MATHEMATICAL MODELING AND COMPUTING, Vol. 11, No. 4, pp. 1135–1140 (2024)

An attack on ELG-LUC3-ECC cryptosystem using Hastad's and Julta's theorem

Wong T. J.[1,2], Koo L. F.[1], Sathar M. H. A.[3], Rasedee A. F. N.[4], Sarbini I. N.[5]

[1] *Universiti Putra Malaysia, Bintulu Campus, Nyabau Road, 97008 Bintulu, Sarawak, Malaysia*
[2] *Baotou Teachers' College of Inner Mongolia Science & Technology University, No. 3, Kexue Road, Baotou 014030, Qingshan District, Inner Mongolia, China*
[3] *Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*
[4] *Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia*
[5] *Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia*

(Received 21 July 2024; Accepted 25 November 2024)

In this study, an attack on the El-Gamal encryption scheme ELG-LUC3-ECC is proposed, which is based on a third-order Lucas sequence over an elliptic curve finite field, using Hastad's and Julta's theorems. Hastad's theorem was used to solve the problem of multivariate modular equations system, whereas Julta's theorem was used to find the solutions of multivariable modular equation. As a result, the minimum amount of plaintext required for a successful attack may be determined. Thus, similar attacks can be prevented if the quantity of plaintext remains within the appropriate range.

Keywords: *cubic; El-Gamal; Hastad's theorem; Julta's theorem; Lucas sequence.*
2010 MSC: 94A60, 11T71 **DOI:** 10.23939/mmc2024.04.1135

1. Introduction

Cryptography is a study of encrypting plaintext using an encryption key and decrypting ciphertext using a decryption key. Public Key Cryptography (PKC) is a cryptographic system that exposes encryption keys which was proposed by Diffie and Hellman [1] in 1978.

In 1985, El-Gamal [2] proposed a digital signature scheme which was using Diffie–Hellman key exchange method to generate the encryption key and now known as the El-Gamal encryption scheme (ELG). Smith and Skinner [3] extended ELG in 1994, by integrating it with the second order Lucas function, dubbed LUCELG. In 2014, Wong and his team [4] modified LUCELG by incorporating it in an elliptic curve over a finite field, that is now referred as ELG-LUC-ECC. Based on the characteristics of elliptic curve and second order Lucas function, the security of modified cryptosystem had been improved [5–7]. Said and Loxton [8] proposed LUC3, a cubic cryptosystem based on the Lucas sequence. Miller [9] developed a cryptography based on elliptic curve in 1985. At the same time, Koblitz [10] developed the cryptography based on elliptic curve too. Now, these cryptosystems call as Elliptic Curve Cryptography (ECC). The foundation of these cryptosystems is a discrete logarithm problem in the group of point of an elliptic curve defined over a finite field.

In 2021, Wong et al. [11] introduced ELG-LUC3-ECC, a new cryptosystem that combines the ELG, LUC3, and ECC cryptosystems. A security analysis on ELG-LUC3-ECC is presented in this paper utilising Hastad's and Coppersmith's theorems.

2. ELG-LUC3-ECC

Suppose that

$$y^2 = x^3 + ax + b \tag{1}$$

is the equation of elliptic curve with a and b are elements for a finite field F_p and $4a^3 + 27b^2 \neq 0$, then exist a set of group G

$$G(Z) = \{(x, y) \in Z \times Z | y^2 = x^3 + ax + b\} \cup \{\infty\} \tag{2}$$

for field H contains F_p.

In ELG-LUC3-ECC, the system modulus denoted as n, where n is the order of group G, and the encryption key, $e = stR \in G$ is generated by a key exchange method, whereas $R \in G$ is a secret number known to both sender and receiver, $s \in G$ is a secret number for sender, and $t \in G$ is a secret number for receiver. In this case, the encryption key for ELG-LUC3-ECC is not the receiver's public key. The receiver's public key is $Q = tR \in G$.

In the process of encryption, the sender will generate the ciphertexts as follows:

$$c_1 = sR, \tag{3}$$

$$c_2 \equiv V_{sQ}(m_1, m_2, 1) \mod n, \tag{4}$$

$$c_3 \equiv V_{sQ}(m_2, m_1, 1) \mod n, \tag{5}$$

where m_1 and m_2 denoted as plaintexts and c_1 and c_2 denoted as ciphertexts.

Before recovering the original plaintexts, the receiver should be calculating the decryption key while the decryption key is depending on encryption key. Therefore, the receiver needs to calculate the encryption key by

$$e = tc_1. \tag{6}$$

After getting the encryption key, the receiver can generate the decryption key by

$$d \equiv e^{-1} \mod \phi(n), \tag{7}$$

where

$$\phi(n) = \begin{cases} n^2 + n + 1, \text{ if } g(x) \mod n \text{ is an irreducible cubic,} \\ n^2 - 1, \text{ if } g(x) \mod n \text{ is product of irreducible quadratic and a linear factor,} \\ n - 1, \text{ if } g(x) \mod n \text{ is roduct of three linear factors,} \end{cases} \tag{8}$$

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

In essence, the receiver is able to compute the original plaintexts by

$$m_1 \equiv V_d(c_2, c_3, 1) \mod n, \tag{9}$$

$$m_2 \equiv V_d(c_3, c_2, 1) \mod n. \tag{10}$$

3. An attack

There are several theorems will be used in Hastad's attack. The first theorem will be discussed is Hastad's theorem which is a theorem to solve the multivariate modular equations system.

Theorem 1. *Let* $N = \prod_{i=1}^{k} n_i$ *and* $n = \min\limits_{1<i<k}(n_i)$. *Given a set of* k *equations* $\sum_{j=0}^{\delta} a_{i,j}x^j \equiv 0 \mod n_i$ *where all the modulus* n_i *are relatively prime to each other and* $\gcd(\langle a_{i,j}\rangle_{j=0}^{\delta}, n_i) = 1$ *for all values of* i. *Then,* $x < n$ *in polynomial time can be found if* $N > 2^{(\delta+1)(\delta+2)/4}(\delta+1)^{\delta+1}n^{\delta(\delta+1)/2}$.

Proof. Refer [12, 13]. ∎

Theorem 2. *Assume that the* p *modular polynomial system with degree* $\leqslant k$ *and* l *variables denoted as*

$$\sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\ldots+j_l\leqslant k} a_{i,j_1,j_2,\ldots,j_i}x_1^{j_1}x_2^{j_2}\ldots x_l^{j_l} \equiv 0 \mod n_i, \tag{11}$$

for $i = 1, \ldots, p$, $x_1, \ldots, x_i < n$ *and* $n = \min\limits_{1<i<k}(n_i)$. *Let* $N = \prod_{i=1}^{p} n_i$, $f = \sum_{m=1}^{\delta} m\binom{m+l-1}{m}$ *and* $g = \sum_{m=0}^{\delta} m\binom{m+l-1}{m}$, *if all the modulus* n_i *are relatively prime to each other, then* $\gcd\left(\langle a_{i,j_1,j_2,\ldots,j_l}\rangle_{j_1,j_2,\ldots,j_l}^{j_1+j_2+\ldots+j_l\leqslant\delta}, n_i\right) = 1$ *for* $i = 1, \ldots, p$ *and if*

$$N > 2^{g(g+1)/4}g^g n^f \tag{12}$$

the result is a real-valued equation in polynomial time which is equivalent to Eq. (11).

Proof. Refer [13]. ∎

Coppersmith's theorem [14] is an extended result from Hastad's theorem. This theorem is used to find the solution of a modular equation. It is specific for a single variable integer polynomial with degree k. The integer polynomial in ELG-LUC3-ECC is a multivariable polynomial. Thus, Julta's Theorem [15] is used to solve this problem. Before discussing Julta's theorem, it is important to understand Coppersmith's theorem, which is specific to single variable integer polynomial.

Theorem 3. *Suppose that a single variable integer polynomial $P(x)$ with degree k and a positive integer N of unknown factorization, then in time polynomial in $\log(N)$ and k, all integer solutions x_0 to $P(x_0) \equiv 0 \mod N$ with $\mid x_0 \mid < N^{1/k}$ can be found.*

Proof. Refer [13, 14]. ∎

In 1998, Julta [15] improved Coppersmith's theorem, in which it is able to find the integer solution for multivariable polynomial.

Theorem 4. *Let $P(x_1, \ldots, x_m) \equiv 0 \mod N$ be a m variables polynomial with total degree k and a root x_0, then exist an algorithm with determines $c(\geqslant 1)$ integer polynomial equation of total degree in $cmk\log(N)$, in time polynomial in $cmk\log(N)$, such that x_0 as a root for each of the equation.*

Proof. Refer [15]. ∎

Let m_1 and m_2 are the plaintexts of ELG-LUC3-ECC, then

$$m_{1,i} \equiv \alpha_i m_1 + \beta_i \mod n_i, \tag{13}$$

and

$$m_{2,i} \equiv \alpha_i m_2 + \beta_i \mod n_i. \tag{14}$$

The corresponding ciphertexts can be generated by computing

$$c_{1,i} = s_i R_i, \tag{15}$$

$$c_{2,i} \equiv V_{s_iQ_i}(m_{1,i}, m_{2,i}, 1) \mod n, \tag{16}$$

$$c_{3,i} \equiv V_{s_iQ_i}(m_{2,i}, m_{1,i}, 1) \mod n. \tag{17}$$

Since the third order of Lucas sequence in ELG-LUC3-ECC is equal to two variables of Dickson polynomial [16, 17], then

$$\begin{aligned} V_{s_iQ_i}(m_{1,i}, m_{2,i}, 1) &= D_{s_iQ_i}(m_{1,i}, m_{2,i}, 1) \\ &= \sum_{i=0}^{\lfloor s_iQ_i/2 \rfloor} \sum_{j=0}^{\lfloor s_iQ_i/3 \rfloor} \frac{s_iQ_i(-1)^i}{s_iQ_i - i - 2j} \binom{s_iQ_i - i - 2j}{i+j} \binom{i+j}{i} m_{1,i}^{s_iQ_i - 2i - 3j} m_{2,i}^{i}, \end{aligned} \tag{18}$$

where $2i+3j \leqslant s_iQ_i$. Similar for $V_{s_iQ_i}(m_{2,i}, m_{1,i}, 1)$. Thus, $c_{2,i}$ and $c_{3,i}$ can be considered as polynomial in term of $m_{1,i}$ and $m_{2,i}$ with degree s_iQ_i.

Corollary 1. *Suppose that $N = \prod_{i=1}^{k} n_i$ and $n = \min\limits_{1<i<k}(n_i)$. Given a set of k equations $\sum_{j_1,j_2=0}^{j_1+j_2\leqslant\delta} a_{i,j_1,j_2} x_1^{j_1} x_2^{j_2} \equiv 0 \mod n_i$ where all the modulus n_i are relatively prime to each other and $\gcd(\langle a_{i,j_1,j_2}\rangle_{j_1,j_2}^{j_1+j_2\leqslant\delta}, n_i) = 1$ for all values of i. Then, $x < n$ in polynomial time can be found if*

$$N > 2^{(\delta+1)(\delta+2)(\delta^2+3\delta+4)/16} \left(\frac{1}{2}(\delta+1)(\delta+2)\right)^{\frac{1}{2}(\delta+1)(\delta+2)} n^{\frac{1}{3}\delta(\delta+1)(\delta+2)}. \tag{19}$$

Proof. In two variable case for Theorem 1.

$$f = \sum_{m=1}^{\delta} m \binom{m+1}{m} = \frac{1}{3}\delta(\delta+1)(\delta+2), \tag{20}$$

$$g = \sum_{m=0}^{\delta} m \binom{m+1}{m} = \frac{1}{2}\delta(\delta+1)(\delta+2), \tag{21}$$

Replace Eq. (20) and Eq. (21) into Eq. (12) will get Eq. (19). ∎

Corollary 2. *Let k be the number of set of the plaintexts in ELG-LUC3-ECC such as $(m_{1,1}, m_{2,1}), \ldots, (m_{1,k}, m_{2,k})$, then the original plaintexts can be recovered if*

$$k > \frac{1}{3}sQ(sQ+1)(sQ+2), \tag{22}$$

and

$$n > 2^{\frac{(sQ+1)(sQ+2)((sQ)^2+3sQ+4)}{16}} \left(\frac{1}{2}(sQ+1)(sQ+2)\right)^{\frac{1}{2}(sQ+1)(sQ+2)}, \tag{23}$$

where $sQ = \max\limits_{1 \leqslant i \leqslant k}(s_iQ_i)$.

Proof. The proof can be accomplished by verifying the conditions of Corollary 1 are satisfied. Since there are k set of plaintexts in ELG-LUC3-ECC, then exist k set of ciphertexts $(c_{1,1}, c_{2,1}, c_{3,1}), \ldots, (c_{1,k}, c_{2,k}, c_{3,k})$, and $2k$ equations

$$P_{1,i}(m_1, m_2) \equiv D_{s_iQ_i}(m_{1,i}, m_{2,i}, 1) - c_{2,i} \equiv 0 \mod n_i, \tag{24}$$

and

$$P_{2,i}(m_2, m_1) \equiv D_{s_iQ_i}(m_{2,i}, m_{1,i}, 1) - c_{3,i} \equiv 0 \mod n_i, \tag{25}$$

where $1 \leqslant i \leqslant k$. Assume that all the modulus n_i and the coefficients of Eq. (24) and Eq. (25) are relatively prime to each other, then

$$\begin{aligned} N = \prod_{i=1}^{k} n_i &\geqslant n_1 \prod_{i=2}^{\frac{1}{3}sQ(sQ+1)(sQ+2)+1} n_i \\ &> 2^{\frac{(sQ+1)(sQ+2)((sQ)^2+3sQ+4)}{16}} \left(\frac{1}{2}(sQ+1)(sQ+2)\right)^{\frac{1}{2}(sQ+1)(sQ+2)} \end{aligned} \tag{26}$$

if satisfied Eq. (22), Eq. (23) and $n = \min\limits_{1<i<k}(n_i)$. ∎

Based on Corollary 2, we find the maximum number of plaintexts in ELG-LUC3-ECC to avoid this type of attack. This mean that the system is secure if the number of plaintexts is less than the maximum number.

Table 1. Examples of the maximum number of plaintexts for ELG-LUC-ECC and ELG-LUC3-ECC.

sQ	1001 (10-bits)	3997 (12-bits)	15843 (14-bits)
ELG-LUC-ECC	501 501	79 900 003	125 508 246
ELG-LUC3-ECC	670 674 004	42 602 695 996	2 647 054 861 360

Therefore, Table 1 gives examples of the maximum number of plaintexts for ELG-LUC-ECC and ELG-LUC3-ECC in different bits system.

4. Conclusion

For the ELG-LUC3-ECC cryptosystem, the two-variable Dickson polynomials were used to transform the third-order Lucas sequence into two-variable polynomials. According to the theorems and corollaries presented in Section;3, if the number of plaintexts encrypted by ELG-LUC3-ECC exceeds $\frac{1}{3}sQ(sQ+1)(sQ+2)$, then the corresponding plaintexts can be recovered without the recipient's knowledge. Additionally, Table;1 indicates that the maximum allowable number of plaintexts for ELG-LUC3-ECC is greater than that for ELG-LUC-ECC.

In other words, ELG-LUC3-ECC requires a higher minimum number of plaintexts than ELG-LUC-ECC to execute an attack successfully. Thus, the results demonstrate that ELG-LUC3-ECC offers greater security than ELG-LUC-ECC.

[1] Diffie W., Hellman M. New Directions in Cryptography. IEEE Transaction on Information Theory. **22** (6), 644–654 (1976).

[2] Elgamal T. A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms. IEEE Transaction on Information Theory. **31** (4), 469–472 (1985).

[3] Smith P. J., Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms. Advances in Cryptology – ASIACRYPT'94. 355–364 (1994).

[4] Wong T. J., Said M. R. M., Othman M., Koo L. F. A Lucas based cryptosystem analog to the ElGamal cryptosystem and elliptic curve cryptosystem. AIP Conference Proceedings. **1635** (1), 256–259 (2014).

[5] Sarbini I. N., Wong T. J., Koo L. F., Othman M., Said M. R. M., Yiu P. H. Garbage-man-in-the-middle (type 2) attack on the Lucas based El-Gamal cryptosystem in the elliptic curve group over finite field. 6th International Cryptology and Information Security Conference. 35–41 (2018).

[6] Sarbini I. N., Wong T. J., Koo L. F., Naning F. H., Yiu P. H. 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), 1193–1196 (2019).

[7] Koo L. F., Wong T. J., Naning F. H., Yiu P. H., Sathar M. H. A., Rasedee A. F. N. Security Analysis on Elliptic Curve Cryptosystem Based on Second Order Lucas Sequence using Faults Based Attack. Advances in Mathematics: Scientific Journal. **9** (12), 10845–10854 (2020).

[8] Said M. R. M., Loxton J. A cubic analogue of the RSA cryptosystem. Bulletin of Australia Mathematical Society. **68** (1), 21–38 (2003).

[9] Miller V. Use of Elliptic Curves in Cryptography. Advances in Cryptology – CRYPTO'85 Proceedings. **85**, 417–426 (1985).

[10] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation. **48** (177), 203–209 (1987).

[11] Wong T. J., Koo L. F., Naning F. H., Rasedee A. F. N., Magiman M. M., Sathar M. H. A. A Cubic El-Gamal Encryption Scheme Based On Lucas Sequence And Elliptic Curve. Advances in Mathematics: Scientific Journal. **10** (11), 3439–3447 (2021).

[12] Hastad J. On using RSA with low exponent in a public key network. Advances in Cryptology – CRYPTO'85 Proceedings. 403–408 (1986).

[13] Joye M. Security Analysis of RSA-type Cryptosystems. PhD Thesis, Universite Catholique de Louvain, Belgium (1997).

[14] Coppersmith D. Finding a Small Root of a Univariate Modular Equation. Advances in Cryptology – EUROCRYPT'96. 155–165 (1996).

[15] Julta C. S. On finding small solutions of modular multivariate polynomial equations. Advances in Cryptology – EUROCRYPT'98. 158–170 (1998).

[16] Dickson L. E. The analytic representation of substitutuions on a power of a prime nnumber of letters with a discussion of the linear group. The Annals of Mathematics. **11** (1/6), 65–120 (1896).

[17] Lidl R. Theory and application of Dickson Polynomial. Topics in Polynomials of One and Several Variables and Their Applications. 371–395 (1993).

Атака на ELG-LUC3-ECC з використанням теореми Хастада та Юлти

Вонг Т. Дж.[1,2], Ку Л. Ф.[1], Сатар М. Х. А.[3], Раседі А. Ф. Н.[4], Сарбіні І. Н.[5]

[1] *Університет Путра Малайзія, Кампус Бінтулу, дорога Ньябау, 97008 Бінтулу, Саравак, Малайзія*
[2] *Педагогічний коледж науково-технічного університету Внутрішньої Монголії Баотоу, дорога Кешуе №3, Баотоу 014030, район Циншань, внутрішня Монголія, Китай*
[3] *Університет Путра Малайзія, 43400 UPM Серданг, Селангор, Малайзія*
[4] *Університет ісламських наук Малайзії, 71800 Нілай, Негері-Сембілан, Малайзія*
[5] *Саравакський університет Малайзії, 94300 Кота Самарахан, Саравак, Малайзія*

У цьому дослідженні запропоновано атаку на схему шифрування Ель–Гамаля, засновану на послідовності Лукаса третього порядку над скінченним полем еліптичної кривої з використанням теореми Хастада та Юлти. Теорема Хастада була використана для розв'язування задачі системи багатовимірних модульних рівнянь, тоді як теорема Юлта використовувалася для знаходження розв'язків багатовимірного модульного рівняння. У результаті можна визначити мінімальний обсяг відкритого тексту, який необхідний для успішної атаки. Отже, подібним атакам можна запобігти, якщо кількість відкритого тексту залишається в межах визначеного діапазону.

Ключові слова: *кубічний; Ель-Гамаль; теорема Хастада; теорема Джулта; послідовність Лукаса.*