Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

SEMARAK ILMU PUBLISHING
Journal of ADVANCED RESEARCH IN APPLIED SCIENCES AND ENGINEERING TECHNOLOGY
ISSN 2462 - 1943

Security Analysis on LUC-type Cryptosystems Using Common Modulus Attack

Izzatul Nabila Sarbini[1], Tze Jin Wong[2,3,*], Lee Feng Koo[2], Ahmad Fadly Nurullah Rasedee[4], Fatin Hana Naning[2], Mohammad Hasan Abdul Sathar[5]

[1] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia
[2] Faculty of Humanities, Management and Science, Universiti Putra Malaysia, Bintulu Campus, 97008 Bintulu, Sarawak, Malaysia
[3] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia
[4] Faculty of Economi and Mualamat, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia
[5] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 15 November 2022
Received in revised form 27 December 2022
Accepted 17 January 2023
Available online 18 February 2023

Keywords:
Common modulus; Decryption; Sncryption; Keys; Lucas sequence

ABSTRACT

LUC-type cryptosystems are asymmetric key cryptosystems based on the Lucas sequence that is extended from RSA. The security challenge is comparable to RSA, which is based on the intractability of factoring a large number. This paper analysed the security of LUC, LUC3, and LUC4,6 cryptosystems using a common modulus attack. For a common modulus attack to be successful, a message must be transmitted to two distinct receivers with the same modulus. The strengths and limitations of the LUC, LUC3, and LUC4,6 cryptosystems when subjected to a common modulus attack were discussed as well. The results reveal that the LUC4,6 cryptosystem provides greater security than the LUC and LUC3.

1. Introduction

Cryptography is the process or technique of transforming plaintext to ensure that information is secure and inaccessible to intruders. It has become one of the most important components of computer and network security to ensure the confidentiality and integrity of data and protect it from unauthorised access. In addition, public demand for cryptographic systems has increased, especially given the widespread use of e-commerce in the digital economy, such as internet banking, shopping and payment. Currently, there is a growing awareness that the potential work of cryptography is in line with environmental sustainability as framework in the Sustainable Development Goals (SDGs) [1] through investment in technological innovation. Therefore, in the future, further exploration of the use of cryptography in line with environmental sustainability may be considered in the context of renewable energy research [2-4] in conjunction with strategies to improve health and preserve our planet.

[*] *Corresponding author.*
E-mail address: w.tzejin@upm.edu.my

https://doi.org/10.37934/araset.29.3.206213

The concept of public key cryptography, which uses two different keys, i.e. public encryption key and private decryption key, was discovered by Diffie and Hellman [5] in 1976. The public key is made public and used for enciphering, whilst another key is kept secret and used for deciphering. Both keys are crucial components of digital communication systems and are frequently employed in information security to maintain the system's confidentiality. Nevertheless, the concept of public key cryptography was not substantiated until the breakthrough in public key cryptography in 1978, which provided the world with a new paradigm through the pioneering practical implementation of cryptography by three mathematicians, Rivest, Shamir, and Adleman [6]. As a result, it became known as the RSA cryptosystem.

RSA exploits an integer factorisation problem that was previously one of the irresolvable number theoretic problems. Currently, RSA cryptosystem is the most promising and widely used system. It is extensively used to safeguard digital data in web browsers, smart cards, and chat applications such as WhatsApp. Accordingly, academicians and researchers focus their efforts on enhancing the efficiency and effectiveness of RSA and its security.

The LUC cryptosystem is an extension of RSA cryptosystem based on the Lucas function proposed by Smith and Lennon [7]. It has been modified to boost security or efficiency by taking advantage of the recurring character of the Lucas sequence. Inspired by their effort, Said and Loxton [8] and Wong *et al.,* [9] worked on LUC3 and LUC4,6 cryptosystems, intending to eliminate all potential weaknesses. LUC is a cryptosystem based on quartic polynomials. The LUC3 cryptosystem is extended from the LUC cryptosystem based on a cubic polynomial. In comparison, LUC4,6 is an extension of LUC and LUC3 cryptosystems based on quadratic polynomials. Additionally, Smith and Skinner [10] developed another public key cryptosystem analogous to the Diffie-Hellman and El-Gamal cryptosystems [11] and later presented another cryptosystem - LUCELG cryptosystems - to boost their efficiency.

A common modulus attack is an attack that can be used to recover the original plaintext when plaintext is encrypted via two different keys in the same modulus. This attack works if and only if these two different keys are relatively prime to each other.

The authenticity of data and information when it is stored or transmitted across the network is heavily reliant on encryption and decryption processes. Emulating sophisticated cryptanalytic attack techniques is critical for determining a cryptosystem's strengths and weaknesses. As a result, numerous studies on cryptanalytic attacks and efficiency analyses have been conducted [12-23]. This study uses common modulus attacks to evaluate the security of LUC, LUC3, and LUC4,6 cryptosystems.

2. Preliminaries

2.1 Mathematics Background

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

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

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

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

Definition 1. Suppose that the second order of the Lucas function is denoted as $V_k(a_1, 1) = \alpha^k + \beta^k$ and $U_k(a_1, 1) = \frac{\alpha^k - \beta^k}{\alpha - \beta}$, then

$$2V_{a+b}(xa_1, 1) = V_a(a_1, 1)V_b(a_1, 1) + DU_a(a_1, 1)U_b(a_1, 1) \tag{3}$$

$$V_{ab}(a_1, 1) = V_a(V_b(a_1, 1),1), \text{ and} \tag{4}$$

$$U_{ab}(a_1, 1) = U_a(U_b(a_1, 1),1). \tag{5}$$

where D is the discriminant of quadratic polynomial.

Definition 2. Suppose that $V_k(a_1, a_2, 1) = \alpha^k + \beta^k + \gamma^k$, $U_k'(a_1, a_2, 1) = \alpha^k + \omega^2\beta^k + \omega\gamma^k$, and $U_k''(a_1, a_2, 1) = \alpha^k + \omega\beta^k + \omega^2\gamma^k$ with $\omega = \frac{-1+\sqrt{-3}}{2}$, then

$$3V_{a+b}(a_1, a_2, 1) = V_aV_b + U_a'U_b'' + U_a''U_b', \tag{6}$$

$$V_{ab}(a_1, a_2, 1) = V_a(V_b(a_1, a_2, 1), V_b(a_2, a_1, 1), 1), \tag{7}$$

$$U'_{ab}(a_1, a_2, 1) = U'_a(U'_b(a_1, a_2, 1), U'_b(a_2, a_1, 1), 1), \tag{8}$$

$$U''_{ab}(a_1, a_2, 1) = U''_a(U''_b(a_1, a_2, 1), U''_b(a_2, a_1, 1), 1). \tag{9}$$

Definition 3. Suppose that $V_k(a_1, a_2, a_3, 1) = \alpha^k + \beta^k + \gamma^k + \lambda^k$, $U_k'(a_1, a_2, a_3, 1) = \alpha^k - \beta^k + \gamma^k - \lambda^k$, $U_k''(a_1, a_2, a_3, 1) = \alpha^k - \beta^k - \gamma^k + \lambda^k$ and $U_k'''(a_1, a_2, a_3, 1) = \alpha^k + \beta^k - \gamma^k - \lambda^k$, then

$$4V_{a+b}(a_1, a_2, a_3, 1) = V_aV_b + U_a'U_b''' + U_a''U_b'' + U_a'''U_b'. \tag{10}$$

$$\begin{aligned} T_{ab}(a_1, a_2, a_3, 1) = T_a(&T_b(a_1, a_2, a_3, 1), T_b(a_2, a_1a_3 - 1, a_1^2 + a_3^2 - 2a_2, a_1a_3 - 1, a_2, 1),\\ &T_b(a_3, a_2, a_1, 1), 1) \end{aligned} \tag{11}$$

where T_{ab}, T_a and T_b can be representative $V, U', U''$and U'''. Note that, $T_b(a_2, a_1a_3 - 1, a_1^2 + a_3^2 - 2a_2, a_1a_3 - 1, a_2, 1)$ is sixth-order linear recurrence sequence based on quartic polynomial.

Definition 4. For sixth order Lucas function, all kind of functions are denoted as $V_k = \alpha_1^k + \alpha_2^k + \alpha_3^k + \alpha_4^k + \alpha_5^k + \alpha_6^k$, $U_k' = \alpha_1^k + \omega\alpha_2^k + \omega^2\alpha_3^k + \alpha_4^k + \omega\alpha_5^k + \omega^2\alpha_6^k$, $U_k'' = \alpha_1^k + \omega^2\alpha_2^k + \omega\alpha_3^k + \alpha_4^k + \omega^2\alpha_5^k + \omega\alpha_6^k$, $U_k''' = \alpha_1^k + \alpha_2^k + \alpha_3^k - \left(\alpha_4^k + \alpha_5^k + \alpha_6^k\right)$, $U_k^{IV} = \alpha_1^k + \omega\alpha_2^k + \omega^2\alpha_3^k - \left(\alpha_4^k + \omega\alpha_5^k + \omega^2\alpha_6^k\right)$, and $U_k^V = \alpha_1^k + \omega^2\alpha_2^k + \omega\alpha_3^k - \left(\alpha_4^k + \omega^2\alpha_5^k + \omega\alpha_6^k\right)$ with $\omega = \frac{-1+\sqrt{-3}}{2}$, then the $(a+b)$-th term of sixth order Lucas function can be defined as

$$6V_{a+b}(a_1, a_2, a_3, a_4, a_5, 1) = V_aV_b + U_a'U_b'' + U_a''U_b' + U_a'''U_b''' + U_a^{IV}U_b^V + U_a^VU_b^{IV}. \tag{12}$$

Since the LUC4,6 cryptosystem is a system based on a quartic polynomial, then the roots of the polynomial for sixth order Lucas sequence in the LUC4,6 cryptosystem were modified to 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 a quartic polynomial. Note that all the sequences defined above satisfy the linear recurrence sequence defined in Eq. (1).

2.2 LUC-type Cryptosystem

This section discusses the different types of LUC-type cryptosystems. Like other public key cryptosystems, the computational time of encryption and decryption relies on the size of public key, e , private key, d, and the plaintext message, M as well as the value of modulus, $n = pq$, where p and q are a large prime number. LUC-type cryptosystems algorithm consists of three processes, i.e., the process of encryption, the process of key generation, and the process of decryption. The encryption process will produce the ciphertext, C, whilst the plaintext, M will be recovered through the decryption process.

2.2.1 LUC cryptosystem

In the process of encryption, the generation of ciphertext can be defined as

$$c \equiv V_e(m, 1) \; mod \; n. \tag{13}$$

In the process of generation of the decryption key, the receiver can compute

$$ed \equiv 1 \; mod \; \phi(n), \tag{14}$$

where

$$\phi(n) = \left(p - \left(\frac{c^2-4}{p}\right)\right)\left(q - \left(\frac{c^2-4}{q}\right)\right) \tag{15}$$

with $\left(\frac{C^2-4}{p}\right)$ and $\left(\frac{C^2-4}{q}\right)$ are the Legendre symbols. It is clear that the Legendre symbols are either $+1$ or -1.

Similar to the generation of ciphertext, the original plaintext can be calculated by replacing the encryption key with the decryption key, and the plaintext is replaced with ciphertext in Eq. (13).

2.2.2 LUC3 cryptosystem

The encryption function is defined by

$$E(m_1, m_2) = \left(V_e(m_1, m_2, 1), V_e(m_2, m_1, 1)\right) \equiv (c_1, c_2) \; mod \; n \tag{16}$$

with initial values $V_0(x_1, x_2, 1) = 3$, $V_1(x_1, x_2, 1) = x_1$, and $V_2(x_1, x_2, 1) = x_1^2 - 2x_2$.

The process of generation of the decryption key is similar to LUC cryptosystem, whilst Euler totient function, $\phi(n)$ corresponds to cubic equation. To decrypt the message, the user evaluates

$$D(c_1, c_2) = \left(V_d(c_1, c_2, 1), V_d(c_2, c_1, 1)\right) \equiv (m_1, m_2) \; mod \; n \tag{17}$$

which recovers the original plaintexts completely.

2.2.2 LUC4,6 cryptosystem

The process of encryption is defined by

$$E(m_1, m_2, m_3,) = (V_e(m_1, m_2, m_3, 1), V_e(m_2, m_1m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1),\\ V_e(m_3, m_2, m_1, 1) mod\ n. \quad (18)$$

Analogous to LUC3 and LUC cryptosystems, the decryption key of the LUC4,6 system is the inverse of e modulo $\phi(n)$. However, in this case, the Euler totient function corresponds to quartic equation. In order to recover the original plaintext, the user evaluates

$$D(c_1, c_2, c_3,) = (V_d(c_1, c_2, c_3, 1), V_d(c_2, c_1c_3 - 1, c_1^2 + c_3^2 - 2c_2, c_1c_3 - 1, c_2, 1)\\ V_d(c_3, c_2, c_1, 1) mod\ n. \quad (19)$$

3. Results

The common modulus attack is one of the homomorphic attacks with respect to multiplication structure based on homomorphic nature. The attack works in the situation when a message is encrypted using the same RSA modulus but a distinct public encryption key, which are relatively prime to each other. Following, we analyse the strength and weaknesses of variants of LUC-type cryptosystems via common modulus attack. In the common modulus attack, there are two pairs of public encryption and private decryption keys, (e_1, d_1) and (e_2, d_2) with e_1 and e_2 are relatively prime to each other. There exist $u, v \in \mathbb{Z}$ such that $ue_1 + ve_2 = 1$ by using the Euclidean algorithm.

Theorem 1. In the LUC cryptosystem, the ciphertext c_1 and c_2 which corresponds to the plaintext m is given by $c_1 \equiv V_{e_1}(m, 1)\ mod\ n$ and $c_2 \equiv V_{e_2}(m, 1)\ mod\ n$. Then the plaintext m can be recovered without the decryption key d_1 or d_2 by calculating

$$m \equiv 2^{-1}\big(V_u(c_1, 1)V_v(c_2, 1) + (c_2^2 - 4)U_u(c_1, 1)U_v(c_2, 1)\big)\ mod\ n. \quad (20)$$

Proof. Since $(e_1, e_2) = 1$, then exist $u, v \in \mathbb{Z}$ such that $ue_1 + ve_2 = 1$. Therefore,

$$V_u(c_1, 1)V_v(c_2, 1) + (c_2^2 - 4)U_u(c_1, 1)U_v(c_2, 1)\\ \equiv V_{d_2ue_1}(c_2, 1)V_v(c_2, 1) + (c_2^2 - 4)U_{d_2ue_1}(c_2, 1)U_v(c_2, 1)\\ \equiv V_{d_2ue_1+v}(c_2, 1) \equiv V_{ue_1+ve_2}(m, 1) \equiv 2m\ mod\ n.$$

Due to $V_k(x_1, 1) = \alpha^k + \beta^k$ and $U_k(x_1, 1) = \frac{\alpha^k - \beta^k}{\alpha - \beta}$, where α and β are the roots of quadratic polynomial $x^2 - x_1x + 1 = 0$, then the initial values $V_0(x_1, 1) = 2$, $V_1(x_1, 1) = x_1$, $U_0(x_1, 1) = 0$ and $U_1(x_1, 1) = 1$. Thus, the original plaintext can be recovered without a decryption key by calculating Eq. (20).

Theorem 2. In the LUC3 cryptosystem, the ciphertexts which are corresponding to the plaintexts m_1 and m_2 are denoted as $c_{1,1} \equiv V_{e_1}(m_1, m_2, 1)\ mod\ n$, $c_{1,2} \equiv V_{e_1}(m_2, m_1, 1)\ mod\ n$, $c_{2,1} \equiv V_{e_2}(m_1, m_2, 1)\ mod\ n$, and $c_{2,2} \equiv V_{e_2}(m_2, m_1, 1)\ mod\ n$, then the plaintexts can be recovered by calculating

$$m_1 \equiv 3^{-1}\Big(V_u(c_{1,1},c_{1,2},1)V_v(c_{2,1},c_{2,2},1) + U'_u(c_{1,1},c_{1,2},1)U''_v(c_{2,1},c_{2,2},1) + U''_u(c_{1,1},c_{1,2},1)U'_v(c_{2,1},c_{2,2},1)\Big) \; mod \; n \tag{21}$$

and

$$m_2 \equiv 3^{-1}\Big(V_u(c_{1,2},c_{1,1},1)V_v(c_{2,2},c_{2,1},1) + U'_u(c_{1,2},c_{1,1},1)U''_v(c_{2,2},c_{2,1},1) + U''_u(c_{1,2},c_{1,1},1)U'_v(c_{2,2},c_{2,1},1)\Big) \; mod \; n. \tag{22}$$

Proof. Since $(e_1, e_2) = 1$, then exist $u, v \in \mathbb{Z}$ such that $ue_1 + ve_2 = 1$. Therefore,

$$\begin{aligned}
&V_u(c_{1,1},c_{1,2},1)V_v(c_{2,1},c_{2,2},1) + U'_u(c_{1,1},c_{1,2},1)U''_v(c_{2,1},c_{2,2},1) + U''_u(c_{1,1},c_{1,2},1)U'_v(c_{2,1},c_{2,2},1)\\
&\equiv V_{d_2ue_1}(c_{2,1},c_{2,2},1)V_v(c_{2,1},c_{2,2},1) + U'_{d_2ue_1}(c_{2,1},c_{2,2},1)U''_v(c_{2,1},c_{2,2},1) +\\
&\quad U''_{d_2ue_1}(c_{2,1},c_{2,2},1)U'_v(c_{2,1},c_{2,2},1)\\
&\equiv 3V_{d_2ue_1+v}(c_{2,1},c_{2,2},1) \equiv 3V_{ue_1+ve_2}(m_1,m_2,1) \equiv 3m_1 \; mod \; n.
\end{aligned}$$

A similar method for recovering the plaintext m_2. Thus, the plaintexts can be recovered by computing Eq. (21) and Eq. (22).

Theorem 3. In the LUC4,6 cryptosystem, the ciphertexts which are corresponding to the plaintexts m_1, m_2, and m_3 are denoted as $c_{1,1} \equiv V_{e_1}(m_1, m_2, m_3, 1) \; mod \; n$, $c_{1,2} \equiv V_{e_1}(m_2, m_1m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1) \; mod \; n$, $c_{1,3} \equiv V_{e_1}(m_3, m_2, m_1, 1) \; mod \; n$, $c_{2,1} \equiv V_{e_2}(m_1, m_2, m_3, 1) \; mod \; n$, $c_{2,2} \equiv V_{e_2}(m_2, m_1m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1) \; mod \; n$, and $c_{2,3} \equiv V_{e_2}(m_3, m_2, m_1, 1) \; mod \; n$, then the plaintexts can be recovered by calculating

$$m_1 \equiv 4^{-1}\Big(V_u(c_{1,1},c_{1,2},c_{1,3},1)V_v(c_{2,1},c_{2,2},c_{2,3},1) + U'_u(c_{1,1},c_{1,2},c_{1,3},1)U'''_v(c_{2,1},c_{2,2},c_{2,3},1) + U''_u(c_{1,1},c_{1,2},c_{1,3},1)U''_v(c_{2,1},c_{2,2},c_{2,3},1) + U'''_u(c_{1,1},c_{1,2},c_{1,3},1)U'_v(c_{2,1},c_{2,2},c_{2,3},1)\Big) \; mod \; n, \tag{23}$$

$$m_2 \equiv 6^{-1}\big(V_u(A)V_v(B) + U'_u(A)U'''_v(B) + U''_u(A)U''_v(B) + U'''_u(A)U'_v(B)\big) \; mod \; n, \tag{24}$$

$$m_3 \equiv 4^{-1}\Big(V_u(c_{1,3},c_{1,2},c_{1,1},1)V_v(c_{2,3},c_{2,2},c_{2,1},1) + U'_u(c_{1,3},c_{1,2},c_{1,1},1)U'''_v(c_{2,3},c_{2,2},c_{2,1},1) + U''_u(c_{1,3},c_{1,2},c_{1,1},1)U''_v(c_{2,3},c_{2,2},c_{2,1},1) + U'''_u(c_{1,3},c_{1,2},c_{1,1},1)U'_v(c_{2,3},c_{2,2},c_{2,1},1)\Big) \; mod \; n, \tag{25}$$

where $A = (c_{1,2}, c_{1,1}c_{1,3} - 1, c_{1,1}^2 + c_{1,3}^2 - 2c_{1,2}, c_{1,1}c_{1,3} - 1, c_{1,2}, 1)$ and
$B = (c_{2,2}, c_{2,1}c_{2,3} - 1, c_{2,1}^2 + c_{2,3}^2 - 2c_{2,2}, c_{2,1}c_{2,3} - 1, c_{2,2}, 1)$.

Proof. Since $(e_1, e_2) = 1$, then exist $u, v \in \mathbb{Z}$ such that $ue_1 + ve_2 = 1$. Therefore,

$$\begin{aligned}
&V_u(c_{1,1},c_{1,2},c_{1,3},1)V_v(c_{2,1},c_{2,2},c_{2,3},1) + U'_u(c_{1,1},c_{1,2},c_{1,3},1)U'''_v(c_{2,1},c_{2,2},c_{2,3},1) +\\
&\quad U''_u(c_{1,1},c_{1,2},c_{1,3},1)U''_v(c_{2,1},c_{2,2},c_{2,3},1) + U'''_u(c_{1,1},c_{1,2},c_{1,3},1)U'_v(c_{2,1},c_{2,2},c_{2,3},1)\\
&\equiv V_{d_2ue_1}(c_{2,1},c_{2,2},c_{2,3},1)V_v(c_{2,1},c_{2,2},c_{2,3},1) + U'_{d_2ue_1}(c_{2,1},c_{2,2},c_{2,3},1)U'''_v(c_{2,1},c_{2,2},c_{2,3},1) +\\
&\quad U''_{d_2ue_1}(c_{2,1},c_{2,2},c_{2,3},1)U''_v(c_{2,1},c_{2,2},c_{2,3},1) + U'''_{d_2ue_1}(c_{2,1},c_{2,2},c_{2,3},1)U'_v(c_{2,1},c_{2,2},c_{2,3},1)\\
&\equiv 4V_{d_2ue_1+v}(c_{2,1},c_{2,2},c_{2,3},1) \equiv 4V_{ue_1+ve_2}(c_{2,1},c_{2,2},c_{2,3},1) \equiv 4m_1 \; mod \; n.
\end{aligned}$$

A similar method for recovering the plaintexts m_2 and m_3.

Theoretically, the eavesdropper can break the implementation of the LUC4,6 encryption system and reveal the original message using Theorem 3. However, it is difficult to recover the original plaintexts or messages due to the unable obtaining the initial values of the sequences, U', U'', U''', U^{IV}, and U^{V}. Currently, as far as we know, the initial values for the sequences U', U'', U''', U^{IV}, and U^{V} can be found by calculating the roots of quartic polynomial, not the coefficients of quartic polynomial. Consequently, the process of revealing the original plaintexts or messages is unable to be accomplished via common modulus attack when using LUC4,6 cryptosystem. This implies that the security of LUC4,6 cryptosystem is more competent than other's LUC-type cryptosystems.

4. Conclusions

The strength and weaknesses of the variants of LUC cryptosystems have been studied via Common Modulus Attack. Results showed that the eavesdropper could break the encryption system and recover the original plaintext or message successfully when the sender uses a same system modulus to encrypt the plaintext or message to two different receivers in the LUC or LUC3 cryptosystem. However, the eavesdropper unable to reveal the original plaintexts or messages for LUC4,6 cryptosystem without knowing the decryption key due to the difficulties in obtaining the initial values of the sequences, U', U'', U''', U^{IV}, and U^{V} where the initial values are based on coefficients or original plaintexts. This implies that the LUC4,6 cryptosystem withstands the common modulus attack. By using common modulus attack, it can be concluded that LUC4,6 cryptosystem is more secure compared to LUC and LUC3 cryptosystem. As a part of future work, the quintic system can be developed to improve its encryption system and attack resistance performance. Further, the enhanced cryptosystem will be analysed against possible cryptanalysis to ensure the system can safeguard the end users.

References

[1] Parmentola, Adele, Antonella Petrillo, Ilaria Tutore, and Fabio De Felice. "Is blockchain able to enhance environmental sustainability? A systematic review and research agenda from the perspective of Sustainable Development Goals (SDGs)." *Business Strategy and the Environment* 31, no. 1 (2022): 194-217. https://doi.org/10.1002/bse.2882

[2] Samsudin, Muhammad Syazwan Nizam, Md Mizanur Rahman, and Muhamad Azhari Wahid. "Sustainable power generation pathways in Malaysia: Development of long-range scenarios." *Journal of Advanced Research in Applied Mechanics* 24, no. 1 (2016): 22-38.

[3] Ilham, Zul. "Multi-criteria decision analysis for evaluation of potential renewable energy resources in Malaysia." *Progress in Energy and Environment* 21 (2022): 8-18. https://doi.org/10.37934/progee.21.1.818

[4] Yong, Jiunn Boon, Lian See Tan, and Jully Tan. "Comparative life cycle assessment of biomass-based and coal-based activated carbon production." *Progress in Energy and Environment* 20 (2022): 1-15. https://doi.org/10.37934/progee.20.1.115

[5] Diffie, W., and M. E. Hellman. "" New Directions in Cryptography" IEEE Transactions on Information Theory, v. IT-22, n. 6." (1976). https://doi.org/10.1109/TIT.1976.1055638

[6] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21, no. 2 (1978): 120-126. https://doi.org/10.1145/359340.359342

[7] Smith, Peter J., and Michael JJ Lennon. "LUC: A New Public Key System." In *SEC*, pp. 103-117. 1993.

[8] Said, Mohamad Rushdan Md, and John Loxton. "A cubic analogue of the RSA cryptosystem." *Bulletin of the Australian Mathematical Society* 68, no. 1 (2003): 21-38. https://doi.org/10.1017/S0004972700037382

[9] Jin, Wong Tze, Mohamad Rushdan Md Said, Kamel Ariffin Mohd Atan, and Bekbaev Ural. "The Quartic Analog to the RSA Cryptosystem."

[10] Smith, Peter, and Christopher Skinner. "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms." In *Advances in Cryptology—ASIACRYPT'94: 4th International*

Conferences on the Theory and Applications of Cryptology Wollongong, Australia, November 28–December 1, 1994 Proceedings, pp. 355-364. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005. https://doi.org/10.1007/BFb0000447

[11] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." *IEEE transactions on information theory* 31, no. 4 (1985): 469-472. https://doi.org/10.1109/TIT.1985.1057074

[12] Ahmad, Musheer, Mohammad Najam Doja, and Mirza Mohd Sufyan Beg. "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system." *Journal of King Saud University-Computer and Information Sciences* 33, no. 1 (2021): 77-85. https://doi.org/10.1016/j.jksuci.2018.02.002

[13] Jin, Wong Tze, Hailiza Kamarulhaili, and Mohd Rushdan Md Said. "On the Hastad's Attack to LUC\(_ {4, 6}\) Cryptosystem and Compared with Other RSA-Type Cryptosystem." *Malaysian Journal of Mathematical Sciences* 7 (2013): 1-17.

[14] Joye, Marc. "Security analysis of RSA-type cryptosystems." PhD diss., PhD thesis, Université catholique de Louvain, 1997.

[15] Koo, Lee Feng, Tze Jin Wong, Fatin Hana Naning, Pang Hung Yiu, Mohammad Hasan Abdul Sathar, and Ahmad Fadly Nurullah Rasedee. "Security analysis on elliptic curve cryptosystem based on second order lucas sequence using faults based attack." *Advances in Mathematics: Scientific Journal* 9, no. 12 (2020): 10845-10854. https://doi.org/10.37418/amsj.9.12.69

[16] bin Sarbini, Izzatul Nabila, Wong Tze Jin, Koo Lee Feng, Mohamed Othman, Mohd Rushdan Md Said, and Yiu Pang Hung. "Garbage-man-in-the-middle (type 2) Attack on the Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Group Over Finite Field." In *Cryptology and Information Security Conference 2018*, p. 35. 2018.

[17] Sarbini, I. N., L. F. Koo, T. J. Wong, and F. H. Naning. "FH, PH 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, no. 11 (2019): 1193-1196.

[18] Wong, Tze Jin, Lee Feng Koo, Fatin Hana Naning, Pang Hung Yiu, Ahmad Fadly Nurullah Rasedee, Mohamad Maulana Magiman, and Mohammad Hasan Abdul Sathar. "On the security comparison of luc-type cryptosystems using chosen message attack." *Advances in Mathematics: Scientific Journal* 9, no. 12 (2020): 10883-10894. https://doi.org/10.37418/amsj.9.12.72

[19] Wong, Tze Jin, Mohd Rushdan Md Said, Mohamed Othman, and Lee Feng Koo. "On the common modulus attack into the LUC4, 6 cryptosystem." In *AIP Conference Proceedings*, vol. 1660, no. 1, p. 090052. AIP Publishing LLC, 2015. https://doi.org/10.1063/1.4926641

[20] Wong, Tze Jin, Mohd Rushdan Md Said, Mohamed Othman, and Lee Feng Koo. "A Lucas based cryptosystem analog to the ElGamal cryptosystem and elliptic curve cryptosystem." In *AIP Conference Proceedings*, vol. 1635, no. 1, pp. 256-259. American Institute of Physics, 2014. https://doi.org/10.1063/1.4903592

[21] Jin, Wong Tze, Mohd Rushdan Md. Said, Mohamed Othman, and Koo Lee Feng. "A method to decrease computation time for fourth order Lucas sequence." In *AIP Conference Proceedings*, vol. 1557, no. 1, pp. 55-58. American Institute of Physics, 2013. https://doi.org/10.1063/1.4823874

[22] WONG, TZEJIN, IZZATUL NABILA SARBINI, LEE FENG KOO, FATIN HANA NANING, MOHAMED OTHMAN, and MOHAMAD MAULANA MAGIMAN. "AN ALGORITHM FOR REDUCING LUC4, 6 AND LUC4, 6ELG CRYPTOSYSTEMS COMPUTATIONAL TIME."

[23] Savić, Dragan, Petar Milić, Borislaw Mazinjanin, and Petar Spalević. "Cryptanalytic attacks on RSA algorithm and its variants." *Przegląd Elektrotechniczny* 98, no. 2 (2022): 14-20. https://doi.org/10.15199/48.2022.02.04