ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.12, 10883–10894
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.12.72 Special Issue SMS-2020

ON THE SECURITY COMPARISON OF LUC-TYPE CRYPTOSYSTEMS USING CHOSEN MESSAGE ATTACK

TZE JIN WONG[1], LEE FENG KOO, FATIN HANA NANING, PANG HUNG YIU, AHMAD FADLY NURULLAH RASEDEE, MOHAMAD MAULANA MAGIMAN, AND MOHAMMAD HASAN ABDUL SATHAR

ABSTRACT. The security of LUC type cryptosystems was investigated. In this study, chosen message attack was employed to analyze the security of LUC, LUC_3 and $LUC_{4,6}$ cryptosystems. The cryptanalyst invades the system by obtaining a signature without the sender's consent, and use it to break the system. Finding shows that $LUC_{4,6}$ cryptosystem is more resilient against chosen message attack compare with LUC and LUC_3 cryptosystems.

1. INTRODUCTION

The Fourth Industrial Revolution shapes the world into digital and automatic paradigm. Accordingly, every sector industry is transformed, and the revolution hastens the digitalization of work as well as human life in every aspect. The increasing of digital marketplace transaction such as e-banking and e-commerce has unfortunately attracted cybercriminals, consequently become a huge challenge in digital economy. As such, data integrity and cyber security is a vital component to ensure security or authentication of confidential data and information in a system against the abuse, misuse, unauthorized access and theft. Hence, the world

[1]*corresponding author*

2020 *Mathematics Subject Classification.* 94A60, 11T71.

Key words and phrases. ciphertext, decryption, encryption, keys, Lucas sequence, plaintext.

of virtual marketplace is established by cryptography that plays a key role in ensuring data integrity and data secrecy of stakeholders as well as the reputation of businesses.

Public key cryptography (PKC) is an encryption technique for secret writing that comprises of two keys. Public encryption key is used to encrypt the plaintexts, whilst private decryption key is used to decrypt the ciphertexts. The well known public key cryptosystem, RSA scheme is widely employed to secure communication that required elevated confidentiality. The modulus n of RSA is the product of two different prime numbers. The security of RSA scheme is based on hard mathematical problem that is the intractability of factoring large integers.

Smith and Lennon [1] modified Dickson-Scheme

and proposed a LUC cryptosystem after examined the weakness of RSA scheme. LUC is asymmetric key cryptosystem which is analogous to RSA scheme but based on the factorization problem and Lucas function. LUC type cryptosystem utilized the Lucas sequence to either generate the ciphertext from the plaintext, or recover the plaintext from the ciphertext. Further exercise done by Said and John [2] extended LUC cryptosystem with cubic polynomial, termed as LUC_3 cryptosystem. Wong et al. [3] implemented the Lucas sequence and based on quartic polynomial to develop $\text{LUC}_{4,6}$ cryptosystem.

Numerous efficiency and security analysis for cryptosystem had been investigated previously [4, 6, 8, 9]. In this paper, the chosen message attack had been selected as a threat against LUC, LUC_3 and $\text{LUC}_{4,6}$ cryptosystems. The chosen message attack is a technique based on homomorphic nature of the cryptosystem. This attack enables the cryptanalyst to obtain a signature without the sender's consent. The cryptanalyst chooses a random number and encrypts the plaintext to become the faulty plaintext. Subsequently, the cryptanalyst would request the sender to decrypt the faulty plaintext to become the faulty signature. Finally, the cryptanalyst will generate the corresponding signature by using extend Euclidean algorithm to break the system.

2. PRELIMINARIES

An N-th order of linear recurrence sequence is a sequence of integers, T_k defined by [10]

$$T_k = \sum_{i=1}^{N} (-1)^{i+1} a_i T_{k-i}, \tag{2.1}$$

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

$$x^N + \sum_{i=1}^{N-1} (-1)^i a_i x^{N-i} + a_N = 0. \tag{2.2}$$

2.1. **Second Order of Lucas Sequence.** Suppose that a_1, a_2 are the coefficients and α, β are the roots of quadratic polynomial defined in (2.2), then the first and second type of Lucas sequence can be defined as follows:

Definition 2.1. *The first and second type of second order Lucas sequence [1] is defined as*

$$V_n(a_1, a_2) = \alpha^n + \beta^n$$
$$U_n(a_1, a_2) = \alpha^n - \beta^n,$$

with initial values $V_0 = 2$, $V_1 = a_1$, $U_0 = 0$ *and* $U_1 = 1$.

The sequences V_n and U_n satisfy the linear recurrence properties defined in (2.1).

Definition 2.2. *The* $(a + b)$*-th term of second order Lucas sequence [1] is defined as*

$$2V_{a+b} = V_a V_b + D U_a U_b,$$

where D *is the discriminant of quadratic polynomial.*

2.2. **Third Order of Lucas Sequence.** Suppose that a_1, a_2, a_3 are the coefficients and α, β, γ are the roots of cubic polynomial defined in (2.2), then the first, second and third type of Lucas sequence can be defined as follows:

Definition 2.3. *The first, second and third type of third order Lucas sequence [2] is defined as*

$$V_n(a_1, a_2, a_3) = \alpha^n + \beta^n + \gamma^n$$
$$U_n(a_1, a_2, a_3) = \alpha^n + \omega^2 \beta^n + \omega \gamma^n$$
$$W_n(a_1, a_2, a_3) = \alpha^n + \omega \beta^n + \omega^2 \gamma^n,$$

where $\omega = (-1 + \sqrt{-3})/2$ *is a cube root of unity.*

The sequences V_n, U_n and W_n satisfy the linear recurrence properties defined in (2.1).

Definition 2.4. *The $(a+b)$-th term of third order Lucas sequence [2] is defined as*

$$3V_{a+b} = V_aV_b + U_aW_b + W_aU_b.$$

2.3. **Fourth Order of Lucas Sequence.** Suppose that a_1, a_2, a_3 and a_4 are the coefficients and α, β, γ and λ are the roots of quartic polynomial defined in (2.2), then the first until fourth type of Lucas sequence can be defined as follows:

Definition 2.5. *The four type of fourth order Lucas sequence [3] is defined as*

$$\begin{aligned} V_n(a_1,a_2,a_3,a_4) &= \alpha^n + \beta^n + \gamma^n + \lambda^n, \\ U_n(a_1,a_2,a_3a_4) &= \alpha^n - \beta^n + \gamma^n - \lambda^n, \\ U''_n(a_1,a_2,a_3a_4) &= \alpha^n - \beta^n - \gamma^n + \lambda^n, \\ U'''_n(a_1,a_2,a_3a_4) &= \alpha^n + \beta^n - \gamma^n - \lambda^n. \end{aligned}$$

The sequences V_n, U'_n, U''_n and U'''_n satisfy the linear recurrence properties defined in (2.1).

Definition 2.6. *The $(a+b)$-th term of fourth order Lucas sequence [3] is defined as*

$$4V_{a+b} = V_aV_b + U'_aU'''_b + U''_aU''_b + U'''_aU'_b.$$

2.4. **Sixth Order of Lucas Sequence.** Suppose that a_1, a_2 a_3, a_4, a_5 and a_6 are the coefficients; and α_1, α_2, α_3, α_4, α_5 and α_6 are the roots of sextic polynomial defined in (2.2), then the first until sixth type of Lucas sequence can be defined as follows:

Definition 2.7. *The first until sixth type of sixth order Lucas sequence [3] are defined as*

$$\begin{aligned} V_n &= \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n + \alpha_5^n + \alpha_6^n, \\ U'_n &= \alpha_1^n + \omega\alpha_2^n + \omega^2\alpha_3^n + \alpha_4^n + \omega\alpha_5^n + \omega^2\alpha_6^n, \\ U''_n &= \alpha_1^n + \omega^2\alpha_2^n + \omega\alpha_3^n + \alpha_4^n + \omega^2\alpha_5^n + \omega\alpha_6^n, \\ U'''_n &= \alpha_1^n + \alpha_2^n + \alpha_3^n - (\alpha_4^n + \alpha_5^n + \alpha_6^n), \\ U_n^{IV} &= \alpha_1^n + \omega\alpha_2^n + \omega^2\alpha_3^n - (\alpha_4^n + \omega\alpha_5^n + \omega^2\alpha_6^n), \\ U_n^{V} &= \alpha_1^n + \omega^2\alpha_2^n + \omega\alpha_3^n - (\alpha_4^n + \omega^2\alpha_5^n + \omega\alpha_6^n), \end{aligned}$$

where $\omega = (-1+\sqrt{-3})/2$ is a cube root of unity.

The sequences V_n until U_n^V satisfy the linear recurrence properties defined in (2.1). In $\text{LUC}_{4,6}$ cryptosystem, the sixth order Lucas sequence is based on quartic polynomial. Thus, the roots of polynomial were modified become $\alpha_1 = \alpha\beta$, $\alpha_2 = \alpha\gamma$, $\alpha_3 = \alpha\lambda$, $\alpha_4 = \beta\gamma$, $\alpha_5 = \beta\lambda$, and $\alpha_6 = \gamma\lambda$, where α, β, γ and λ are the roots of quartic polynomial in the section 2.3.

Definition 2.8. *The $(a+b)$-th term of sixth order Lucas sequence [3] is defined as*

$$6V_{a+b} = V_aV_b + U'_aU''_b + U''_aU'_b + U'''_aU'''_b + U_a^{IV}U_b^V + U_a^VU_b^{IV}.$$

3. The LUC-type Cryptosystems

In [5, 7], the application of Lucas sequences in LUC type cryptosystem was proposed, apparently independent on earlier publication in [1, 2].

3.1. **LUC Cryptosystem.** Suppose that $n = pq$, the public key, e must be relatively primes to $(p \pm 1)(q \pm 1)$, and the message denoted as M. Then, the ciphertext, C can be calculated as

$$E(M) = C \equiv V_e(M, 1) \mod n, \tag{3.1}$$

where $V_e(M, 1)$ is the $e-$th term of second order Lucas sequence.

The corresponding decryption key, d can be generated by

$$ed \equiv 1 \mod \phi(n),$$

where $\phi(n)$ is Euler Totient function defined as

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

$\left(\frac{C^2-4}{p}\right)$ and $\left(\frac{C^2-4}{q}\right)$ are Legendre symbols of (C^2-4) with respect to p and q.

Similar to the encryption process, the plaintext can be recovered in the decryption process by substituting e and M with d and C respectively into (3.1).

3.2. **LUC_3 Cryptosystem.** 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 are are coefficients for cubic polynomial. Both P and Q constitute the plaintexts. Analogous to LUC cryptosystems, LUC_3 cryptosystem has a system nodulus $n = pq$, the public encryption key, e must be chosen relatively prime to the Euler Totient function ,$\Phi(n)$ in order to solve the congruence $ed \equiv 1$

$\mod \phi(n)$, and consequently used to find the decryption key d. The $\Phi(n)$ for LUC$_3$ cryptosystem is defined as

$$\Phi(n) = \overline{pq},$$

where

$$\bar{p} = \begin{cases} p^2+p+1, & \text{if } f(x) \text{ is of type of } t[3] \mod p \\ p^2-1, & \text{if } f(x) \text{ is of type of } t[2,1] \mod p \\ p-1, & \text{if } f(x) \text{ is of type of } t[1] \mod p \end{cases}$$

with $f(x) = x^3 - Px^2 + Qx - 1$. In practise, the public key, e must relatively prime to $p \pm 1$, $q \pm 1$, $p^2 + p + 1$ and $q^2 + q + 1$ since the $\Phi(n)$ depends on the type of an auxiliary polynomial.

The encryption function is defined by

$$E(P,Q) = (V_e(P,Q,1), V_e(Q,P,1)) \equiv (C_1, C_2) \mod n,$$

where $V_e(P,Q,1)$ and $V_e(Q,P,1)$ are the $e-$th term of the third order Lucas sequence. The decryption key, d is defined as $d \equiv e^{-1} \mod \Phi(n)$. In order to decrypt the plaintext, the receiver must know or be able to compute $\Phi(n)$ followed by calculating

$$D(C_1,C_2) = (V_d(C_1,C_2,1), V_d(C_2,C_1,1)) \equiv (P,Q) \mod n,$$

where C_1 and C_2 constitutes the ciphertexts; which recovers the original plaintext (P,Q).

3.3. **LUC$_{4,6}$ Cryptosystem.** In the LUC$_{4,6}$ cryptosystem, the fourth and sixth order Lucas sequence had been selected to generate the ciphertext or recover the plaintext, where the fourth order Lucas sequence is applied to create the first and third plaintext or ciphertext, whilst the sixth order Lucas sequence is used to create the second plaintext or ciphertext. Therefore, in LUC$_{4,6}$ are three plaintexts in each set. However, in LUC, there is only one plaintext, whilst the number of plaintexts in the LUC$_3$ cryptosystem is two.

The encryption key (e,n) is made public, whilst (m_1,m_2,m_3) is set of plaintext wherein must make private. The prime number e must be relatively prime to the Euler totient function, $\Phi(n) = \overline{pq}$ in order to solve the congruence $ed \equiv 1 \mod \Phi(n)$, thus to find the decryption key, d. The Euler totient function, $\Phi(n)$ can be defined as

$$\Phi(n) = p_1^{b_1-1}\bar{p_1}p_2^{b_2-1}\bar{p_2}\ldots p_r^{b_r-1}, \bar{p_r}$$

$$\bar{p}_l = \begin{cases} p_i^3 + p_i^2 + p_i + 1, & \text{if } f(x) \text{ is of type of } t[4] \mod p_i \\ p_i^3 - 1, & \text{if } f(x) \text{ is of type of } t[3,1] \mod p_i \\ p_i^2 - 1, & \text{if } f(x) \text{ is of type of } t[2,1] \mod p_i \\ p_i + 1, & \text{if } f(x) \text{ is of type of } t[2] \mod p_i \\ p_i - 1, & \text{if } f(x) \text{ is of type of } t[1] \mod p_i \end{cases}$$

where $f(x) = x^4 - m_1x^3 + m_2x^2 - m_3x + 1$. 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 type of $g(x) = x^4 - c_1x^3 + c_2x^2 - c_3x + 1$ must same type of $f(x)$ so that the original plaintext can be revealed correctly. In practice, $\Phi(n)$ depends on the type of auxiliary polynomial. As such, the encryption key, e must be relatively prime to $p \pm 1, q \pm 1$, $p^2 + p + 1, q^2 + q + 1, p^3 + p^2 + p + 1$, and $q^3 + q^2 + q + 1$ to cover all possible cases.

With these preliminary evaluations, 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 as

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

where $n = pq$, (m_1, m_2, m_3) constitutes the plaintext and the coefficients of quartic polynomial; and (e, n) is the encryption key. $V_e(m_1, m_2, m_3, 1)$ and $V_e(m_3, m_2, m_1, 1)$ are the e-th term of the fourth order of Lucas sequence; whilst, $V_e(m_2, m_1m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1)$ is e-th term of the sixth order of Lucas sequence.

Akin to LUC and LUC$_3$, the decryption key is (d, n) where d is the inverse of e modulo $\Phi(n)$. The receiver must adequate to compute $\Phi(n)$ and afterward evaluate

$$\begin{aligned} D(c_1, c_2, c_3) &= (m_1, m_2, m_3) \\ &= (V_d(c_1, c_2, c_3, 1), \\ &\quad V_d(c_2, c_1c_3 - 1, c_1^2 + c_3^2 - 2c_2, c_1c_3 - 1, c_2, 1), \\ &\quad V_d(c_3, c_2, c_1, 1)) \mod n. \end{aligned}$$

which recovers the original message $(m - 1, m_2, m_3)$.

4. The Chosen Message Attack

4.1. **Attack on LUC Cryptosystem.**

Proposition 4.1. *Let m be the message, (e, n) be the public key for sender, d be the decryption key, k be the transformation key with $gcd(k, e) = 1$ and $s \equiv V_d(m, 1) \mod n$ be the signature of message, the cryptanalyst able to obtain the message by calculating*

$$s \equiv 2^{-1}[V_u(s', 1)V_v(m, 1) + (m^2 - 4)U_u(s', 1)U_v(m, 1)] \mod n.$$

where $s' \equiv V_d(m', 1) \mod n$, $m' \equiv V_k(m, 1) \mod n$ and $ku + ev = 1$ for $u, v \in \mathbb{Z}$.

Proof. Since $gcd(k, e) = 1$, then, there exists $u, v \in \mathbb{Z}$ such that $ku + ev = 1$. Cryptanalyst computes the faulty message,

$$m' \equiv V_k(m, 1) \mod n,$$

and sends to the sender. The sender will then decrypt the faulty message become faulty signature,

$$s' \equiv V_d(m', 1) \mod n.$$

As such, the cryptanalyst can compute

$$\begin{aligned} U_{ku}(s, 1) &\equiv U_{edku}(s, 1) \equiv U_u(V_{edk}(s, 1), 1) \\ &\equiv U_u(V_{dk}(m, 1), 1) \equiv U_u(V_d(m', 1), 1) \\ &\equiv U_u(s', 1) \mod n, \end{aligned} \tag{4.1}$$

$$U_{ev}(s, 1) \equiv U_v(V_e(s, 1), 1) \equiv U_v(m, 1) \mod n, \tag{4.2}$$

and

$$\begin{aligned} V_u(s', 1)V_v(m, 1) &\equiv V_{du}(m', 1)V_v(m, 1) \equiv V_{kdu}(m, 1)V_v(m, 1) \\ &\equiv V_{edku}(s, 1)V_{ev}(s, 1) \equiv V_{ku}(s, 1)V_{ev}(s, 1) \mod n \end{aligned} \tag{4.3}$$

after obtaining the faulty signature, s' from sender. Based on the Definition 2.2, the $(ku + ev)$-th term of Lucas sequence can be defined as

$$2V_{ku+ev}(s, 1) \equiv V_{ku}(s, 1)V_{ev}(s, 1) + DU_{ku}(s, 1)U_{ev}(s, 1) \mod n, \tag{4.4}$$

where $D = m^2 - 4$ is the discriminant of quadratic polynomial, $x^2 - mx + 1 = 0$.

Since $ku + ev = 1$ and $V_1(s, 1) = s$, then substitute (4.1) - (4.3) into (4.4), gives

$$s \equiv 2^{-1}[V_u(s', 1)V_v(m, 1) + (m^2 - 4)U_u(s', 1)U_v(m, 1)] \mod n.$$

This implies that the cryptanalyst successfully breaks the system. □

4.2. **Attack on LUC$_3$ Cryptosystem.** The attack is akin to LUC cryptosystem.

Proposition 4.2. *Let (m_1, m_2) be the set of messages, the public key denoted as (e, n), the decryption key denoted as d, the transformation key denoted as k, with $gcd(k, e) = 1$, and the set of signatures (s_1, s_2) are*

$$s_1 \equiv V_d(m_1, m_2, 1) \mod n, \qquad \textit{and}$$
$$s_2 \equiv V_d(m_2, m_1, 1) \mod n.$$

The cryptanalyst able to obtain the message by calculating

$$\begin{aligned} s_1 \equiv & 3^{-1} \left[V_u(s_1', s_2', 1)V_v(m_1, m_2, 1) + U_u(s_1', s_2', 1)W_v(m_1, m_2, 1)\right. \\ & \left. + W_u(s_1', s_2', 1)U_v(m_1, m_2, 1)\right] \mod n \end{aligned}$$

and

$$\begin{aligned} s_2 \equiv & 3^{-1} \left[V_u(s_2', s_1', 1)V_v(m_2, m_1, 1) + U_u(s_2', s_1', 1)W_v(m_2, m_1, 1)\right. \\ & \left. + W_u(s_2', s_1', 1)U_v(m_2, m_1, 1)\right] \mod n, \end{aligned}$$

where

$$\begin{aligned} s_1' &\equiv V_d(m_1', m_2', 1) \mod n, \\ s_2' &\equiv V_d(m_2', m_1', 1) \mod n, \\ m_1' &\equiv V_k(m_1, m_2, 1) \mod n, \\ m_2' &\equiv V_k(m_2, m_1, 1) \mod n, \end{aligned}$$

and $ku + ev = 1$ with $u, v \in \mathbb{Z}$.

Proof. The proof of this proposition is similar to the Proposition 4.1. □

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

Proposition 4.3. *Let (m_1, m_2, m_3) is the set of plaintext, the sender's public key denoted as (e, n), private key denoted as d, cryptanalyst's transformation key denoted as k such that $gcd(k, e) = 1$ and the set of signature (s_1, s_2, s_3), where*

$$s_1 \equiv V_d(m_1, m_2, m_3, 1) \mod n,$$
$$s_2 \equiv V_d(m_2, m_1m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1) \mod n,$$
$$s_3 \equiv V_d(m_3, m_2, m_1, 1) \mod n,$$

then, the cryptanalyst able to obtain the message by calculating

$$\begin{aligned} s_1 \equiv & 4^{-1} \left[V_u(s_1', s_2', s_3', 1) V_v(m_1, m_2, m_3, 1) \right. \\ & + U_u'(s_1', s_2', s_3', 1) U_v'''(m_1, m_2, m_3, 1) \\ & + U_u''(s_1', s_2', s_3', 1) U_v''(m_1, m_2, m_3, 1) \\ & \left. + U_u'''(s_1', s_2', s_3', 1) U_v'(m_1, m_2, m_3, 1) \right] \mod n, \end{aligned}$$

$$\begin{aligned} s_2 \equiv & 6^{-1} \left[V_u(S') V_v(M) + U_u'(S') U_v''(M) + U_u''(S') U_v'(M) \right. \\ & \left. + U_u'''(S') U_v'''(M) + U_u^{IV}(S') U_v^V(M) + U_u^V(S') U_v^{IV}(M) \right] \mod n, \end{aligned}$$

and

$$\begin{aligned} s_3 \equiv & 4^{-1} \left[V_u(s_3', s_2', s_1', 1) V_v(m_3, m_2, m_1, 1) \right. \\ & + U_u'(s_3', s_2', s_1', 1) U_v'''(m_3, m_2, m_1, 1) \\ & + U_u''(s_3', s_2', s_1', 1) U_v''(m_3, m_2, m_1, 1) \\ & \left. + U_u'''(s_3', s_2', s_1', 1) U_v'(m_3, m_2, m_1, 1) \right] \mod n, \end{aligned}$$

where

$$\begin{aligned} (S') &= (s_2', s_1' s_3' - 1, s_1'^2 + s_3'^2 - 2s_2', s_1' s_3' - 1, s_2', 1) \\ (M) &= (m_2, m_1 m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1 m_3 - 1, m_2, 1), \end{aligned}$$

and (s_1', s_2', s_3') *is set of faulty signature and* $ku + ev = 1$ *with* $u, v \in \mathbb{Z}$.

Proof. The proof of this proposition is similar to rhe Proposition 4.1. □

Note that, the calculation for s_2 is based on sixth order Lucas sequence and involve U' until U^V. However, the cryptanalyst unable to obtain the signature for $\text{LUC}_{4,6}$ cryptosystem by using chosen plaintext attack as the sequences U_n' until U_n^V are not Fibonacci sequence wherein the initial values of these sequences are calculate based on the roots of polynomial (refer Definition 2.5 and 2.7). Accordingly, it is not easy to reveal the original plaintexts due to the difficulties in calculating the roots of polynomial which use to obtain the initial value of the sequences U_n', U_n'', U_n''', U_n^{IV}, and U_n^V. In this situation, the cryptanalyst can recover the original plaintext directly without any attacks if he able find the roots of polynomials. However, theoretically, to best of our knowledge, the roots of polynomial are necessarily to obtain the exact initial values of the sequences and subsequently break the system. Hence, this affirmed that the security level of $\text{LUC}_{4,6}$ considerably more secure as compared to the LUC and LUC_3 cryptosystem.

5. CONCLUSION

In this paper, chosen message attack was employed to analyze the security of LUC, LUC_3 and $LUC_{4,6}$ cryptosystems. This is a severe attack where the cryptanalyst can easily extract a signature without the permission of the sender. The cryptanalyst firstly chooses a random number and encrypts the plaintext to faulty plaintext. The cryptanalyst will then request the sender to decrypt the faulty plaintext to become the faulty signature. Finally, the cryptanalyst will generate the signature, and eventually break the system easily. Results shown that the LUC, and LUC_3 cryptosystems can be crashed easily without decryption key by using chosen plaintext attack. However, the cryptanalyst unable to intervene $LUC_{4,6}$ cryptosystem at this moment. Thus, it can concluded that the $LUC_{4,6}$ cryptosystem is more secure than the LUC and LUC_3 cryptosystems.

ACKNOWLEDGMENT

The authors wish to acknowledge financial support from Putra Grant (Vote No. 9664500).

REFERENCES

[1] P. J. SMITH, M. J. J. LENNON: *LUC: A New Public Key System*, Proceedings of the Ninth IFIP International Symposium on Computer Security, (1993), 103–117.

[2] M. R. M. SAID, L. JOHN: *A Cubic Analogue of the RSA Cryptosystem*, Bulletin of the Australia Mathematical Society, **68** (2003) 21–38.

[3] T. J. WONG, M. R. M. SAID, K. A. M. ATAN, B. URAL: *The Quartic Analog to the RSA Cryptosystem*, Malaysian Journal of Mathematical Sciences, **1**(1) (2007), 63–81.

[4] N.N.A. RAHMAN, M.A. ASBULLAH, M.R.K. ARIFFIN, S.H. SAPAR, F. YUNOS : *Cryptanalysis of RSA Key Equation Of $N = p2q$ For Small $|2q - p|$ Using Continued Fraction*, Malaysian Journal of Science, **39**(1) (2020), 72–80.

[5] W.T. JIN, H. KAMARULHALI, 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) (2013), 1–17.

[6] I.N. SARBINI, T.J. WONG, L.F. KOO, M. OTHMAN, M.R.M. SAID, P.H. YIU: *Garbage-man-in-the-middle (type2) attack on the Lucas Based El-gamal Cryptosystem in the Elliptic Curve Group Over Finite Field*, Proceedings of the 6th International Cryptology and Information Security Conference, (2018), 35–41.

[7] I. N. SARBINI, L.F. KOO, T.J. WONG, F.H. NANING, F.H., P.H. YIU: *An analysis for chosen plaintext attack in elliptic curve cryptosystem based on second order lucas sequence*, International Journal of Scientific and Technology Research, **8**(11) (2019), 1193–1196.

[8] I.N. SARBINI, T.J. WONG, M. OTHMAN, L.F. KOO, A.F.N. RASEDEE, P.H. YIU, F.N. NANING: *Cryptographic attack on luc-type cryptosystems using gmitm (Type 1)*, Journal of Advanced Research in Dynamical and Control Systems, **11**(12 Special Issue) (2019), 806–813.

[9] T.J. WONG, M.R.M. SAID, M. OTHMAN, L.F. KOO : *On the common modulus attack into LUC4,6 Cryptosystem*, AIP Conference Proceeding, **1660** (2015), 090052.

[10] T.J. WONG, M.R.M. SAID, M. OTHMAN, L.F. KOO : *A Method to Decrease Computation Time for Fourth Order Lucas Sequence*, AIP Conference Proceeding, **1557** (2013), 55–58.

DEPARTMENT OF SCIENCE AND TECHNOLOGY, UNIVERSITI PUTRA MALAYSIA,
BINTULU CAMPUS, NYABAU ROAD, 97008 BINTULU, SARAWAK, MALAYSIA
Email address: w.tzejin@upm.edu.my

DEPARTMENT OF SCIENCE AND TECHNOLOGY, UNIVERSITI PUTRA MALAYSIA,
BINTULU CAMPUS, NYABAU ROAD, 97008 BINTULU, SARAWAK, MALAYSIA
Email address: leefeng@upm.edu.my

DEPARTMENT OF SCIENCE AND TECHNOLOGY, UNIVERSITI PUTRA MALAYSIA,
BINTULU CAMPUS, NYABAU ROAD, 97008 BINTULU, SARAWAK, MALAYSIA
Email address: fatinhanaz@upm.edu.my

DEPARTMENT OF SCIENCE AND TECHNOLOGY, UNIVERSITI PUTRA MALAYSIA,
BINTULU CAMPUS, NYABAU ROAD, 97008 BINTULU, SARAWAK, MALAYSIA
Email address: yiuph@upm.edu.my

FACULTY OF ECONOMICS AND MUAMALAT, UNIVERSITI SAINS ISLAM MALAYSIA,
78100 NILAI, NEGERI SEMBILAN, MALAYSIA
Email address: fadlynurullah@usim.edu.my

DEPARTMENT OF SOCIAL SCIENCE AND MANAGEMENT, UNIVERSITI PUTRA MALAYSIA,
BINTULU CAMPUS, NYABAU ROAD, 97008 BINTULU, SARAWAK, MALAYSIA
Email address: mdmaulana@upm.edu.my

CENTRE OF FOUNDATION STUDIES FOR AGRICULTURAL SCIENCE, UNIVERSITI PUTRA MALAYSIA,
43400 UPM SERDANG, SELANGOR, MALAYSIA
Email address: mohdhasan@upm.edu.my