International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:13, No:4, 2019

An Attack on the Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Group Over Finite Field Using Greater Common Divisor

Lee Feng Koo, Tze Jin Wong, Pang Hung Yiu, Nik Mohd Asri Nik Long

***Abstract*—**Greater common divisor (GCD) attack is an attack that relies on the polynomial structure of the cryptosystem. This attack required two plaintexts differ from a fixed number and encrypted under same modulus. This paper reports a security reaction of Lucas Based El-Gamal Cryptosystem in the Elliptic Curve group over finite field under GCD attack. Lucas Based El-Gamal Cryptosystem in the Elliptic Curve group over finite field was exposed mathematically to the GCD attack using GCD and Dickson polynomial. The result shows that the cryptanalyst is able to get the plaintext without decryption by using GCD attack. Thus, the study concluded that it is highly perilous when two plaintexts have a slight difference from a fixed number in the same Elliptic curve group over finite field.

***Keywords*—**Decryption, encryption, elliptic curve, greater common divisor.

I. Introduction

DIFFIE and Hellman [1] proposed the concept of public key cryptography in 1978. This is an encryption scheme that uses a public key and a private key. Public key can be freely shared, allowing users to encrypt their messages and verify their digital signature easily and conveniently. However, private key must be kept secret and only the sender or receiver can use it to decrypt the ciphertext or create the digital signature. El-Gamal [2] introduced a signature scheme which is based on Diffie-Hellman Key exchange method, which is now, referred as El-Gamal cryptosystem in 1985. The security of this cryptosystem is based on discrete logarithm problem. In the same year, Koblitz [3] and Miller [4] independently proposed the public key cryptosystem using elliptic curve group over finite field, which is referred as elliptic curve cryptography. The security problem of the elliptic curve cryptography is the ability to compute a point multiplication and the inability of the attacker to calculate the multiplicand using the given the original and product points. Therefore, the difficulty of the security problem is the size of the elliptic curve.

Lucas sequences are certain constant recursive integer sequences that satisfy the recurrence relation, $T_n = PT_{n-1} - QT_{n-2}$, where P and Q are integers. Generally, the Lucas sequences represent the polynomial in which P and Q are integer coefficients. Due to the recurrence characteristics, Lucas sequences are used to develop the cryptosystem in order to increase the security or efficiency. In this manner, LUCDIF, LUCELG [5], LUC [6], LUC_3 [7], and $LUC_{4,6}$ [8], [9] cryptosystems had been developed based on the Lucas sequences to increase their efficiency or security.

The Lucas sequence, $V_k(P, Q)$ satisfy the second order linear recurrence sequence,

$$V_k = PV_{k-1} - QV_{k-2} \tag{1}$$

where P and Q are the coefficients for quadratic polynomial.

Let α and β be the roots of the quadratic polynomial, then $P = \alpha + \beta$ and $Q = \alpha\beta$. Therefore, V_k can be defined by $V_k = \alpha^k + \beta^k$, with initial values $V_0 = 2$, and $V_1 = P$.

Dickson [10] studies various algebraic and number-theoretic properties of polynomials and introduced it in 1897. Now, these polynomials were called Dickson polynomial. The second order of first kind Dickson polynomial denoted by $D_n(x, a)$ is given as

$$D_n(x, a) = \sum_{i=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i} \tag{2}$$

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

Furthermore, Dickson polynomial satisfies the following recurrence

$$D_n(x, a) = xD_{n-1}(x, a) - aD_{n-1}(x, a), \tag{3}$$

with initial values $D_0(x, a) = 2$ and $D_1(x, a) = x$.

Therefore, it enables to consider the Lucas sequence as polynomial. since Lucas sequence can be modified to become a polynomial, it is possible to prove that the GCD attack has the ability to recover the original plaintext without knowing the decryption key.

Lee Feng Koo is with Department of Basic Science and Engineering, Universiti Putra Malaysia, Bintulu, Sarawak, 97008 Malaysia. She also is an associate research with Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor 43400 Malaysia (corresponding author, e-mail: leefeng@upm.edu.my).

Tze Jin Wong is with Department of Basic Science and Engineering, Universiti Putra Malaysia, Bintulu, Sarawak, 97008 Malaysia. He also is an associate research with Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor 43400 Malaysia (e-mail: w.tzejin@upm.edu.my).

Pang Hung Yiu is with Department of Basic Science and Engineering, Universiti Putra Malaysia, Bintulu, Sarawak, 97008 Malaysia (e-mail: yiuph@upm.edu.my).

Nik Mohd Asri Nik Long is with Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Serdang, Selangor, 43400 Malaysia. He also is an associate research with Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor 43400 Malaysia (e-mail: nmasri@upm.edu.my).

In this paper, GCD Attack had been selected to against the cryptosystem which is based on Lucas sequence and in the elliptic curve group over finite field. This cryptosystem had been proposed by Wong et. al [11], in which the garbage-man-in-the-middle attack was chosen to verify the security. It is necessary to select other types of mathematical attack to analysis the security of the cryptosystem. In addition, the papers analyse its security by using Wiener's attack [12] and Lenstra's attack [13] had been done in 2018.

II. The Cryptosystem

Let $\mathbb{F}_p$ denote a finite filed of characteristic p and two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. An elliptic curve E defined over $\mathbb{F}_p$ is given by an equation

$$y^2 = x^3 + ax + b \tag{4}$$

where $a.b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.

For every field K containing $\mathbb{F}_p$ one considers the set

$$E(K) = \{(x, y) \in K \times K \,|\, y^2 = x^3 + ax + b\} \cup \{\infty\} \tag{5}$$

In the cryptosystem, 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 product of two prime number, r and t.

Let the sender and the receiver want to communicate using Lucas based El-Gamal cryptosystem in the elliptic curve over finite field with order $n = rt$, then they will choose a secret number R which is an element of group G. Then, the sender will choose a secret number, a and the receiver will choose a secret number b. Both secret numbers are elements in the group G. Hence, the receiver will calculate the public key,

$$Q = bR \in R \tag{6}$$

If the sender wants to send a plaintext, m to Bob, then he/she encrypts the plaintext with the public key, Q. So, he/she will compute the two cyphertexts as follows.

$$c_1 = aR \tag{7}$$

and

$$c_2 = V_{aQ}(m,1) \bmod n \tag{8}$$

where $V_{aQ}(m,1)$ is second order Lucas sequence.

Now, the sender will send the ciphertext (c_1, c_2) to the receiver. Before the receiver recovered the original plaintext, he/she needs to compute the encryption key,

$$e = b \cdot c_1 \tag{9}$$

and decryption key,

$$d \equiv e^{-1} \bmod \left[\left(r - \left(\frac{{c_2}^2 - 4}{r}\right)\right)\left(t - \left(\frac{{c_2}^2 - 4}{t}\right)\right)\right] \tag{10}$$

where $\left(\frac{{c_2}^2 - 4}{r}\right)$ and $\left(\frac{{c_2}^2 - 4}{t}\right)$ are Legendre symbol.

Finally, the receiver is able to recover the original plaintext by compute

$$V_d(c_2, 1) \equiv m \bmod n \tag{11}$$

The prove for (11) is shown as below.

$$\begin{aligned} V_d(c_2,1) &\equiv V_{e^{-1}}(c_2,1) \bmod n \\ &\equiv V_{(bc_1)^{-1}}(c_2,1) \bmod n \\ &\equiv V_{(baR)^{-1}}(c_2,1) \bmod n \\ &\equiv V_{(baR)^{-1}}(V_{aQ}(m,1),1) \bmod n \\ &\equiv V_{(baR)^{-1}}(V_{abR}(m,1),1) \bmod n \\ &\equiv V_1(m,1) \bmod n \\ &\equiv m \bmod n \end{aligned} \tag{12}$$

In fact, the receiver uses the ciphertext, c_2 to compute the Legendre symbol. Therefore, the quadratic polynomial,

$$g(x) = x^2 - c_2 x + 1 \tag{13}$$

must be same type of the quadratic polynomial,

$$f(x) = x^2 - mx + 1 \tag{14}$$

So that, the Legendre symbol $\left(\frac{{c_2}^2 - 4}{n}\right) = \left(\frac{m^2 - 4}{n}\right)$. To ensure the polynomial, *g(x)* is same type of the polynomial *f(x),* the values a, b, R must be relative to r and t. Thus, the plaintext can be recovered correctly by the receiver.

As an example, suppose that a cryptosystem using an elliptic curve

$$y^2 = x^3 + 13x + 21$$

with the modulus $n = 101 \times 107 = 10807$.

The sender and receiver choose a number $R = 7$ together. Then, the sender chooses an another number $a = 13$. After that, the receiver chooses a number $b = 49$ and generate the public key, $Q = 343$.

Let the sender send a message, $m = (20, 91)$ to the receiver, where $m = (20, 91)$ is a point on the elliptic curve. Then, the sender computes

$$c_1 = aR = 91,$$
$$c_2 = V_{4459}(20,1) \bmod 10807 \equiv 5933,$$
$$c_3 = V_{4459}(20,1) \bmod 10807 \equiv 1164,$$

and sends (91, 5933, 1164) to the receiver.

When the receiver wants to recover the original message, he will do as follow:

Step 1: Computes the Legendre symbol

$$\left(\frac{5933^2-4}{101}\right) = 1,$$
$$\left(\frac{5933^2-4}{107}\right) = 1,$$
$$\left(\frac{1164^2-4}{101}\right) = 1,$$
$$\left(\frac{1164^2-4}{107}\right) = 1.$$

Step 2: Computes Encryption key

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

Step 3: Generates Decryption keys

$$d_1 = 4459^{-1} \equiv 3271 \bmod 10812$$
$$d_2 = 4459^{-1} \equiv 3139 \bmod 10800$$

Finally, the receiver will be able to get the original plaintext by computes

$$x = V_{3271}(5933,1) \equiv 20 \bmod 10807$$
$$y = V_{3271}(1164,1) \equiv 91 \bmod 10807.$$

III. The Attack

If two plaintexts, m_1 and m_2 differ from a fixed number, δ, then the plaintext can be recovered by using GCD. This type of attack called as GCD attack. GCD attack is an attack that relies on the polynomial structure of the cryptosystem. The structure of Lucas based cryptosystem in the Elliptic curve group over finite field is based on Lucas sequence which can be expressed in the term of Dickson Polynomial. Therefore, GCD attack can be adapted on this cryptosystem.

Suppose that m_1 and $m_2 = m_1 + \delta$ are the two plaintexts, then the corresponding ciphertexts can be defined as

$$c_{2,1} \equiv V_{aQ}(m_1, 1) \bmod n \tag{15}$$

and

$$c_{2,2} \equiv V_{aQ}(m_2, 1) \bmod n \tag{16}$$

where $a \in G$ is a secret number chosen by sender, Q is a public key generated by receiver and n is the order of group G.

To success the attack, the cryptanalyst will be asked the sender encrypted the fault plaintexts x_1 and $x_2 = x_1 + \delta$ and get it. Then, the cryptanalyst computes

$$X(x) \equiv V_{aQ}(x_1, 1) - c_{2,1} \bmod n \tag{17}$$

and

$$Y(x) \equiv V_{aQ}(x_2, 1) - c_{2,2} \bmod n \tag{18}$$

By using Dickson polynomial, equations $X(x)$ and $Y(x)$ can be transform in form of polynomial as follows

$$\begin{aligned} X(x) &\equiv V_u(x_1, 1) - c_{2,1} \bmod n \\ &\equiv V_{aQ}(x_1, 1) - V_{aQ}(m_1, 1) \bmod n \equiv \\ &\sum_{i=0}^{\lfloor \frac{u}{2} \rfloor} \left(\frac{u}{u-i}\right)\binom{u-i}{i}(-1)^i (x_1)^{u-2i} \\ &- \sum_{i=0}^{\lfloor u/2 \rfloor} \left(\frac{u}{u-i}\right)\binom{u-i}{i}(-1)^i \\ &\times (m_1)^{u-2i} \bmod n \equiv \sum_{i=0}^{\lfloor u/2 \rfloor} \left(\frac{u}{u-i}\right)\binom{u-i}{i}(-1)^i \\ &\times ({x_1}^{u-2i} - {m_1}^{u-2i}) \bmod n \equiv \\ &(x_1 - m_1)\sum_{i=0}^{\lfloor aQ/2 \rfloor} \left(\frac{aQ}{aQ-i}\right)\binom{aQ-i}{i}(-1)^i \\ &\times \left[\sum_{j=0}^{aQ-2i-1} {x_1}^j {m_1}^{aQ-2i-1-j}\right] \bmod n \end{aligned} \tag{19}$$

where $u = aQ$ and $2i \le aQ$.

$$\begin{aligned} Y(x) &\equiv V_u(x_2, 1) - c_{2,2} \bmod n \equiv V_u(x_1 + \delta, 1) \\ &- V_u(m_1 + \delta, 1) \bmod n \equiv \sum_{i=0}^{\lfloor u/2 \rfloor} \left(\frac{u}{u-i}\right)\binom{u-i}{i}(-1)^i \\ &\times (x_1 + \delta)^{u-2i} - \sum_{i=0}^{\lfloor u/2 \rfloor} \left(\frac{u}{u-i}\right) \\ &\times \binom{u-i}{i}(-1)^i \times (m_1 + \delta)^{u-2i} \bmod n \\ &\equiv \sum_{i=0}^{\lfloor u/2 \rfloor} \left(\frac{u}{u-i}\right)\binom{u-i}{i}(-1)^i \times [(x_1 + \Delta)^{u-2i} - \\ &(m_1 + \delta)^{u-2i}] \\ &\equiv (x_1 - m_1)\sum_{i=0}^{\lfloor u/2 \rfloor}\sum_{j=1}^{u-2i}\sum_{k=0}^{j-1} \left(\frac{u}{u-i}\right) \\ &\times \binom{u-i}{i}(-1)^i \binom{u-2i}{j} \delta^{u-2i-j} \\ &\times {x_1}^k {m_1}^{j-1-k} \bmod n. \end{aligned} \tag{20}$$

where $u = aQ$ and $2i \le aQ$.

Since

$$\sum_{i=0}^{\lfloor u/2 \rfloor} \left(\frac{u}{u-i}\right)\binom{u-i}{i}(-1)^i \left[\sum_{j=0}^{u-2i-1} {x_1}^j {m_1}^{u-2i-1-j}\right] \tag{21}$$

and

$$\begin{aligned} &\sum_{i=0}^{\lfloor u/2 \rfloor}\sum_{j=1}^{u-2i}\sum_{k=0}^{j-1} \left(\frac{u}{u-i}\right)\binom{u-i}{i}(-1)^i \\ &\times \binom{u-2i}{j} \delta^{u-2i-j} {x_1}^k {m_1}^{j-1-k} \end{aligned} \tag{22}$$

are irreducible polynomial, then

$$\gcd\big(X(x), Y(x)\big) = x_1 - m_1. \tag{23}$$

Thus, cryptanalyst solves $\gcd\big(X(x), Y(x)\big)$ that will get the

original plaintext m_1.

IV. Conclusion

GCD Attack could successfully attack the Lucas based El-Gamal cryptosystem in the elliptic curve group over finite field if the sender encrypts two plaintexts differ form a fixed number. Cryptanalyst is able to get the original plaintext without knowing the secret numbers, $a, b,$ and R, providing that the sender encrypts two plaintexts differing from a fixed number under same order of elliptic curve group over finite field. Thus, the result suggested that the sender does not encrypt the same plaintext twice or send the same plaintext to two different addresses, to avoid any attack from similar forms of GCD attack.

Acknowledgment

We would like to thank Putra Grant (Vote no: 9588900) for financial support.

References

[1] W. Diffie, and M. Hellman, "New directions in cryptography". *IEEE Transaction on Information Theory* vol. 22, p644-654, 1976.
[2] T. ElGamal, "A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms". *IEEE Transaction on Information Theory* vol. 31, p469-472, 1985.
[3] N. Koblitz. "Elliptic curve cryptosystems". *Mathematics of Computation* 48 (177): p203–209, 1985.
[4] V. Miller. "Use of elliptic curves in cryptography". *CRYPTO* 85: p417–426, 1985.
[5] 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*, p298-306, 1994.
[6] P. J. Smith and M. J. J. Lennon. "LUC: A new public key system". *Proceedings of the ninth IFIP international Symposium on Computer Security*, p103-117, 1993.
[7] M. R. M. Said. "*Application of Recurrence Relations to Cryptography"*. PhD Thesis, Macquarie University, Australia, 1997.
[8] T. J. Wong. "*A RSA-type Cryptosystem Based on Quartic Polynomials"*. PhD Thesis, Universiti Putra Malaysia, Malaysia, 2011.
[9] T. J. Wong, M. R. M. Said, K. A. M. Atan, and B. Ural, "The Quartic Analog to the RSA Cryptosystem". *Malaysian Journal of Mathematical Sciences* vol. 1(1), p63-81, 2007.
[10] L. E. Dickson. "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group." *The Annals of Mathematics* 11(1/6): p65–120; 161–183, 1897.
[11] 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* vol. 1635, p256-259, 2014.
[12] T. J. Wong, L. F. Koo, and P. H. Yiu. "On the Wiener's Attack into Lucas Based El- Gamal Cryptosystem in the Elliptic Curve Over Finite Field". *International Journal of Science and Engineering Investigations* vol 7(72), p37-39, 2018.
[13] T. J. Wong, L. F. Koo, and P. H. Yiu. "Lucas Based El-Gamal Cryptosystem in the Elliptic CurveGroup over finite field under Lenstra's Attack". Asian Journal of Mathematics and Computer Research vol. 23(4), p207-213, 2018.