International Journal of Cryptology Research 8(2): 24 - 38 (2018)

Security Analysis of Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Group Over Finite Field using Two Types of GMITM Attacks

Izzatul Nabila Sarbini[1,5], **Tze Jin Wong**[*1,2], **Lee Feng Koo**[1,2], **Mohamed Othman**[2,3], **Mohamad Rushdan Md Said**[2,4], and **Pang Hung Yiu**[1]

[1]*Department of Basic Science and Engineering, Universiti Putra Malaysia, Bintulu Campus.*
[2]*Institute for Mathematical Research, Universiti Putra Malaysia.*
[3]*Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia.*
[4]*Department of Mathematics, Faculty of Science, Universiti Putra Malaysia.*
[5]*Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak.*

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

ABSTRACT

The success of Garbage-man-in-the-middle (GMITM) attack relies on the possibility to access to the ”bin” of recipient in the cryptosystem. It is capable to recover the original plaintext by granting an entry to the ”bin”. There are basically two types of GMITM attacks, a polynomial attack and a homomorphic attacks. In this paper, an investigation was carried out to evaluate the polynomial structure of cryptosystem and the nature of a homomorphic attack on cryptosystem. The results show that the cryptanalyst could obtain the plaintext without knowing the secret number, a, b and R.

Keywords: Bin, Decryption, Elliptic Curve, Encryption, Lucas Sequence

1 INTRODUCTION

The concept of public key cryptography was proposed by Diffie and Hellman (1976). This is a cryptosystem making use of a public key and a private key. The public key is used to encrypt the plaintext and the private key is used to decrypt the ciphertext. El-Gamal (1985) introduced a signature scheme which is based on Diffie-Hellman key exchange method. This technique is now referred as El-Gamal Cryptosystem. The security problem of this cryptosystem is based on discrete logarithm. 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. Recently, Singh and Singh (2015) proposed a new technique where the classic technique of mapping the characters to affine points in the elliptic curve has been removed to perform the text cryptography using elliptic curve cryptography whilst Thangarasu and Selvakumar (2018) advocated modified Elliptical Curve Cryptography and Abelian group theory to solve linear system problem in sensor-cloud cluster computing.

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. $\mathrm{LUC}_{4,6}$ 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 attack (type 2) attack (Sarbini et al., 2018), Wiener's attack (Wong et al., 2018b), and Lenstra's attack (Wong et al., 2018a).

The garbage-man-in-the-middle (GMITM) attack is the attack derived from Davida's attack and further improved by Joye (1997). There are basically two type of GMITM attacks rely on the possibility of the cryptanalyst to access the "bin" of the recipient to success the attack. These attacks comprise of three important steps, i.e. the Lagranges modification step, the step of recovering corresponding plaintext, and concluded by the non-trivial relation step. In this paper, both GMITM attack had been selected to strike against the cryptosystem (Wong et al., 2014) which was based on Lucas sequence and in the elliptic curve group over finite field. The security performance of the cryptosystem was then assessed by using Wiener's attack (Wong et al., 2018b), Lenstra's attack (Wong et al., 2018a) and GMITM (type 2) (Sarbini et al., 2018). The GMITM attack had been used to evaluate the security levels (Joye, 1997) (Wong et al., 2009) of RSA, LUC , KMOV and Demytko's and $\mathrm{LUC}_{4,6}$ cryptosystems.

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

$$V_{ab}(P, 1) = V_a(V_b(P, 1), 1). \tag{9}$$

Definition 2.4. *The Legendre symbol can be defined as*

$$\begin{aligned}\left(\frac{a}{p}\right) &= 0 \quad \textit{if } a \textit{ is divisible by } p,\\ &= 1 \quad \textit{if } a \textit{ quadratic modulus } p \ , \quad \textit{or} \\ &= -1 \quad \textit{if } a \textit{ is quadratic non residue modulus } p \ .\end{aligned} \tag{10}$$

Definition 2.5. *The Euler totient function for quadratic polynomial modulus $N = pq$ can be defined as*

$$\phi(N) = \left(p - \left(\frac{D}{p}\right)\right)\left(q - \left(\frac{D}{q}\right)\right) \tag{11}$$

where D is defined in Definition 2.1 and 2.2.

Definition 2.6. *Let $Q = 1$, $ed = k\phi(N) + 1$, and $N = pq$ where $\phi(N)$ is defined in Definition 2.5, then the reverse function of Lucas sequence can be defined as*

$$\begin{aligned}V_e(V_d(P,1),1) &\equiv V_{ed}(P,1) \mod N\\ &\equiv V_{\phi(N)+1}(P,1) \mod N\\ &\equiv V_1(P,1) \equiv P \mod N.\end{aligned} \tag{12}$$

Definition 2.7. *The Dickson polynomial can be defined as*

$$D_n(x,a) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-1} \left(\begin{array}{c} n-i \\ n \end{array} \right) (-a)^i x^{n-2i} \tag{13}$$

where $\lfloor \frac{n}{2} \rfloor$ is largest integer less than $\frac{n}{2}$.

Futhermore, Dickson polynomial satisfy the linear recurrence sequence

$$D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a), \tag{14}$$

where $D_0(x,a) = 2$ and $D_1(x,a) = x$.

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:

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

4. Recover the Original Plaintext:

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

4 THE ATTACK

4.1 Garbage-man-in-the-middle Attack (Type 1)

The GMITM (type 1) attack rely on the polynomial structure of cryptosystem. Since Lucas sequence can be expressed in terms of Dickson polynomial, the GMITM attack can straightforwardly be adapted on Lucas based cryptosystem. So, as to make a success of GMITM attack, cryptanalyst should fulfill the following steps.

First step is Lagrange's modification step. In this step, the cryptanalyst intercepts, transforms and re-sends the ciphertext. The next step is recovering the corresponding plaintext. In this step, the cryptanalyst should be able to get corresponding plaintext from the receiver's "bin". Final step is a non-trivial relation step. The cryptanalyst will be able to recover the original plaintext in this step.

Theorem 4.1. *Lucas based El-Gamal Cryptosystem in the Elliptic Curve Group, G, over finite field is unsecure if the receiver decrypts the faulty ciphertexts and cryptanalyst could steal the corresponding decrypted faulty plaintexts.*

Proof. Suppose that N is the product of two prime numbers, p and q. Let R be an element of G which is only known to the sender and receiver. Both of sender and receiver chooses their secret number, $a \in G$ and $b \in G$, respectively; and generates the public key, $Q = bR \in G$. Suppose that (m_x, m_y) be the plaintexts and (c_1, c_x, c_y) be the ciphertexts where

$$\begin{aligned} c_1 &= aR \\ c_x &\equiv V_e(m_x, 1) \equiv V_{abR}(m_x, 1) \mod n \qquad \text{and} \\ c_y &\equiv V_e(m_y, 1) \equiv V_{abR}(m_y, 1) \mod n \end{aligned}$$

with the encryption key, $e = abR$, decryption key, $d \equiv e^{-1} \mod \Phi(N)$ and $\Phi(N)$ is Euler function.

Step 1 Lagrange's modification step

The cryptanalyst chooses a integers, $k \in G$ and $\gcd(k, Q) = 1$. Then, the cryptanalyst modifies the first ciphertext,

$$\begin{aligned} c'_x &\equiv V_k(c_x, 1) \mod N \qquad \text{and} \\ c'_y &\equiv V_k(c_y, 1) \mod N \end{aligned}$$

Step 2 Recovering step

The receiver will generates the decryption key by

$$\begin{aligned} d_x &= (bc_1)^{-1} \mod \left(p - \left(\frac{(c'_x)^2 - 4}{p}\right)\right)\left(q - \left(\frac{(c'_x)^2 - 4}{q}\right)\right) \\ d_y &= (bc_1)^{-1} \mod \left(p - \left(\frac{(c'_y)^2 - 4}{p}\right)\right)\left(q - \left(\frac{(c'_y)^2 - 4}{q}\right)\right). \end{aligned}$$

To decrypt the ciphertexts, c_x and c_y, the receiver computes

$$\begin{aligned} m'_x &\equiv V_{d_x}(c'_x, 1) \mod n \\ m'_y &\equiv V_{d_y}(c'_y, 1) \mod n. \end{aligned}$$

Step 3 Non-trivial relation step.

The cryptanalyst constructs the polynomial $P, Q \in G$

$$\begin{aligned} P(x) &\equiv D_e(x, 1) - c_x \mod N, \\ Q(x) &\equiv D_k(x, 1) - m'_x \mod N, \\ P(y) &\equiv D_e(y, 1) - c_y \mod N, \qquad \text{and} \\ Q(y) &\equiv D_k(y, 1) - m'_y \mod N. \end{aligned}$$

Since, m_x is root of polynomial $P(x)$ and $Q(x)$, and m_y is root of polynomial $P(y)$ and $Q(y)$, then

$$\begin{aligned} R(x) &= \gcd(P(x), Q(x)), \qquad \text{and} \\ R(y) &= \gcd(P(y), Q(y)). \end{aligned}$$

Thus, the cryptanalyst is able to obtain the value of (m_x, m_y) by solving $R(x)$ and $R(y)$ in x and y respectively.

■

As summary, cryptanalyst intercepts the original ciphertext (c_1, c_x, c_y) in the Lagrange's modification step. Subsequently, a random number k will be chosen to modify the second and third ciphertext and the modified ciphertexts, (c_1, c'_x, c'_y) will be sent to the receiver.

During the recovering step, the receiver obtain the ciphertexts, (c_1, c'_x, c'_y), and generate the decryption keys, d_x and d_y using the first ciphertext, c_1. He will then decrypts the faulty ciphertexts c'_x and c'_y to obtain the corresponding faulty plaintexts, m'_x and m'_y. Since the faulty plaintexts are meaningless, the faulty plaintexts will thrown into the bin.

If the cryptanalyst is able to obtain the faulty plaintexts from the receiver's bin in time, then he can recover the original plaintext using Non-trivial relation step.

4.2 Garbage-man-in-the-middle Attack (Type 2)

The GMITM (type 2) is an attack straightly extended from chosen plaintext attack. Similar to the GMITM (type 1) attack, GMITM (type 2) consists following three steps:

i. Lagrange's modification step

ii. Recovering step and

iii. Non-trivial relation step.

Theorem 4.2. *Lucas based El-Gamal Cryptosystem in the Elliptic Curve Group, G, over finite field is unsecure if the receiver decrypts the ciphertexts using faulty decryption key.*

Proof. Suppose that N is the product of two prime numbers, p and q. Let R be an element of G which is only known to the sender and receiver. Both of sender and receiver chooses their secret number, $a \in G$ and $b \in G$, respectively; and generates the public key, $Q = bR \in G$. Suppose that (m_x, m_y) be the plaintexts and (c_1, c_x, c_y) be the ciphertexts where

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

with the encryption key, $e = abR$, decryption key, $d \equiv e^{-1} \mod \Phi(N)$ and $\Phi(N)$ is Euler function.

Step 1 Lagrange's modification step
The cryptanalyst chooses a integers, $k \in G$ and $\gcd(k, Q) = 1$. Then, the cryptanalyst modifies the first ciphertexts, $c_1' = kc_1$.

Step 2 Recovering step

The receiver will generates the decryption key by

$$\begin{aligned} d'_x &= (bc'_1)^{-1} \mod \left(p - \left(\frac{c_x^2-4}{p}\right)\right)\left(q - \left(\frac{c_x^2-4}{q}\right)\right) \\ d'_y &= (bc'_1)^{-1} \mod \left(p - \left(\frac{c_y^2-4}{p}\right)\right)\left(q - \left(\frac{c_y^2-4}{q}\right)\right). \end{aligned}$$

To decrypt the ciphertexts, c_x and c_y, the receiver computes

$$\begin{aligned} m'_x &\equiv V_{d'_x}(c_x, 1) \mod n \\ m'_y &\equiv V_{d'_y}(c_y, 1) \mod n. \end{aligned}$$

Step 3 Non-trivial relation step.

The cryptanalyst is able to obtains the original plaintexts by evaluate

$$\begin{aligned} V_k(m'_x, 1) &\equiv V_k(V_{d'_x}(c_x, 1), 1) \equiv V_{kd_{x'}}(c_x, 1) \equiv V_{k(abkR)^{-1}}(c_x, 1) \\ &\equiv V_{(abR)^{-1}}(c_x, 1) \equiv m_x \mod n \\ V_k(m'_y, 1) &\equiv V_k(V_{d'_y}(c_y, 1), 1) \equiv V_{kd_{y'}}(c_y, 1) \equiv V_{k(abkR)^{-1}}(c_y, 1) \\ &\equiv V_{(abR)^{-1}}(c_y, 1) \equiv m_y \mod n \end{aligned}$$

■

In the Lagrange's modification step, the cryptanalyst intercepts the ciphertext. Subsequently, he chooses a random number, k, to modify the first ciphertext and sends the modified ciphertexts, (c'_1, c_x, c_y), to the receiver.

During the recovering step, the receiver receives the ciphertexts, (c'_1, c_x, c_y), and generates the decryption keys, d_x and d_y using the modified ciphertext, c'_1. Later, he decrypts the ciphertexts c_x and c_y in order to obtain the faulty plaintexts, m'_x and m'_y. Since the faulty plaintexts are meaningless, then the receiver will throws the faulty plaintexts into the bin.

If the cryptanalyst able to obtain the faulty plaintexts in the receiver's bin in time, then he can recover the original plaintext in Non-trivial relation step.

5 CONCLUSION

In this paper, an investigation was carried out to evaluate the polynomial and homomorphic structure 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 he can access the receiver's ”bin” in time. Thus, the result suggested that the receiver should always clean up his trash bin in time to avoid any type of GMITM attack.

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.

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.

Singh, L. and Singh, K. (2015). Implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science*, 54:73–82.

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.

Thangarasu, N. and Selvakumar, A. (2018). Improved elliptical curve cryptography and abelian group theory to resolve linear system problem in sensor-cloud cluster computing. *Cluster Computing*, pages 1–10.

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 Atan, K. A. M. (2009). Garbage-man-in-the-middle attack on the luc4 cryptosystem. *International Journal of Cryptology Research*, 1(1):33–41.

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.