ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **10** (2021), no.11, 3439–3447
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.11.5

A CUBIC EL-GAMAL ENCRYPTION SCHEME BASED ON LUCAS SEQUENCE AND ELLIPTIC CURVE

Tze Jin Wong[1], Lee Feng Koo[1], Fatin Hana Naning, Ahmad Fadly Nurullah Rasedee, Mohamad Maulana Magiman, and Mohammad Hasan Abdul Sathar

ABSTRACT. The public key cryptosystem is fundamental in safeguard communication in cyberspace. This paper described a new cryptosystem analogous to El-Gamal encryption scheme, which utilizing the Lucas sequence and Elliptic Curve. Similar to Elliptic Curve Cryptography (ECC) and Rivest-Shamir-Adleman (RSA), the proposed cryptosystem requires a precise hard mathematical problem as the essential part of security strength. The chosen plaintext attack (CPA) was employed to investigate the security of this cryptosystem. The result shows that the system is vulnerable against the CPA when the sender decrypts a plaintext with modified public key, where the cryptanalyst able to break the security of the proposed cryptosystem by recovering the plaintext even without knowing the secret key from either the sender or receiver.

1. INTRODUCTION

Cryptology is part of the number theory. It is regarding the application of formulas and algorithms. The roots of cryptology are cryptography and cryptanalysis. Cryptography is a study or technique to safeguard private data. In contrast, cryptanalysis is a study of methods to obtain confidential data without the sender's

[1]*corresponding author*

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

Key words and phrases. ciphertext, cubic, elliptic curve, Lucas sequence, plaintext.

Submitted: 20.10.2021; *Accepted:* 12.11.2021; *Published:* 23.11.2021.

concern. There are three types of cryptography - private key or symmetric cryptography, public key or asymmetric cryptography, and cryptographic hash function (CHF). Private key cryptography is an encryption technique in which the plaintext or ciphertext is encrypted or decrypted using just a private key. The public key is an encryption mechanism that uses both a private key and public key. The private key is kept secret and used to decrypt the ciphertext, whereas the public key is made open and used to encrypt the plaintext. The cryptographic hash function is a technique that maps the message or plaintext into a bit array of a message digest.

The emergence of Corona Virus Disease (COVID-19) has increased in online transactions and usage. This phenomenon combined with the ever-evolving technology, necessitates a concomitant focus on cybersecurity. Therefore, many studies regarding cryptology were done in the past few years [1–5]. In this paper, a new public key cryptography was proposed. The proposed cryptosystem is analogous to the El-Gamal encryption scheme [6], LUCELG [7], and Menezes-Vanstone Elliptic Curve Cryptography (MVECC). At the same time, it is based on the cubic of Lucas sequence and elliptic curve. The proposed cryptosystem's security problem is similar to Rivest-Shamir-Adleman (RSA) [8] cryptosystem and Elliptic Curve Cryptography (ECC) [9, 10] based on mathematical problem's intractability. To assess its security, the chosen plaintext attack (CPA) was chosen. The CPA is an attack for cryptanalysis in which the attacker or hacker can encrypt the plaintexts and obtain the corresponding ciphertext. Using an alternative algorithm, the attacker or hacker can decrypt any ciphertext without knowing the secret key.

2. Preliminaries

2.1. **Third Order of Lucas Sequence.** The third order of Lucas sequence is a recurrence sequence of integers, V_k defined by,

$$V_k = a_1 V_{k-1} - a_2 V_{k-2} + V_{k-3}, \tag{2.1}$$

for $k \geq 3$. The initial values for (2.1) is defined as

$$\begin{aligned} V_0 &= 3, \\ V_1 &= a_1, \\ V_2 &= a_1^2 - 2a_2, \end{aligned}$$

where a_1 and a_2 are coefficients for cubic polynomial,

$$x^3 - a_1x^2 + a_2x + 1 = 0. \tag{2.2}$$

Suppose that α, β, γ are the roots of cubic polynomial defined in (2.2), then the $(a+b)$-th term of third order Lucas sequence can be defined as follows.

Definition 2.1. *The $(a+b)$-th term of third order Lucas sequence [11] is defined as*

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

where

$$V_n(a_1, a_2, 1) = \alpha^n + \beta^n + \gamma^n$$

$$U_n(a_1, a_2, 1) = \alpha^n + \omega^2\beta^n + \omega\gamma^n$$

$$W_n(a_1, a_2, 1) = \alpha^n + \omega\beta^n + \omega^2\gamma^n$$

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

Note that the sequences U_n and W_n are satisfy the linear recurrence properties

$$T_k = a_1T_{k-1} - a_2T_{k-2} + T_{k-3}.$$

Definition 2.2. *The (ab)-th term of third order Lucas sequence [11] is defined as*

$$3V_{ab}(a_1, a_2, 1) = V_a(V_b(a_1, a_2, 1), V_b(a_2, a_1, 1), 1).$$

2.2. **Elliptic Curve.** Suppose that finite field or Galois field denote as F_p with p elements, then the equation for the elliptic curve over F_p is defined as

$$y^2 = x^3 + \alpha x + \beta,$$

where α and β are elements for F_p and $4\alpha^3 + 27\beta^2 \neq 0$. The set group G is defined as

$$G(H) = \{(x, y) \in H \times H | y^2 = x^3 + \alpha x + \beta\} \cup \{\infty\}$$

for field H contains F_p.

3. THE SYSTEM

Suppose that a general group G will be defined based on the elliptic curve defined in Section 2.2, then the system modulus, n is the order of the group G. In this system, the Diffie-Hellman Key Exchange method was used to obtain the encryption key. Firstly, the sender and receiver choose a secret key $R \in G$ together. Then, the sender and receiver decided their own secret key $a \in G$ and $b \in G$, respectively. Finally, the receiver generates his public key $Q = bR \in G$. Note that the public key for this system is not the encryption key. Whilst, the public key is the encryption key for others public key cryptosystems, i.e. RSA, LUC, LUC3, LUC4,6 etc.

Theorem 3.1. *Support that the plaintexts denoted as* (m_1, m_2) *and the ciphertexts denoted as*

$$\begin{aligned} c_1 &\equiv aR \mod n, \\ c_2 &\equiv V_{aQ}(m_1, m_2, 1) \mod n, \\ c_3 &\equiv V_{aQ}(m_2, m_1, 1) \mod n, \end{aligned}$$

then, the original plaintexts can recovered by computing

$$m_1 \equiv V_d(c_2, c_3, 1) \mod n$$

and

$$m_2 \equiv V_d(c_3, c_2, 1) \mod n,$$

where d *is decryption key.*

Proof. The theorem can be proved based on the concept of the inverse of recurrence sequence.

Suppose that the cubic equation is defined as

$$f(x) = x^3 - m_1 x^2 + m_2 x - 1,$$

then, the Euler totient function can be defined as

$$\phi(n) = \begin{cases} n^2 + n + 1, & \text{if } f(x) \mod n \text{ is of type of } t[3] \\ n^2 - 1, & \text{if } f(x) \mod n \text{ is of type of } t[2,1] \\ n - 1, & \text{if } f(x) \mod n \text{ is of type of } t[1] \end{cases}, \tag{3.1}$$

where $t[3]$ is an irreducible cubic equation, $t[2,1]$ is the product of an irreducible quadratic equation and a linear factor, and $t[1]$ is the product of three linear factors.

The inverse of encryption key is denoted as decryption key d, where the encryption key defined as

$$e = b \cdot c_1.$$

Thus, the decryption key can be obtained by calculating

$$d \equiv e^{-1} \mod \phi(n).$$

As such, the original plaintext can be recovered by evaluating

$$\begin{aligned} m_1 &\equiv V_d(c_2, c_3, 1) \equiv V_{(bc_1)^{-1}}(c_2, c_3, 1) \\ &\equiv V_{(baR)^{-1}}(V_{aQ}(m_1, m_2, 1), V_{aQ}(m_2, m_1, 1), 1) \\ &\equiv V_{(baR)^{-1}}(V_{abR}(m_1, m_2, 1), V_{abR}(m_2, m_1, 1), 1) \\ &\equiv V_1(m_1, m_2, 1) \equiv m_1 \mod n \end{aligned}$$

and

$$\begin{aligned} m_2 &\equiv V_d(c_3, c_2, 1) \equiv V_{(bc_1)^{-1}}(c_3, c_2, 1) \\ &\equiv V_{(baR)^{-1}}(V_{aQ}(m_2, m_1, 1), V_{aQ}(m_1, m_2, 1), 1) \\ &\equiv V_{(baR)^{-1}}(V_{abR}(m_2, m_1, 1), V_{abR}(m_1, m_2, 1), 1) \\ &\equiv V_1(m_2, m_1, 1) \equiv m_2 \mod n \end{aligned}$$

□

Practically, the receiver does not have the plaintexts to compute the Euler totient function. However, the receiver able to calculate the Euler totient function by using

$$g(x) = x^3 - c_2x^2 + c_3x - 1.$$

Hence, the type of $g(x)$ must be the same as the type of $f(x)$. Thus, the value of a, b, and R must be relatively prime to $n - 1$, $n^2 - 1$, and $n^2 + n + 1$ in order to ensure that their are in the same type.

4. The Attack

In this study, the CPA had been selected to analyse the security of proposed system. The CPA enable the cryptanalyst to choose plaintexts and view the corresponding ciphertexts or obtain the signatures.

Theorem 4.1. *The cryptanalyst is able to obtain the sender's signatures* (s_1, s_2) *if the sender decrypt the plaintext* (m_1, m_2) *by using modified public key* Q' *in the cubic El-Gamal encryption scheme based on Lucas sequence and elliptic curve, where the signatures defined as*

$$s_1 \equiv V_d(m_1, m_2, 1) \mod n,$$
$$s_2 \equiv V_d(m_2, m_1, 1) \mod n,$$

Proof. Suppose that a and b are the secret keys for the sender and receiver, respectively. R is the secret key for both sender and receiver. The public key Q is defined in Section 3. The encryption key is denoted as

$$e = aQ = abR,$$

the decryption key is denoted as

$$d = e^{-1} \mod \phi(n),$$

and the signatures for the sender is denoted as

$$s_1 \equiv V_d(m_1, m_2, 1) \mod n,$$
$$s_2 \equiv V_d(m_2, m_1, 1) \mod n,$$

where (m_1, m_2) are the plaintexts.

First, the cryptanalyst chooses the plaintexts (m_1, m_2) and generated a transformation key k where k is relatively prime to a, b, R, $n-1$, n^2-1, n^2+n+1 and in the group G defined in Section 2.2.

Then, the cryptanalyst modified the public key Q by integrating the transformation key k. The modified public key is denoted as

$$Q' = kQ.$$

Next, the cryptanalyst asks the sender to decrypt the chosen plaintexts (m_1, m_2) by using the modified public key Q'. If the sender does not aware that the received public key is fake and decrypted the chosen plaintexts, then the sender will generated the faulty signatures (s_1', s_2') as follows,

$$e' = aQ',$$
$$d' = e'^{-1} \mod \phi(n),$$
$$s_1' \equiv V_{d'}(m_1, m_2, 1) \mod n,$$

and

$$s_2' \equiv V_{d'}(m_2, m_1, 1) \mod n,$$

where $\phi(n)$ is defined in (3.1).

Lastly, if the cryptanalyst able to obtain the faulty signatures (s_1', s_2') from the sender. Thus, the cryptanalyst manages to obtain the real signatures (s_1, s_2) by calculating

$$\begin{aligned} s_1 &\equiv V_d(m_1, m_2, 1) \equiv V_{(abR)^{-1}}(m_1, m_2, 1) \\ &\equiv V_{k(kabR)^{-1}}(m_1, m_2, 1) \\ &\equiv V_{kd'}(m_1, m_2, 1) \\ &\equiv V_k(V_{d'}(m_1, m_2, 1), V_{d'}(m_2, m_1, 1), 1) \\ &\equiv V_k(s_1', s_2', 1) \mod n, \end{aligned}$$

and

$$\begin{aligned} s_2 &\equiv V_d(m_2, m_1, 1) \equiv V_{(abR)^{-1}}(m_2, m_1, 1) \\ &\equiv V_{k(kabR)^{-1}}(m_2, m_1, 1) \\ &\equiv V_{kd'}(m_2, m_1, 1) \\ &\equiv V_k(V_{d'}(m_2, m_1, 1), V_{d'}(m_1, m_2, 1), 1) \\ &\equiv V_k(s_2', s_1', 1) \mod n. \end{aligned}$$

□

5. Conclusion

In this study, a new cryptosystem to safeguard private data was proposed. This cryptosystem is analogous to the El-Gamal encryption scheme and integrated with the third order of Lucas sequence and elliptic curve. The CPA was adopted to analyse the security of the cryptosystem. The system is defenceless against the CPA if the sender decrypts a plaintext with a modified public key. The cryptanalyst is capable of obtaining the signature without having the secret key from the sender and receiver. As such, the cryptanalyst manages to recover the other plaintexts by using the signature. Consequently, relevant improvements are needed to make the system variant vulnerable.

ACKNOWLEDGMENT

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

REFERENCES

[1] T. J. WONG, L. F. KOO, F. H. NANING, P. H. YIU, A. F. N. RASEDEE, M. M. MAGIMAN, AND M. H. A. SATHAR: *On the security comparison of luc-type cryptosystems using chosen message attack*, Advances in Mathematics: Scientific Journal **9**(12) (2020), 10883–10894.

[2] L. F. KOO, T. J. WONG, F. H. NANING, P. H. YIU, A. F. N. RASEDEE, AND M. H. A. SATHAR: *Security analysis on elliptic curve cryptosystem based on second order lucas sequence using faults based attack*, Advances in Mathematics: Scientific Journal **9**(12) (2020), 10845–10854.

[3] I. N. SARBINI, L. F. KOO, T. J. WONG, F. H. NANING, F.H., AND 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.

[4] I. N. SARBINI, T. J. WONG, L. F. KOO, M. OTHMAN, M. R. M. SAID, AND 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.

[5] T. J. WONG, M. R. M. SAID, M. OTHMAN, AND L. F. KOO : *A Lucas based cryptosystem analog to the ElGamal cryptosystem and elliptic curve cryptosystem*, AIP Conference Proceedings **1635** (2014), 256–259.

[6] T. ELGAMAL: *A Public Key Cryptosystem and A signature Scheme Based on Discrete Logarithms*, IEEE Transaction on Information Theory **31** (1985), 469–472.

[7] P. J. SMITH AND C. SKINNER: *A Public Key Cryptosystem and A Digital Signature Systems Based on the Lucas Function Analogue to Discrete Logarithms*, Pre-proceedings Asia Crypt'94 (1994), 298–306.

[8] R. RIVEST, A. SHAMIR, AND L. ADLEMAN: *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communication of the ACM **21** (1978), 120–126.

[9] N. KOBLITZ: *Elliptic curve cryptosystems*, Mathematics of Computation **48**(177) (1985), 203–209.

[10] V. MILLER: *Use of elliptic curves in cryptography*, CRYPTO **85** (1985), 417–426.

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

Department of Science and Technology
Universiti Putra Malaysia, Bintulu Campus
Nyabau Road, 97008 Bintulu, Sarawak, Malaysia
and
Institute for Mathematical Research
Universiti Putra Malaysia
43300 UPM Serdang, Selangor, 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

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