International Journal of Cryptology Research 8(2): 1 - 10 (2018)

Common Modulus Attack Against Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Group Over Finite Field

Lee Feng Koo[*1,2], **Tze Jin Wong**[1,2], **Pang Hung Yiu**[2], **Izzatul Nabila Sarbini**[2,3], **Yee Min Kwan**[2], and **Fatin Hana Naning**[2]

[1]*Institute for Mathematical Research, Universiti Putra Malaysia*
[2]*Faculty of Agriculture and Food Science, Universiti Putra Malaysia, Bintulu Campus*
[3]*Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak.*

E-mail: leefeng@upm.edu.my
[*]*Corresponding author*

ABSTRACT

Common modulus attack is one of the various homomorphic attacks based on homomorphism nature of cryptosystems. This type of attack requires a plaintext encrypted under same modulus while two encryption keys are relatively prime to each other. In this paper, an investigation was carried out to evaluate the nature of a homomorphic attack on the Lucas based El-Gamal Cryptosystem in the elliptic curve group over finite field. The attack can be proven by using extend Euclidean algorithm together with composite and reverse functions of Lucas and Fibonacci sequences. Results showed that common modulus attack can be used to obtain the original plaintexts. Thus, it is dangerous to send a plaintext to two different users using same modulus. Sender must use different modulus to communicate with two different users.

Keywords: Decryption, Encryption, Fibonacci Sequence, Lucas Sequence, Modulus

1 INTRODUCTION

Diffie and Hellman (1976) were the first to propose the concept of public key cryptosystem. The public key cryptosystem contains two keys; a public key or encryption key, and a private key or decryption key. Accordingly, El-Gamal cryptosystem was introduced by El-Gamal (1985) which is based on Diffie-Hellman key exchange method. Further, Koblitz (1987) and Miller (1985) individually proposed the public key cryptosystem using elliptic curve group over finite field. The security of the elliptic curve cryptography depends on its ability to compute a point multiplication and the inability of the attacker to calculate the multiplicand using the given, the original and the product points. The size of the elliptic curve determines the difficulty of the problem.

In mathematics, Lucas sequences satisfy the linear recurrence relation. Generally, the second order of Lucas sequences represent the quadratics polynomials, the third order of Lucas sequence represent the cubic polynomial and so on. Due to the recurrence characteristics, Lucas sequences are used to develop the cryptosystem in order to increase its security or efficiency. Thereupon, Smith and Lennon (1993) has develiped LUC, followed by LUCELG (Smith and Skinner, 1994), based on second order of Lucas sequence. Said (1997) further expand the Lucas sequence potiential by developing LUC_3 based on its third order. $\text{LUC}_{4,6}$ has benn proposed by Wong et al. (2007) and Wong (2011) using fourth and sixth order. Additionally, Lucas based cryptosystem using elliptic cirve and analog to El-Gamal cryptosystem has been proposed by Wong et al. (2014). The security of this cryptosystem had been assessed by garbage-man-in-the-middle (type 1) attack (Wong et al., 2014), garbage-man-in-the-middle attack (type 2) attack (Sarbini et al., 2018), Wiener's attack (Wong et al., 2018b), and Lenstra's attack (Wong et al., 2018a).

In this paper, common modulus attack had been selected to analyse the security issue for Lucas based El-Gamal cryptosystem in the elliptic curve over finite flied. The common modulus attack is an attack relies on the cryptosystem's homomorphic nature. It will be succeeded if the sender sends the plaintext to two users under same modulus and both of public keys are relatively prime to each other. The common modulus attack had been conducted on RSA, LUC , KMOV and Demytko's cryptosystem by Joye (1997), small private exponent RSA by Hinek and Lam (2009), and LUC$_{4,6}$ cryptosystem by Wong et al. (2015).

2 PRELIMINARIES

A second order linear recurrence sequence defined by

$$T_k = PT_{k-1} - QT_{k-2}, \tag{1}$$

with initial values, $T_0 = a$ and $T_1 = b$ (where a and b are integers) and P, Q are the coefficients for a quadratic polynomial,

$$x^2 - Px + Q = 0. \tag{2}$$

Let α and β be the roots of (2), then $P = \alpha + \beta$ and $Q = \alpha\beta$. Therefore, Lucas function U_k and V_k can be defined by

$$U_k(P, Q) = \frac{\alpha^k - \beta^k}{\alpha - \beta} \tag{3}$$

and

$$V_k(P, Q) = \alpha^k + \beta^k. \tag{4}$$

Since $U_0 = 0$ and $U_1 = 1$, then $U_k(P, Q)$ is called Fibonacci sequence. Futher, $V_k(P, Q)$ is called Lucas sequence due to $V_0 = 2$ and $V_1 = P$. Both of sequences satisfy the linear recurrence sequence which defined in (1). Thus, equations (3) and (4) can be rewritten as

$$U_k(P, Q) = PU_{k-1}(P, Q) - QU_{k-2}(P, Q) \tag{5}$$

and

$$V_k(P, Q) = PU_{k-1}(P, Q) - QU_{k-2}(P, Q) \tag{6}$$

where $k \geq 2$.

Some important concepts which are used throughout this study will be defined as follows.

Definition 2.1. *The discriminant of quadratic polynomial can be defined as*

$$D = (\alpha - \beta)^2 \tag{7}$$

where α and β are the roots of quadratic polynomial.

Definition 2.2. *If $Q = \alpha\beta = 1$, and $P = \alpha + \beta$, then the discriminant of quadratic polynomial can be defined as*

$$D = P^2 - 4. \tag{8}$$

Definition 2.3. *The addition function for Lucas sequence can be defined as*

$$2V_{a+b} = V_a V_b + DU_a U_b \tag{9}$$

where D is defined in Definition 2.1 and 2.2.

Definition 2.4. *Let $Q = 1$, then the composite function of Lucas sequence can be defined as*

$$V_{ab}(P, 1) = V_a(V_b(P, 1), 1). \tag{10}$$

Definition 2.5. *Let $Q = 1$, then the composite function of Fibonacci sequence can be defined as*

$$U_{ab}(P, 1) = U_a(V_b(P, 1), 1). \tag{11}$$

Definition 2.6. *The Legendre symbol can be defined as*

$$\begin{aligned} \left(\frac{a}{p}\right) &= 0 \quad \textit{if } a \textit{ is divisible by } p, \\ &= 1 \quad \textit{if } a \textit{ quadratic modulus } p\ , \quad \textit{or} \\ &= -1 \quad \textit{if } a \textit{ is quadratic non residue modulus } p\ . \end{aligned} \tag{12}$$

Definition 2.7. *The Euler totient function for quadratic polynomial modulus $N = pq$ can be defined as*

$$\phi(N) = \left(p - \left(\frac{D}{p}\right)\right)\left(q - \left(\frac{D}{q}\right)\right) \tag{13}$$

where D is defined in Definition 2.1 and 2.2.

Definition 2.8. *Let $Q = 1$, $ed = k\phi(N) + 1$, and $N = pq$ where $\phi(N)$ is defined in Definition 2.7, then the reverse function of Lucas sequence can be defined as*

$$\begin{aligned} V_e(V_d(P, 1), 1) &\equiv V_{ed}(P, 1) \mod N \\ &\equiv V_{\phi(N)+1}(P, 1) \mod N \\ &\equiv V_1(P, 1) \equiv P \mod N. \end{aligned} \tag{14}$$

3 THE CRYPTOSYSTEM

Let $\mathbb{F}_N$ denotes a finite filed of N. Define two points as $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, respectively. An elliptic curve E defined over $\mathbb{F}_N$ is defined as

$$y^2 = x^3 + ax + b \tag{15}$$

where $a, b \in \mathbb{F}_N$ and $4a^3 + 27b^2 \neq 0$. For every field K containing $\mathbb{F}_N$, one considers the set:

$$E(K) = \{(x, y) \in K \times K | y^2 = x^3 + ax + b\} \cup \{\infty\} \tag{16}$$

In the Lucas based El-Gamal cryptosystem in the elliptic curve over finite field (Wong et al., 2014), a general group G will be defined based on elliptic curve and the order of the group G, N is the modulus of system, which is the product of two prime number, p and q.

Suppose the sender and the receiver intend to communicate by using Lucas based El-Gamal cryptosystem in the elliptic curve over finite field with order $N = pq$, then they will choose a secret number, R, which is an element of group G. The sender will choose his own private number, a, whilst the receiver will choose his own private number, b. Both a and b are elements in the group G. Subsequently, the receiver will generate the public key, defined as

$$Q = bR \in R \tag{17}$$

The sender will encrypt the plaintexts (m_x, m_y) using the public key, Q; and sends three ciphertexts (c_1, c_x, c_y) which defined as

$$\begin{aligned} c_1 &= aR \\ c_x &= V_{aQ}(m_x, 1) \mod N \qquad \text{and} \\ c_y &= V_{aQ}(m_y, 1) \mod N \end{aligned} \tag{18}$$

to the receiver where $V_{aQ}(m_x, 1)$ and $V_{aQ}(m_y, 1)$ are second order Lucas sequence which is defined in Section 2. Now, the receiver need to recover the original plaintext by compute the encryption key,

$$e = bc_1 \tag{19}$$

and generates the decryption keys,

$$\begin{aligned} d_x &= e^{-1} \mod \left[\left(p - \left(\frac{c_x^2-4}{p}\right)\right)\left(q - \left(\frac{c_x^2-4}{q}\right)\right)\right] \\ d_y &= e^{-1} \mod \left[\left(p - \left(\frac{c_y^2-4}{p}\right)\right)\left(q - \left(\frac{c_y^2-4}{q}\right)\right)\right] \end{aligned} \tag{20}$$

where $\left(\frac{c_i^2-4}{p}\right)$ and $\left(\frac{c_i^2-4}{q}\right)$ are Legendre symbol. Employ composite and reverse of Lucas sequences to obtain

$$\begin{aligned} V_{d_x}(c_x, 1) &\equiv m_x \mod N \\ V_{d_y}(c_y, 1) &\equiv m_y \mod N \end{aligned} \tag{21}$$

The receiver uses the ciphertext, c_x to compute the Legendre symbol. Therefore the both quadratic polynomials, $g_1(x) = x^2 - c_x x + 1$ and $f_1(x) = x^2 - m_x x + 1$ must be same type such that the Legendre symbols are $\left(\frac{c_x^2-4}{p}\right) = \left(\frac{m_x^2-4}{p}\right)$ and $\left(\frac{c_x^2-4}{q}\right) = \left(\frac{m_x^2-4}{q}\right)$. Similar situation is also applied to the ciphertext c_y. Thus, the values of a, b and R must be relative to p and q such that the plaintext can be recovered by the receiver correctly.

Consider the following cryptosystem using elliptic curve, $y^2 = x^3 + 13x + 21$ with the modulus $N = 10807$. The sender and receiver agreed to choose $R = 7$. Then, the sender and receiver choose their secret number, $a = 13$ and $b = 49$, respectively; and generates a public key, $Q = 343$. Now, the sender wants to encrypt a set of plaintext, $(m_x, m_y) = (20, 91)$ and send the ciphertext (c_1, c_x, c_y) to the receiver, where $(20, 91)$ is a point on the elliptic curve. Therefore, the sender computes

$$\begin{aligned} c_1 &= aR = 91 \\ c_x &= V_{4459}(20, 1) \mod 10807 \equiv 5933 \quad \text{and} \\ c_y &= V_{4459}(91, 1) \mod 10807 \equiv 1164 \end{aligned}$$

When the receiver receives the ciphertext, he will recover the original plaintext as follow steps:

1. Computes Legendre symbol:

$$\left(\frac{5933^2-4}{101}\right)=-1$$
$$\left(\frac{5933^2-4}{107}\right)=1$$
$$\left(\frac{1164^2-4}{101}\right)=1 \qquad \text{and}$$
$$\left(\frac{1164^2-4}{107}\right)=-1$$

2. Computes Encryption Key:

$$e=c_1\times b=4459$$

3. Generates Decryption Key:

$$\begin{aligned}d_x &\equiv 4459^{-1} \mod (101+1)(107-1)\equiv 3271 \mod 10812 \qquad \text{and}\\ d_y &\equiv 4459^{-1} \mod (101-1)(107+1)\equiv 3139 \mod 10800\end{aligned}$$

4. Recover the Original Plaintext:

$$\begin{aligned}m_x &= V_{3271}(5933,1) \mod 10807 = 20 \qquad \text{and}\\ m_y &= V_{3139}(1164,1) \mod 10807 = 91.\end{aligned}$$

4 THE ATTACK

Assume the sender wants to send a same plaintext (m_x, m_y) under same modulus $n = pq$ to two different receiver A and B using their public keys, $Q_A = b_AR_A$ and $Q_B = b_BR_B$, respectively. The ciphertexts $(c_{1,A}, c_{x,A}, c_{y,A})$ send to receiver A are

$$\begin{aligned}c_{1,A} &= a_AR_A,\\ c_{x,A} &= V_{a_AQ_A}(m_x,1) \mod N, \qquad \text{and}\\ c_{y,A} &= V_{a_AQ_A}(m_y,1) \mod N\end{aligned} \tag{22}$$

whilst the ciphertexts $(c_{1,B}, c_{x,B}, c_{y,B})$ send to receiver B are

$$\begin{aligned} c_{1,B} &= a_B R_B, \\ c_{x,B} &= V_{a_B Q_B}(m_x, 1) \mod N, \qquad \text{and} \\ c_{y,B} &= V_{a_B Q_B}(m_y, 1) \mod N, \end{aligned} \tag{23}$$

where a_A and a_B are secret number chosen by the sender, and $e_A = a_A Q_A$ and $e_B = a_B Q_B$ are relatively prime to each other.

Since $(e_A, a_B) = 1$, then the cryptanalyst uses the extend Euclidean algorithm to find $u, v \in \mathbb{Z}$ such that $ue_A + ve_B = 1$. Based on definitions defined in Section 2, cryptanalyst can compute

$$\begin{aligned} & V_u(c_{x,A}, 1)V_v(c_{x,B}, 1) + (c_{x,B}^2 - 4)U_u(c_{x,A}, 1)U_v(c_{x,B}, 1) \\ &\quad \equiv V_{ue_1}(m_x, 1)V_v(c_{x,B}, 1) + (c_{x,B}^2 - 4)U_{ue_1}(m_x, 1)U_v(c_{x,B}, 1) \\ &\quad \equiv V_{d_B ue_1}(c_{x,B}, 1)V_{e_B d_B v}(c_{x,B}, 1) \\ &\qquad + (c_{x,B}^2 - 4)U_{d_B ue_1}(c_{x,B}, 1)U_{e_B d_B v}(c_{x,B}, 1) \\ &\quad \equiv 2V_{d_B ue_A + e_B d_B v}(c_{x,B}, 1) \\ &\quad \equiv 2V_{ue_A + e_B v}(m_x, 1) \\ &\quad \equiv 2m_x \mod N. \end{aligned}$$

Similar calculation for the ciphertext m_y.

5 CONCLUSION

In this paper, an investigation was carried out to evaluate the nature of a homomorphic attack on the Lucas based El-Gamal Cryptosystem in the elliptic curve group over finite field. Result shows that the cryptanalyst is able to obtain the original plaintext if the sender sent a same plaintext using same modulus to two different users. Thus, the result suggested that the sender must using different modulus when the sender wants to send the plaintext to two users.

ACKNOWLEDGMENT

The authors would like to thank University Putra Malaysia for providing financial support under the Putra-Grant scheme (Vote no: 9588900).

REFERENCES

Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE Transaction on Information Theory*, 22:644–654.

El-Gamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transaction on Information Theory*, 31:469–472.

Hinek, M. J. and Lam, C. C. Y. (2009). Common modulus attacks on small private exponent rsa and some fast variants (in practice). In *Cryptology ePrint Archive*, pages 1–37.

Joye, M. (1997). *Security Analysis of RSA-type Cryptosystems*. PhD thesis, Universite Catholique de Louvain, Belgium.

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

Miller, V. (1985). Use of elliptic curves in cryptography. In *Advances in Cryptology ł CRYPTO 85 (Conference on the Theory and Application of Cryptographic Techniques) Proceedings*, volume 85, pages 417–426.

Said, M. (1997). *Application of Recurrence Relations to Cryptography*. PhD thesis, Macquarie University, Australia.

Sarbini, I. N., Wong, T. J., Said, M. R. M., Othman, M., Koo, L. F., and Yiu, P. H. (2018). Garbage-man-in-the-middle (type 2) attack on the lucas based el-gamal cryptosystem in the elliptic curve group over finite filed. In *Proceedings of the 6th International Cryptology and Information Security Conference 2018*, pages 35–41.

Smith, P. and Lennon, M. (1993). Luc: A new public key system. In *Proceedings of the ninth IFIP international Symposium on Computer Security*, pages 103–117.

Smith, P. and Skinner, C. (1994). A public key cryptosystem and a digital signature systems based on the lucas function analogue to discrete logarithms. In *ASIACRYPT 1994: Advances in Cryptology ł ASIACRYPT'94*, pages 298–306.

Wong, T. J. (2011). *A RSA-type Cryptosystem Based on Quartic Polynomials*. PhD thesis, Universiti Putra Malaysia, Malaysia.

Wong, T. J., Koo, L. F., and Yiu, P. H. (2018a). Lucas based el-gamal cryptosystem in the elliptic curve over finite field under lenstras attack. *Asian Journal of Mathematics and Computer Research*, 23(4):207–213.

Wong, T. J., Koo, L. F., and Yiu, P. H. (2018b). On the wieners attack into lucas based el- gamal cryptosystem in the elliptic curve over finite field. *International Journal of Science and Engineering Investigations vol 7*, 7:37–39.

Wong, T. J., Said, M. R. M., Atan, K. A. M., and Ural, B. (2007). The quartic analog to the rsa cryptosystem. *Malaysian Journal of Mathematical Sciences*, 1(1):63–81.

Wong, T. J., Said, M. R. M., Othman, M., and Koo, L. F. (2014). A lucas based cryptosystem analog to the elgamal cryptosystem and elliptic curve cryptosystem. In *AIP Conference Proceedings*, volume 1635, pages 256–259.

Wong, T. J., Said, M. R. M., Othman, M., and Koo, L. F. (2015). On the common modulus attack into $\text{luc}_4, 6$ cryptosystem. In *AIP Conference Proceedings*, volume 1660, page 090052.