International Journal of
Science and Engineering Investigations vol. 7, issue 72, January 2018
ISSN: 2251-8843

On the Wiener's Attack into Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Over Finite Field

Wong Tze Jin[1], Koo Lee Feng[2], Yiu Pang Hung[3]
[1,2,3]Department of Basic Science and Engineering, Putra Malaysia, Bintulu Campus, 97008 Bintulu, Sarawak, Malaysia
[1,2]Institute for Mathematical Research, Putra Malaysia, 43400 Serdang, Selangor, Malaysia
([1]w.tzejin@upm.edu.my, [2]leefeng@upm.edu.my, [3]yiuph@upm.edu.my)

Abstract-This paper reports a security analysis on the Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Over Finite Field. Wiener's Attack was selected to analyze the cryptosystem under a bad implementation practice. Result showed that the cryptosystem was weak if the chosen keys were too small among those in the order of group G.

Keywords- *Encryption, Decryption, Elliptic Curve, Lucas Sequence*

I. INTRODUCTION

Cryptography is a technique for secret writing. Public key cryptography is a cryptographic system, which comprose 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. The public key cryptography was introduced by Diffie and Hellman [1] in 1978.

In 1985, El-gamal [2] introduced a digital signature scheme which reffered as El-Gamal Encryption Scheme. This encryption scheme was based on key exchange method. In 1994, Smith and Skinner [3] modified the El-Gamal encryption scheme based on Lucas function in order to increase the security. In 2014, Wong and his team [4] enhanced the security again with put the cryptosystem in the elliptic curve over finite field. Based on characteristics of Lucas function and elliptic curve, the security of the cryptosystem had been improved.

In this paper, Wiener's attack [5] is selected to analyze the security for the Lucas based El-Gamal cryptosystem in the elliptic curve over finite field.

II. MATHEMATICS BACKGROUND

A. Lucas function

A second order Lucas function is a linear recurrence sequence of integers, defined by

$$T_n(P,Q) = PT_{n-1}(P,Q) - QT_{n-2}(P,Q) \quad (1)$$

where P and Q are coefficient for quadratic polynomial

$$x^2 - Px + Q = 0 \quad (2)$$

Let α and β be the root of quadratic polynomial, then the coefficient of the quadratic can be define as $P = \alpha + \beta$ and $Q = \alpha\beta$. Therefore, there are two particular solution for second order linear recurrence, which are defined as

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad (3)$$

and

$$V_k = \alpha^k + \beta^k \quad (4)$$

with initial values $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, and $V_1 = P$.

The sequence V_k will be used to develop the process of encryption and decryption. In addition, composite of the sequence is used to check decryption key really can recover the original plaintext in the process of decryption, which defines as

$$V_{hk} = V_h(V_k, 1) \quad (5)$$

B. Elliptic Curve

Let $\mathbb{F}_p$ denote a finite filed of characteristic p with p prime and two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$.

For case $p = 2$, an elliptic curve E defined over $\mathbb{F}_q$ is given by an equation

$$y^2 + xy = x^3 + ax^2 + b \quad (6)$$

where $a.b \in \mathbb{F}_q$ and $b \neq 0$. For every field K containing $\mathbb{F}_p$ one considers the set

$$E(K) = \{(x, y) \in K \times K \,|\, y^2 + xy = x^3 + ax^2 + b\} \cup \{\infty\} \quad (7)$$

For case $p > 2$, an elliptic curve E defined over $\mathbb{F}_p$ is given by an equation

$$y^2 = x^3 + ax + b \quad (8)$$

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

$$E(K) = \{(x, y) \in K \times K \,|\, y^2 = x^3 + ax + b\} \cup \{\infty\} \quad (9)$$

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.

III. THE CRYPTOSYSTEM

Let the sender, Alice and the receiver, Bob 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, Alice will choose her own private number, a and Bob will choose his own private number b. Both a and b are elements in the group G. After that, Bob will generate the public key,

$$Q = bR \in R \quad (10)$$

If Alice wants to send a plaintext, m to Bob, then she encrypts the plaintext with the public key, Q. So, she will compute the two ciphertexst as follow.

$$c_1 = aR \text{ and } c_2 = V_{aQ}(m,1) \bmod n$$

where $V_{aQ}(m,1)$ is second order Lucas sequence which is defined in (4) and it is satisfy the linear recurrence sequence defined in (1).

Now, Alice will send the ciphertext (c_1, c_2) to Bob.

Before Bob recovered the original plaintext, he needs to compute

$$e = b \cdot c_1 \quad (11)$$

and

$$d \equiv e^{-1} \bmod \left[\left(r - \left(\frac{{c_2}^2 - 4}{r}\right)\right)\left(t - \left(\frac{{c_2}^2 - 4}{t}\right)\right)\right] \quad (12)$$

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

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

$$V_d(c_2,1) \equiv m \bmod n \quad (13)$$

The prove for (13) is shown as below

$$\begin{aligned} V_d(c_2,1) &\equiv V_{e^{-1}}(c_2,1) \bmod n \\ &\equiv V_{(bc_1)^{-1}}(c_2,1) \bmod n \\ &\equiv V_{(baR)^{-1}}(c_2,1) \bmod n \\ &\equiv V_{(baR)^{-1}}(V_{aQ}(m,1),1) \bmod n \\ &\equiv V_{(baR)^{-1}}(V_{abR}(m,1),1) \bmod n \\ &\equiv V_1(m,1) \bmod n \\ &\equiv m \bmod n \end{aligned} \quad (14)$$

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

$$g(x) = x^2 - c_2 x + 1. \quad (15)$$

must be same type of the quadratic polynomial,

$$f(x) = x^2 - mx + 1. \quad (16)$$

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 recover correctly by Bob.

IV. THE ATTACK

Suppose that the order of group G, $n = rt$ is the modulus of system, where r and t are prime number. The public key and private key are related to

$$ed \equiv 1 \bmod \left[\left(r - \left(\frac{{c_2}^2 - 4}{r}\right)\right)\left(t - \left(\frac{{c_2}^2 - 4}{t}\right)\right)\right] \quad (17)$$

Since $\left(\frac{{c_2}^2 - 4}{r}\right)$ and $\left(\frac{{c_2}^2 - 4}{t}\right)$ are Legendre symbol and the value of Legendre symbol is +1 or –1, then

$$ed \equiv \begin{cases} 1 \bmod (r-1)(t-1), \\ 1 \bmod (r-1)(t+1), \\ 1 \bmod (r+1)(t-1), \text{ or} \\ 1 \bmod (r+1)(t+1). \end{cases} \quad (18)$$

Therefore, exist $h, k \in G$ with $\gcd(h,k) = 1$ such that

$$ed = 1 + \frac{k}{h}(r-1)(t-1) \quad (19)$$

$$ed = 1 + \frac{k}{h}(r-1)(t+1) \quad (20)$$

$$ed = 1 + \frac{k}{h}(r+1)(t-1) \quad (21)$$

or

$$ed = 1 + \frac{k}{h}(r+1)(t+1) \quad (22)$$

Equations (19), (20), (21), and (22) can be expand and combine in an equation as follow

$$ed = 1 + \frac{k}{h}(n \pm r \pm t \pm 1)$$

Then, dividing both sides by dn yields

$$\frac{e}{n} = \frac{1}{dn} + \frac{k}{hdn}(n \pm r \pm t \pm 1) \quad (23)$$

Equation (23) can be rearrange become

$$\frac{k}{hd} - \frac{e}{n} = \frac{k}{hd}(\pm\frac{1}{t} \pm \frac{1}{r} \pm \frac{1}{n}) - \frac{1}{dn}$$

Theorem 1: If $\left|\frac{a}{b} - x\right| < \frac{1}{2b^2}$, then $\frac{a}{b}$ is a continued fraction approximant for *x*.

Proof: See [6], page 153, Theorem 184. ■

If the condition of theorem 1 is fulfilled, then $\frac{k}{hd}$ is continued approximant for $\frac{e}{n}$. Since continued fraction can easily be computed, then it is possible to find the private key, *d* under certain assumption.

Corollary 1: For Lucas based El-Gamal cryptosystem in the elliptic curve over finite field, assume that $r \sim t \sim \sqrt{n}$, $h < d$, and $e \sim n$, then $k \sim hd$ and the attack will be succeed for *d* of order up to $n^{1/4}$.

Proof: If $e \sim n$, then $k \sim hd$ and $\left|\frac{k}{hd} - \frac{e}{n}\right|$ tends to zero. Equation (23) can be wrote as

$$\left|\frac{k}{hd} - \frac{e}{n}\right| \le \frac{k}{hd}(\frac{1}{t} + \frac{1}{r}) + \frac{k+h}{hdn} \sim \frac{1}{\sqrt{n}} \quad (24)$$

So

$$\left|\frac{k}{hd} - \frac{e}{n}\right| < \frac{1}{2h^2d^2} \sim \frac{1}{d^2} \text{ if } d \text{ is of order at most } n^{1/4} \quad ■$$

V. CONCLUSION

Based on corollary 1, Wiener's attack could successfully attack the Lucas based El-Gamal Cryptosystem in the elliptic curve group over finite field, if the private key, *d* is less than $n^{1/4}$, where *n* is the order of elliptic curve group. Result suggested that the sender and the receiver cannot choose those secret numbers, *a*, *b*, and *R*, which the product of them are approximately close to the order of elliptic curve group.

ACKNOWLEDGMENT

We would like to thank Putra Grant (Vote no: 9589000) for financial support.

REFERENCES

[1] W. Diffie, and M. Hellman, "New directions in cryptography". IEEE Transaction on Information Theory vol. 22, p.644-654, 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] 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.

[4] 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.

[5] M. J. Wiener, "Cryptanalysis of Short RSA Secret Exponents". IEEE Transactions on Information Theory vol. 36(3), p386-396, 1990.

[6] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 4th ed., Oxford: Oxford University press, 1979.

[7] 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.

[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, M. Othman, and K. A. M. Atan, "Wiener's Attack on the Fourth Order of LUC Cryptosystem", The proceeding of The 4th International Conference on Research and Education in Mathematics, p386-391.