_{j=0}^{\lfloor \frac{e}{3} \rfloor} \frac{e(-1)^i}{e-i-2j} \binom{e-i-2j}{i+j} \binom{i+j}{i} \\
&\times \sum_{h=1}^{e-2i-3j} \binom{e-2i-3j}{h} k_1{}^h q^{h-1} s_1{}^{e-2i-3j} \times \sum_{l=1}^{i} \binom{i}{l} s_2{}^{i-l} (k_2 q)^{i-l} \bmod n.
\end{aligned}$$

Therefore,

$$\gcd(V_e(\widehat{s_1}, \widehat{s_2}, 1) - m_1 \bmod n, n) = q \,.$$

Similar calculation is also applied to

$$\gcd(V_e(\widehat{s_2}, \widehat{s_1}, 1) - m_2 \bmod n, n) = q \,. \qquad \square$$

Theorem 3. If the faulty signatures, $(\widehat{s_1}, \widehat{s_2})$ are not in congruence with corresponding signatures (s_1, s_2) modulus p, and only one of the faulty signature $\widehat{s_1}$ or $\widehat{s_2}$ in congruence with corresponding signature s_1 or s_2 modulus q, then, it is unable to get the secret factors.

Proof: Suppose that $\widehat{s_1} = s_1 + k_1 q$ and $\widehat{s_2} \neq s_2 + k_2 q$, where k_1 and k_2 are an any integer, then

$$\begin{aligned}
&V_e(s_1 + k_1 q, \widehat{s_2}, 1) \\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2} \rfloor} \sum_{j=0}^{\lfloor \frac{e}{3} \rfloor} \frac{e(-1)^i}{e-i-2j} \binom{e-i-2j}{i+j} \binom{i+j}{i} (s_1 + k_1 q)^{e-2i-3j} \,. \quad (18) \\
&\times (\widehat{s_2})^i \bmod n.
\end{aligned}$$

Equation (18) cannot be transformed into $m_1 + f(s_1, s_2)$ due to inability to get

$$\sum_{i=0}^{\lfloor \frac{e}{2} \rfloor} \sum_{j=0}^{\lfloor \frac{e}{3} \rfloor} \frac{e(-1)^i}{e-i-2j} \binom{e-i-2j}{i+j} \binom{i+j}{i} s_1{}^{e-2i-3j} s_2{}^i \,.$$

Therefore,

$$\gcd(V_e(\widehat{s_1}, \widehat{s_2}, 1) - m_1 \bmod n, n) \neq q \,. \qquad \square$$

Theorem 3 shows that it is necessary to get all faulty signatures in congruence with corresponding signatures modulus q for successful Lenstra's attack.

C. Attack on LUC$_{4,6}$ Cryptosystem

Same as LUC and LUC$_3$ cryptosystems, let p and q be two primes, $n = pq$ denotes the modulus, e is the encryption key, d is the decryption key, (m_1, m_2, m_3) are plaintexts, (s_1, s_2, s_3) are the corresponding signatures, and $(\widehat{s_1}, \widehat{s_2}, \widehat{s_3})$ are the faulty signatures.

Theorem 4. If the faulty signatures, $(\widehat{s_1}, \widehat{s_2}, \widehat{s_3})$ are not in congruence with corresponding signature (s_1, s_2, s_3) modulus p, while in congruence with corresponding signature (s_1, s_2, s_3) modulus q, then

$$\gcd(V_e(\widehat{s_1}, \widehat{s_2}, \widehat{s_3}, 1) - m_1, n) = q \,,$$
$$\gcd(V_e(\widehat{s_2}, \widehat{s_1}\widehat{s_3} - 1, \widehat{s_1}^2 + \widehat{s_3}^2 - 2\widehat{s_2}, \widehat{s_1}\widehat{s_3} - 1, \widehat{s_2}, 1) - m_2, n) = q \,,$$

and

$$\gcd(V_e(\widehat{s_3}, \widehat{s_2}, \widehat{s_1}, 1) - m_3, n) = q \,.$$

Proof: Since

$\widehat{s_1} \equiv s_1 \bmod q = s_1 + k_1 q$, $\widehat{s_2} \equiv s_2 \bmod q = s_2 + k_2 q$, and

$$\widehat{s_3} \equiv s_3 \bmod q = s_3 + k_3 q$$

where k_1 k_2, and k_3 are any integer, then

$$\begin{aligned} & V_e(\widehat{s_1}, \widehat{s_2}, \widehat{s_3}, 1) \\ & \equiv V_e(s_1 + k_1 q, s_2 + k_2 q, s_3 + k_3 q, 1) \\ & \equiv \sum_{i=0}^{\left\lfloor \frac{e}{2} \right\rfloor} \sum_{j=0}^{\left\lfloor \frac{e}{3} \right\rfloor} \sum_{h=0}^{\left\lfloor \frac{e}{4} \right\rfloor} \frac{e(-1)^{i+h}}{e-i-2j-3h} \binom{e-i-2j-3h}{i+j+h} \binom{i+j+h}{i+j} \\ & \times \binom{i+j}{i} (s_1 + k_1 q)^{e-2i-3j} (s_2 + k_2 q)^i (s_3 + k_3 q)^j \bmod n \end{aligned}$$

Similar proving method is from Theorem 2. It is easy to get

$$\begin{aligned} & V_e(\widehat{s_1}, \widehat{s_2}, \widehat{s_3}, 1) \\ & \equiv m_1 + q \sum_{i=0}^{\left\lfloor \frac{e}{2} \right\rfloor} \sum_{j=0}^{\left\lfloor \frac{e}{3} \right\rfloor} \sum_{h=0}^{\left\lfloor \frac{e}{4} \right\rfloor} \frac{e(-1)^{i+h}}{e-i-2j-3h} \binom{e-i-2j-3h}{i+j+h} \binom{i+j+h}{i+j} \\ & \times \binom{i+j}{i} \sum_{l_1=1}^{e-2i-3j} \binom{e-2i-3j-4h}{l_1} s_1^{e-2i-3j-l_1} k_1^{l_1} q^{l_1-1} \\ & \times \sum_{l_2=1}^{i} \binom{i}{l_2} s_2^{i-l_2} k_2^{l_2} q^{l_2} \sum_{l_3=1}^{j} \binom{j}{l_3} s_3^{j-l_3} k_3^{l_3} q^{l_3} \bmod n \end{aligned}$$

Therefore,

$$\gcd(V_e(\widehat{s_1}, \widehat{s_2}, \widehat{s_3}, 1) - m_1, n) = q .$$

Similar calculation is also applied to

$$\gcd(V_e(\widehat{s_2}, \widehat{s_1}\widehat{s_3} - 1, \widehat{s_1}^2 + \widehat{s_3}^2 - 2\widehat{s_2}, \widehat{s_1}\widehat{s_3} - 1, \widehat{s_2}, 1) - m_2, n) = q$$

and

$$\gcd(V_e(\widehat{s_3}, \widehat{s_2}, \widehat{s_1}, 1) - m_3, n) = q .$$

□

Theorem 5. If the faulty signatures, $(\widehat{s_1}, \widehat{s_2}, \widehat{s_3})$ are not in congruence with corresponding signatures (s_1, s_2, s_3) modulus *p,* and at least one of the faulty signature $\widehat{s_1}$ or $\widehat{s_2}$ or $\widehat{s_3}$ not in congruence with corresponding signature s_1 or s_2 or s_3 modulus *q,* then, it is unable to get the secret factors.

Proof: Suppose that $\widehat{s_1} = s_1 + k_1 q$, $\widehat{s_2} = s_2 + k_2 q$, and $\widehat{s_3} \neq s_3 + k_3 q$, where k_1 k_2, and k_3 are an any integer, then

$$\begin{aligned} & V_e(\widehat{s_1}, \widehat{s_2}, \widehat{s_3}, 1) \\ & \equiv V_e(s_1 + k_1 q, s_2 + k_2 q, s_3 + k_3 q, 1) \\ & \equiv \sum_{i=0}^{\left\lfloor \frac{e}{2} \right\rfloor} \sum_{j=0}^{\left\lfloor \frac{e}{3} \right\rfloor} \sum_{h=0}^{\left\lfloor \frac{e}{4} \right\rfloor} \frac{e(-1)^{i+h}}{e-i-2j-3h} \binom{e-i-2j-3h}{i+j+h} \binom{i+j+h}{i+j} \\ & \times \binom{i+j}{i} (s_1 + k_1 q)^{e-2i-3j} (s_2 + k_2 q)^i \widehat{s_3}^j \bmod n \end{aligned} \quad (19)$$

Since, (19) cannot be transformed into form $m_1 + f(s_1, s_2, s_3)$, then

$$\gcd(V_e(\widehat{s_1}, \widehat{s_2}, \widehat{s_3}, 1) - m_1 \bmod n, n) \neq q .$$

□

Theorem 5 shows that it is necessary to get all faulty signatures in congruence with corresponding signatures modulus *q* for successful the Lenstra's attack.

IV. Conclusion

In this paper, the Lenstra's attack against LUC, LUC_3 and $LUC_{4,6}$ cryptosystem was presented. The Dickson polynomial helps to transform the Lucas sequence into polynomial. It gives the provisions for a successful Lenstra's attack into the cryptosystems. Result cannot summarize the security capability comparison among the cryptosystems. However, the possibility for Lenstra's attack to success in the $LUC_{4,6}$ cryptosystem is smaller than in LUC_3 and LUC cryptosystems. This is because the $LUC_{4,6}$ cryptosystem needs three faulty signatures in congruence with corresponding signature while, LUC_3 cryptosystem requires only two faulty signatures and LUC cryptosystem needs only one.

Acknowledgment

The authors would express their gratitude to all that has assisted in the completion of this study.

References

[1] D. Bleichenbacher, W. Bosma, and A. K. Lenstra, "Some remarks on Lucas-Based Cryptosystems", *Lecture Notes in Computer Science* 963:386-396, 1995.

[2] W. Diffie, and M. Hellman, "New directions in cryptography", *IEEE Transaction on Information Theory* 22: 644-654, 1976.

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

[4] M. Joye, "On the importance of securing your bins: The garbage-man-in-the-middle attack", *Proceeding of the 4th ACM Coference on Computer and Communications Security*, ACM press, 135-141, 1997.

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

[6] M. R. M. Said, "Application of Recurrence Relations to Cryptography". *PhD Thesis*, Macquarie University, Australia, 1997.

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

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

[9] H. C. Williams, "On a Generalization of the Lucas Functions", *Acta Arithmetica* 20: 33-51, 1972.

[10] T. J. Wong, "A RSA-type Cryptosytem Based on Quartic Polynomials", *PhD Thesis*, Universiti Putra Malaysia, Malaysia, 2011.
[11] T. J. Wong, M. R. M. Said, K. A. M. Atan, and B. Ural, "The Quartic Analog to the RSA Cryptosystem", *Malaysian Journal of Mathematical Sciences* 1(1), 63-81, 2007.
[12] T. J. Wong, M. R. M. Said, M. Othman, and K.A.M. Atan, "Garbage-Man-In-The-Middle Attack on the LUC4 Cryptosystem", *International Journal of Cryptology Research* 1(1), 33-41, 2009.
[13] T. J. Wong, M. R. M. Said, M. Othman, and K.A.M. Atan, "GCD Attack on the LUC4 Cryptosystem", *International Journal of Cryptology Research* 1(2), 179-189, 2009.
[14] T. J. Wong, H. Kamarulhali, and M. R. M. Said, "On the Hastad's Attack to LUC4,6 Cryptosystem and compared with Other RSA-Type Cryptosystem". *Malaysian Journal of Mathematical Science* 7(S), 1-17, 2013.