ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **9** (2020), no.12, 10845–10854
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.12.69 Special Issue SMS-2020

SECURITY ANALYSIS ON ELLIPTIC CURVE CRYPTOSYSTEM BASED ON SECOND ORDER LUCAS SEQUENCE USING FAULTS BASED ATTACK

LEE FENG KOO[1], TZE JIN WONG, FATIN HANA NANING, PANG HUNG YIU,
MOHAMMAD HASAN ABDUL SATHAR, AND AHMAD FADLY NURULLAH RASEDEE

ABSTRACT. Elliptic Curve Cryptosystem based on second order Lucas sequence is a cryptosystem using elliptic curves over finite fields as a mask and incorporate with second order of Lucas sequence. The security of the Elliptic Curve Cryptography cryptosystem depends on the discrete logarithms. In this cryptosystem, Lucas sequence is employed to compute the ciphertext or recover the plaintext. The Elliptic Curve Cryptosystem based on second order Lucas sequence is vulnerable when the bit of the decryption key, d flips by using fault based attack.

1. INTRODUCTION

The coronavirus pandemic (COVID19) is spreading around the world rapidly, causing deaths and significant disruption to the global health, economic, political as well as social system. Consequently, remote working, remote learning as well as remote business interactions, had been identified as the new opportunities to reduce the rate of infection of COVID19 via social distancing. As such, the increase in remote working (work from home), online learning and online shopping become a new norm. The world is experiencing widespread use of electronic commerce (e-commerce) such as e-banking and internet shopping in contemplation to stay competitive while staying at home in an increasingly borderless global economy. However, the increasing usage of internet network traffic simultaneously

[1] *corresponding author*

2020 *Mathematics Subject Classification.* 94A60, 11T71.

Key words and phrases. decryption, elliptic curve, encryption, keys, Lucas sequence.

escalates the risk of cyberattacks. Cybercriminal and internet fraudster impose immense challenge in the digital economy because prey on our sensitive information and gain unauthorize access as people relies heavily on digital tools. The attack includes malicious malware results in disclosure of financial information that causing financial loss, data stolen or replication, as well as harming one's firm reputation. Thus, the demand of the cryptography system raises dramatically among the public in order to counter the cyberattack. Furthermore, cryptography also plays a crucial role in the digital rights management and copyright management infringement of digital media to prevent unauthorized redistribution of digital media.

Public Key Cryptography (PKC) based on the discrete logarithm problem (DLP) was firstly introduced by Diffie and Hellman in 1976 to provide confidentiality. This is an encryption scheme with two cryptographic keys, i.e., public key or sometimes refer as encryption key and the private key or sometimes is called as the decryption key. The public key allows the sender to encrypt their message and distributed freely to the receiver; meanwhile, the private key must be kept secret by the receiver and used for decrypting or create the digital signature. The RSA and the various type of the RSA cryptosystems, which exploits integer factorization problem (IFP) is the most widely used public key cryptosystem to safeguard the data in e-banking and communication from unauthorized access.

Elliptic Curve Cryptosystem (ECC) is a modern family of PKC, which also consists of two main components, public encryption key and private decryption key as well. The security of ECC depends on the difficulty of the Elliptical Curve Discrete Logarithm Problem (ECDLP). The implementation of ECC provides high security at low computation time. For instance, A 160 bits key in ECC gives the equivalents security as 1024 bit keys in RSA, and 15360 bits key in RSA cryptographic algorithm provide the same security despite the usage of 512 bits in ECC. Taking these advantages, nowadays, ECC gained much popularity and widely used to secure data transmission, particularly in mobile phones and web browsers due to its ability to provide the equivalent level of security. Henceforth, numerous studies had presented by many researchers to discuss the prospects of this protocol as well as to enhance its efficiency and security. Hakerson *et al.* [1] designed Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC) to increase the efficiency of ECC by adopting a masking technique in the process of encryption and decryption which is akin to El-Gamal Cryptosystem. This method showed significant enhancement in the computation of logarithms on a small and unique class of super-singular curves. Subsequently, motivated by the work of Hakerson *et al.* [1], Ziad *et al.* [2] improved the MVECC by reducing the computation and running time for the encryption and decryption process.

Lucas sequence is used extensively in cryptography owing to the recurrence characteristics. Lucas based cryptosystem (LUC cryptosystem) is analogous to RSA scheme, but based on Lucas function to either generate a ciphertext, or to recover the original plaintext through respective encryption and decryption processes. LUC cryptosystem comparable security level with traditional system, but with lesser key sizes. Various studies on the application of LUC cryptosystem had been done to discuss the prospects of this protocol as well as to enhance the security and reliability of cryptography [3, 5, 9].

Protection and security become critical concerns in the universal electronic connectivity paradigm. The study of strength and weaknesses analysis of cryptosystem become vital in order to overcome the vulnerability and provide the better security design and implementation [4, 6–8]. In this study, we present cryptanalysis of ECC based on the Lucas sequence using the transient fault-based attack [10] whereby this type attack usually against PCR on tamper resistant devices. The attack demonstrated the weakness of the ECC based on second order Lucas sequence.

2. Preliminaries

2.1. **Lucas Sequence.** Lucas sequence is an integer sequence that satisfies the linear recurrence relation. A second order Lucas sequence V_k is defined by [9]

$$V_k(x_1, 1) = x_1 V_{k-1}(x_1, 1) - V_{k-2}(x_1, 1), \tag{2.1}$$

with initial value $V_0(x_1, 1) = 2$ and $V_1(x_1, 1) = x_1$, where x_1 is coefficient quadratic polynomial

$$x^2 - x_1 x + 1 = 0. \tag{2.2}$$

The composite function of the Lucas sequence is defined as

$$V_{hk}(x_1, 1) = V_h(V_k(x_1, 1), 1).$$

The inverse function can be determined from the composite of the Lucas sequence. Consider $hk \equiv 1 \mod \phi(n)$ such that $hk = a\phi(n) + 1$ for some integer a and $\phi(n)$

is Euler function. Then, the inverse of the Lucas sequence can be defined as

$$V_{hk}(x_1,1) \equiv V_1(x_1,1) \equiv x_1 \mod n.$$

These composite and inverse of Lucas sequences are employed to validate that the original plaintext can be recovered through the process of decryption.

The addition rule of second order Lucas sequence is defined as

$$V_{h+k}(x_1,1) = V_h(x_1,1)V_k(x_1,1) + (x_1^2-4)U_h(x_1,1)U_k(x_1,1),$$

where $U_k(x_1,1)$ and $U_k(x_1,1)$ are the Fibonacci sequence, which will be defined in the next sub-section.

2.2. **Fibonacci Sequence.** The Fibonacci sequence is a sequence of integers U_k defined recurrently by [3]

$$U_k(x_1,1) = PU_{k-1}(x_1,1) - U_{k-2}(x_1,1),$$

with initial values $U_0 = 0$ and $U_1 = 1$. In addition, x_1 is the coefficient of quadratic polynomial defined in (2.2).

2.3. **Elliptical Curve.** Suppose that finite field or Galois field denote as F_p with p elements, then the equation for the elliptic curve over F_p is defined as [4, 5]

$$y^2 = x^3 + \alpha x + \beta,$$

where α and β are elements for F_p and $4\alpha^3 + 27\beta^2 \neq 0$. The set group G is defined as

$$G(H) = \{(x,y) \in H \times H | y^2 = x^3 + \alpha x + \beta\} \cup \{\infty\}$$

for field H contains F_p.

3. The Cryptosystem

In the Lucas based ECC, the modulus of the cryptosystem is a large prime number denoted as n, and which is also the order of a general group of G. Akin to other asymmetric cryptosystems, the Lucas based ECC consists of three distinct operations: key generation, encryption, and decryption. The ciphertext will be produced through the encryption process while the ciphertext will be decrypted back to the original plaintext through the decryption process.

3.1. **Process of Encryption.** Let $a, b, R, Q \in G$, R is the shared secret number by the sender and receiver; a and b are the chosen secret numbers of sender and receiver, respectively. The receiver employed secret number to generate the public key $Q = bR$, which later used to decrypt the cipher message back to its plain message.

A message or plaintext, $m = (x, y)$, is a set of coordinates lying on the elliptical curve that was encrypted by the sender. In order to encrypt the plaintext message, the sender computes the first and second ciphertext, c_1, c_2 which are defined as

$$c_1 = aR \qquad \text{and} \qquad C_2 = V_{aQ}(m, 1) \mod n,$$

where $c_2 = (c_x, c_y)$. The second ciphertext c_2 is aQ^{th} terms of the Lucas sequence, which defined in (2.1). The ciphertext (c_1, c_2) afterward send to the receiver.

3.2. **Process of Decryption.** In this process, the encrypted information will be decoded based on the concept of the inverse of recurrence. In order to calculate the decryption key, the receiver must be adequate to evaluate the encryption key

$$e = bc_1,$$

which afterward adapted to calculate the decryption key

$$d = e^{-1} \mod \left(n - \left(\frac{c_2^2 - 4}{n} \right) \right),$$

where $\left(\frac{c_2^2-4}{n} \right)$ is the Legendre symbol.

Finally, the original plaintext can be revealed easily by computing

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

Literally, the receiver evaluates the Legendre symbol from second ciphertext, c_2 but not the plaintext, m since the sender sent the ciphertext to the receiver. The quadratic polynomial for receiver defined as

$$f(x) = x^2 - c_2 x + 1$$

whereby the original quadratic polynomial is

$$g(x) = x^2 - m^x + 1.$$

As such, the Legendre symbol for both quadratic polynomials should be the same, that is $\left(\frac{c_2^2-4}{n}\right) = \left(\frac{m^2-4}{n}\right)$ if both quadratic polynomials are the same type of polynomial. Hence, the values of a, b and R must be relatively prime to the Euler function of the modulus n in order to ensure both of the quadratic polynomials have to satisfy the similar identities to the familiar properties of the quadratic function. Hereinafter, the original plaintext can be revealed by the receiver precisely.

Example 1. *Supposed we have two communicating parties, namely Rara as the sender of message and Tata as its corresponding receiver. Let the system modulus denoted as* $n = 1993$.

Key generation:

(1) Both know the shared secret key, $R = 7$.
(2) Rara keeps her secret key, $a = 13$.
(3) Tata keeps her secret key, $b = 17$.
(4) Tata publishes her public key, $Q = 119$.

Encryption
Rara received Tata's public key, Q. She would like to send a message, $m = (20, 91)$ to Tata. She

(1) computes

$$c_1 = 91$$
$$c_2 = V_{1547}(20,1) \mod 1993 \equiv 1545$$
$$c_2 = V_{1547}(91,1) \mod 1993 \equiv 1845,$$

(2) sends the ciphertext $(91, 1545, 1845)$ to Tata.

Decryption
Tata received a set of ciphertext $(91, 1545, 1845)$ from Rara. To decrypt the ciphertext, Tata then

(1) calculates the Legendre symbol

$$\left(\frac{1545^2-4}{1993}\right)=-1 \qquad \text{and} \qquad \left(\frac{1825^2-4}{107}\right)=-1,$$

(2) calculates Encryption key, $e = bc_1 = 1791 = 1547$,

(3) calculates the decryption key from the encryption key and Legendre symbol

$$d_x = 1547^{-1} \equiv 1481 \mod 1994$$
$$d_y = 1547^{-1} \equiv 1481 \mod 1994,$$

(4) recovers the original plaintext by computing $V_d(c_2, 1)$

$$x = V_{d_x}(c_2, 1) = V_{1484}(1545, 1) \equiv 20 \mod 1993$$
$$x = V_{d_y}(c_3, 1) = V_{1484}(1825, 1) \equiv 91 \mod 1993.$$

4. The Attack

Suppose that n denotes the modulus of system and order of elliptic curve group G. Let $R \in G$ is the sender's and receiver's secret number, $a \in G$ is the sender's secret number, and $b \in G$ is the receiver's secret number. The public key $Q = bR \in G$ is generated by the receiver. Let the secret key or decryption key,

$$d = \sum_{i=0}^{t-1} d_i 2^i$$

be the binary expansion of d. Unfortunately, one bit of decryption or secret key d flips when the receiver generates the signature. The corrupted secret key or decryption key is denoted by $\hat{d}$. If bit t of d flips, then

$$\hat{d} = \begin{cases} d + 2^t, & d_t = 0 \\ d - 2^t, & d_t = 1. \end{cases}$$

The attack goes as follows. Firstly, the cryptanalyst chooses a plaintext m and computes

$$c_2 = V_e(m, 1) \mod n$$
$$H \equiv (m^2 - 4)U_e(m, 1)$$
$$\alpha_j \equiv V_{2^j}(c_2, 1) \mod n$$

and

$$\beta_j \equiv U_{2^j}(c_2, 1) \mod n.$$

Secondly, the cryptanalyst requests the sender to decrypt the plaintext m using the corrupted decryption key $\hat{d}$. As such, the cryptanalyst adequate to determine the flipped bit of d as

$$2V_e(\hat{s}, 1) \equiv \begin{cases} \alpha_j m + \beta_j H \mod n, & d_j = 0 \\ \alpha_j m - \beta_j H \mod n, & d_j = 1. \end{cases} \tag{4.1}$$

And hence, break the system after obtaining the faulty signature, $\hat{s}$ from the sender,

$$\hat{s} \equiv V_{\hat{d}}(m, 1) \mod n.$$

It implies that this system is vulnerable to cryptanalytic attacks since the cryptanalyst able to decrypt the original plaintext or message, providing the sender decrypt the original plaintext with a corrupted secret key or decryption key, and the bit of the real secret key or decryption key flips.

Employed the $(-k)$ Lucas sequence and Fibonacci sequence defined as [3]

$$V_{-k}(P, 1) = V_k(P, 1) \quad \text{amd} \quad U_{-k}(P, 1) = -U_k(P, 1),$$

equation (4.1) can be proved as follows

$$\begin{aligned} 2V_e(\hat{s}, 1) &\equiv 2V_e(V_{\hat{d}}(m, 1), 1) \\ &\equiv 2V_e(V_{\hat{d}-d+d}(m, 1), 1) \\ &\equiv 2V_{e(\hat{d}-d)+1}(m, 1) \\ &\equiv V_{e(\hat{d}-d)}(m, 1)V_1(m, 1) + (m^2 - 4)U_{e(\hat{d}-d)}(m, 1)U_1(m, 1) \\ &\equiv V_{e(\hat{d}-d)}(m, 1)m + (m^2 - 4)U_{e(\hat{d}-d)}(m, 1) \\ &\equiv V_{\hat{d}-d}(V_e(m, 1), 1)m + (m^2 - 4)U_e(m, 1)U_{\hat{d}-d}(V_e(m, 1), 1) \\ &\equiv V_{\hat{d}-d}(c_2, 1)m + HU_e(m, 1)U_{\hat{d}-d}(c_2, 1) \mod n. \end{aligned}$$

5. Conclusion

The study demonstrated the pitfall in the implementation of ECC based on the second order Lucas sequence using fault based attack. The result shows that the attack is applicable if the bit of the decryption key, d flips. Therefore, the cryptanalyst able to decrypt the original plaintext or message without knowledge of the secret number of either receiver, sender, or both providing the sender decrypt the original plaintext with a corrupted secret key or decryption key, and the bit of the real secret key or decryption key flips. Thus, the sender must be very careful when decrypting the original plaintext to prevent fatal leakage of the secret key and which will cause inefficiency and insecurity of the system. Further investigation are necessary in order to enhance the design of cryptosystem of ECC based on the second order Lucas sequence in its encryption and attack resistance performance.

ACKNOWLEDGMENT

Authors are wishing to acknowledge financial support from Putra Grant (Vote No. 9664500).

REFERENCES

[1] H. HAKERSON, A. MENEZES, S. VANSTONE: *Guide to Elliptic Curve Cryptography*, Springer-Verlag Inc, New York, 2003.

[2] E.D. ZIAD, N.Y. SHAHRUL, R.R. OTHMAN: *A New Modification for Menezes-Vanstone Elliptic Curve Cryptography*, Journal of Theoretical and Applied Information Technology, **85**(2) (2016), 290–297.

[3] P.J. SMITH AND M.J.J. LENNON: *LUC: A New Public Key System*, Proceedings of the Ninth IFIP International Symposium on Computer Security, (1993), 103–117.

[4] I.N. SARBINI, T.J. WONG, L.F. KOO, M. OTHMAN, M.R.M. SAID, P.H. YIU: *Garbage-man-in-the-middle (type2) attack on the Lucas Based El-gamal Cryptosystem in the Elliptic Curve Group Over Finite Field*, Proceedings of the 6th International Cryptology and Information Security Conference, (2018), 35–41.

[5] I.N. SARBINI, L.F. KOO, T.J. WONG, F.H. NANING, F.H., P.H. YIU: *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) (2019), 1193–1196.

[6] T.J. WONG, M.R.M. SAID, M. OTHMAN, L.F. KOO : *A Lucas based cryptosystem analog to the ElGamal cryptosystem and elliptic curve cryptosystem*, AIP Conference Proceedings, **1635** (2014), 256–259.

[7] M.A. ASBULLAH, M.R.K. ARIFFIN: *Design of Rabin-like Cryptosystem without Decryption Failure*, Malaysian Journal of Mathematical Sciences, **10**(S) (2016), 1–18.

[8] A.M.A. NASHIR, S.F.S. ADNAN, H. HASHIM, M.A.M. ISA, Z. MAHAD, M.A. ASBULLAH: *Analysis of Rabin-p and HIME(R) Encryption Scheme on IoT Platform*, International Journal of Advanced Trends in Computer Science and Engineering, **9**(1.2) (2020), 139–143.

[9] T.J. Wong, M.R.M. Said, M. Othman, L.F. Koo : *A Method to Decrease Computation Time for Fourth Order Lucas Sequence*, AIP Conference Proceeding, **1557** (2013), 55–58.

[10] F. Bao, R. Deng, Y. Han, A. Jeng, D. Narasimhalu, T.H. Ngair: *Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults*, Pre-proceedings of the 1997 Workshop on Security Protocols, France.

Department of Science and Technology, Universiti Putra Malaysia,
Bintulu Campus, Nyabau Road, 97008 Bintulu, Sarawak, Malaysia.
Email address: leefeng@upm.edu.my

Department of Science and Technology, Universiti Putra Malaysia,
Bintulu Campus, Nyabau Road, 97008 Bintulu, Sarawak, Malaysia.
Email address: w.tzejin@upm.edu.my

Department of Science and Technology, Universiti Putra Malaysia,
Bintulu Campus, Nyabau Road, 97008 Bintulu, Sarawak, Malaysia.
Email address: fatinhanaz@upm.edu.my

Department of Science and Technology, Universiti Putra Malaysia,
Bintulu Campus, Nyabau Road, 97008 Bintulu, Sarawak, Malaysia.
Email address: yiuph@upm.edu.my

Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia,
43400 UPM Serdang, Selangor, Malaysia.
Email address: mohdhasan@upm.edu.my

Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia,
78100 Nilai, Negeri Sembilan, Malaysia.
Email address: fadlynurullah@usim.edu.my