Information Sciences Letters
An International Journal

http://dx.doi.org/10.12785/isl/030204

Cryptanalysis of Lin et al.'s Digital Multi-Signature Scheme on the Generalized Conic Curve Over Z_n

SK Hafizul Islam[1,*] *and G. P. Biswas*[2]

[1] Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India
[2] Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, Jharkhand 826004, India

Received: 10 Dec. 2013, Revised: 20 Mar. 2014, Accepted: 22 Mar. 2014
Published online: 1 May 2014

Abstract: In 2009, Lin et al. proposed a digital multi-signature scheme based on the concepts of generalized conic curves over Z_n. They claimed that the multi-signature scheme is well secured and the forgery attack is infeasible on it. Unfortunately, three weaknesses on their proposed multi-signature have been observed and it has been shown that an attacker can compute the secret pairs of all signers using the technique to solve the linear Diophantine equation, a malicious signer can generate a forged signature based on the signatures of other signers, called inside forgery attack, which is very difficult to disproof by the verifier. Also an outsider can compute a forged signature against the valid multi-signature, may be termed as outsider forgery attack.

Keywords: Conic curve, Digital multi-signature, Linear Diophantine equation, Euclid's algorithm, Forgery attack

1 Introduction

Digital signature is a mathematical tool, used in cryptography to provide authentication, integrity and non-repudiation properties of electronic message on the internet. The signer formulates a digital signature using his/her private key on a digital message such that a public verifier can verify the message and signature using signer's public key, but anyone can't forge the signature on any other message. Most of the situations, the signer is generally a single person however, in some cases a message is to be signed or approved by multiple number of signers. In such case, a strategy could be put into practice by having a separate digital signature for every signer, but it will increase the effort to verify the signature one by one with the number of signers. To avoid these difficulties, the multi-signature schemes are adopted in a way that each signer prepares their different signature on the same message and sends to the collector. After receiving all signatures from every signer, the collector coordinates the entire signature and prepares a single multi-signature. The collector sends the final multi-signature with the message to the verifier, who then verifies the received message and multi-signature. The digital multi-signature schemes are extensively used in many applications including electronic contract sign, decision making processes, petitions, work-flow systems, etc.

In last two decades, several multi-signature schemes [1], [2], [3], [4], [5], [6], [7] have been proposed by the researchers such as (1) ID-based multi-signature scheme using RSA algorithm, (2) ID-based multi-signature scheme using elliptic curve cryptography (ECC), (3) Multi-signature scheme based on certificateless public key cryptography (CL-PKC) and ECC, (4) Multi-signature scheme based on the generalized conic curves over Z_n. Most of them are based on the difficulties to solve integer factorization problem (IFP) and discrete logarithm problem (DLP). Several ID-based multi-signature schemes using RSA have been proposed [8], [9], [10], [11], most of them are vulnerable against different attacks such as forgery attack, active attack, etc. [12], [13], [14], [15], [16]. However, ID-based multi-signature scheme using elliptic curve cryptography (ECC) is based on the difficulties of solving the elliptic curve discrete logarithm problem (ECDLP) [17], [18], [19] shows the same level of security performance with less bit size key, but unfortunately all of the schemes are broken [14], [20], [21].

[*] Corresponding author e-mail: hafizul.ism@gmail.com, hafizul@pilani.bits-pilani.ac.in

The multi-signature scheme can be categorized into two types: sequential multi-signature [7], [10] and broadcast multi-signature [5], [6], [7], [8], [22]. In the former scheme, each signer computes a partial multi-signature and forwards to the next successive signer for further signing, i.e., i^{th} signer generates the partial multi-signature based on the partial multi-signature received from the $(i-1)^{th}$ signer. At the end of signing process, the last signer computes the final multi-signature on behalf of all signers, and this can be verified by verifier. However, the sequential approach is not efficient in many applications since the time taken for multi-signature generation and verification is linearly depends on the number of signers. In the latter scheme, the message issuer broadcasts the same message to the signing group, then each signer computes their individual signature and sends them to the collector. Now the collector generates the final multi-signature, and sends it to the verifier for verification. Compared with sequential approach, broadcast approach reduces communication and computation costs.

In 2009, Lin et al. [22] proposed a broadcast digital multi-signature scheme on generalized conic curves over Z_n and its security is based on the discrete logarithm problem (DLP). Design and implementations of cryptographic tools using conic curve is easier than elliptic curve [23]. Lin et al. claimed that their scheme can prevent forgery attack [8] and extraction of signer's secret pairs is infeasible. In this paper, it is proved that Lin et al.'s scheme is no longer secured against *private key extraction attack*, *insider forgery attack* and *outsider forgery attack*. In private key extraction attack, an adversary can compute signer's secret keys using the technique used to solve the linear Diophantine equation. In insider forgery attack, a malicious signer, who belongs to the signing group, can generate a forged signature on behalf of other signers. In outsider forgery attack, an adversary, who does not belong to the signing group, can generate a forged multi-signature δ^* from a valid multi-signature δ on the same message m without knowing the secret keys of all signers.

The rest of the paper is organized as follows. In Section 2, we reviewed Lin et al.'s digital multi-signature scheme. The proposed three attacks on Lin et al.'s scheme are described in Section 3. Finally, some concluding remarks are given in Section 4.

2 Review of Lin et al.'s multi-signature scheme

This section reviews Lin et al.'s multi-signature scheme on generalized conic curves over Z_n. In this scheme, the sender broadcasts the message to each signer simultaneously. Then each signer produces their individual signature on the received message, and sent it to the collector. After receiving all the signatures, the collector organizes these received signatures and prepares a final single signature, which is to be sent to the verifier for verification. A list of notations used in the Lin's multi-signature scheme is given in Table 1.

Table 1: Notations used in Lin et al.'s multi-signature scheme

Notation	Meaning
r, s	Two large primes number such that $p+1=2r$, $q+1=2s$, p, q two integers
F_p	A finite field
Z_n	The residue class ring modulo n
$C_p(a,b)$	The conic curve over Z_n
$R_n(a,b,c)$	Generalized conic curve over Z_n
$H(\cdot)$	One-way secure hash function
U_i	The i^{th} user of a group
d_i	The i^{th} user private key

The whole scheme consists of four phases: System initialization phase, Signing phase, Collecting phase and Verification phase. Now we describe briefly each phase as given below.

2.1 System initialization phase

Step 1.Choose a generalized conic curve $R_n(a,b,c)$, $n=pq$ and $p+1=2r$, $q+1=2s$, $|R_n(a,b,c)|=(p+1)(q+1)=2rs$, r and s are two large primes.

Step 2.Consider a base point $G=(x_G,y_G)$ on $R_n(a,b,c)$ of order $N_n = lcm\{|R_p(a,b,c)|,|R_q(a,b,c)| = (p+1)(q+1)=2rs\}$.

Step 3.Every group member $U_i(i=1,2,\cdots,k)$ sends their public key $Q_i=d_iG$ to the collector.

Step 4.The system publishes the parameters $\langle n$, G, Q_i, $H(\cdot)$, $R_n(a,b,c)\rangle$ as public.

2.2 Signing phase

Step 1.Each U_i selects a random number $k_i \in Z^*_{N_n}$.

Step 2.Each U_i calculates $C_i=k_iG=(x_i,y_i)$.

Step 3.Each U_i calculates $\delta_i=k_i-d_iH(m)(\text{mod } N_n)$. If $\delta_i=0$, then go to Step 1. Therefore (c_i,δ_i) is the signature on the message m of the group member U_i and send it to the collector.

2.3 Collecting phase

Step 1.The collector received all (c_i,δ_i) from the group members and calculates $C=\sum_{i=1}^{n} C_i$ and $\delta=\sum_{i=1}^{n}\delta_i$.

Step 2.The collector sends the final multi-signature (C,δ) of the message m to the verifier.

2.4 Verification phase

Step 1.The verifier computes $Q = \sum_{i=1}^{n} Q_i$.

Step 2.Choose $u_1 = \delta$ and $u_2 = H(m)$, computes $u_1 G \oplus u_2 Q = C^*$.

Step 3.The verifier accepts the signature (C, δ) as valid multi-signature if $C^* = C$, otherwise reject the signature.

3 Cryptanalysis of Lin et al.'s multi-signature scheme

In this section, the cryptanalysis of the Lin et al.'s multi-signature scheme is done and three relevant attacks such as extraction of secret pairs, insider forgery attack and outsider forgery attack have been identified. Each of them is now discussed.

3.1 Private key extraction attack

As stated earlier, each signer in Lin et al.'s scheme computes $\delta_i = k_i - d_i H(m) (\mathrm{mod}\ N_n)$ and generates individual signature (c_i, δ_i), which is found to be solvable to extract the signer's secret keys based on the technique used to solve the linear Diophantine equation [24]. The Theorem 1 given below explains the technique to solve the Liner Diophantine Equation.

Theorem 1.*Any linear Diophantine equation $ax + by = c$, where a and b are two integer coefficients, has an integer solution if and only if $l = gcd(a, b)$ divides c, and then the general solutions for x and y are $x = \frac{uc+bt}{l}$ and $y = \frac{vc+at}{l}$, where t, u, v are integers such that $au + bv = l$ holds.*

Proof of the proposed attack: Now we will prove the proposed attack with the help of the Theorem 1. The expression for δ_i, which is a part of the i^{th} signer's signature, can be rearranged as

$$k_i \times 1 + (-H(m))d_i = \delta_i \tag{1}$$

Now on comparing 1 it with $ax + by = c$, we have $a = 1$, $x = k_i$, $b = -H(m)$, $y = d_i$, $c = \delta_i$. Since

$$\begin{aligned} l_i &= gcd(a, b) \\ &= gcd(1, -H(m)) \end{aligned} \tag{2}$$

and therefore, l_i divides δ_i. After putting the values of a and b in the equation $au + bv = l$, we have

$$au_i + bv_i = 1$$

$$\Rightarrow au_i + bv_i = 1$$

$$\Rightarrow u_i - H(m)v_i = 1$$

Now by applying *Euclid's algorithm* we get, $u_i = 1 + H(m)$ and $v_i = 1$. The general solutions for k_i and d_i can be found as

$$\begin{aligned} k_i &= \{1 + H(m)\}\delta_i - H(m)t_i \\ &= \delta_i + (\delta_i - t_i)H(m) \end{aligned} \tag{3}$$

and

$$\begin{aligned} d_i &= (v_i \delta_i - t_i)/l \quad [\text{where } t_i = 0, 1, \cdots] \\ &= \delta_i - t_i \end{aligned} \tag{4}$$

Since $H(m)$ and δ_i are publicly known, then the attacker by varying t_i and using *trial and error* technique, can compute the secret pair (k_i, d_i) of each signer. The time complexity of the computation is $O(n^2)$ [25], where n is the number of bits used to represent the coefficients in the linear Diophantine equation. Thus the secret pair of each signer is easily extractable using linear Diophantine equation.

3.2 Insider forgery attack

The insider forgery attack may be defined as the forging of the partial signature generated by a valid malicious signer, which affects the final multi-signature (C, δ), generated in the Lin et al.'s multi-signature scheme. Suppose a valid signer U_i acts as forger and before signing, collects all Q_j and all the pairs (C_j, δ_j), $j = 1, 2, \cdots, k; j \neq i$, and generates its own partial forged signing values using all of these. The details of such generation and the proposed insider forgery attack are described below.

Step 1.User U_i selects a random number as forged private key, say d_i^* and computes the corresponding public key as $Q_i^* = d_i^* G$. U_i instead of sending Q_i^*, generates another forged public key $Q_i = Q_i^* - \sum_{j=1, j\neq i}^{k} Q_j$ and sends the same to the collector.

Step 2.U_i selects a random number k_i^* and computes $C_i^* = k_i^* G$. Then a signature pair can be calculated as $C_i = C_i^* - \sum_{j=1, j\neq i}^{k} C_j$, $\delta_i^* = k_i^* - d_i^* H(m)$ and $\delta_i = \delta_i^* - \sum_{j=1, j\neq i}^{k} \delta_j$. The pair (C_i, δ_i) thus calculated is sent to the collector.

Step 3.The collector computes the common multi-signature as

$$\begin{aligned} C &= \sum_{j=1}^{k} C_j \\ &= C_i + \sum_{j=1,j\neq i}^{k} C_j \\ &= C_i^* - \sum_{j=1,j\neq i}^{k} C_j + \sum_{j=1,j\neq i}^{k} C_j \\ &= C_i^* \end{aligned} \tag{5}$$

and

$$\begin{aligned} \delta &= \sum_{j=1}^{k} \delta_j \\ &= \delta_i + \sum_{j=1,j\neq i}^{k} \delta_j \\ &= \delta_i^* - \sum_{j=1,j\neq i}^{k} \delta_j + \sum_{j=1,j\neq i}^{k} \delta_j \\ &= \delta_i^* \end{aligned} \tag{6}$$

Then the collector sends the forged multi-signature $(C,\delta) = (C^*,\delta^*)$ for verification.

Theorem 2.*For any message m, the forged multi-signature (C^*,δ^*) generated by U_i is a valid multi-signature..*

*Proof.*The verifier computes the common public key as

$$\begin{aligned} Q_i &= \sum_{j=1}^{k} Q_j \\ &= Q_i + \sum_{j=1,j\neq i}^{k} Q_j \\ &= Q_i^* - \sum_{j=1,j\neq i}^{k} Q_j + \sum_{j=1,j\neq i}^{k} Q_j \\ &= Q_i^* \end{aligned} \tag{7}$$

It shows that the common public key Q_i equals to the forgery public key Q_i^* of U_i. Finally, the verifier obtains the following

$$\begin{aligned} C &= \delta G + H(m)Q \\ &= \delta^* G + H(m)Q^* \\ &= (k_i^* - d_i^* H(m))G + H(m)d_i^* G \\ &= k_i^* G - H(m)d_i^* G + H(m)d_i^* G \\ &= k_i^* G \\ &= C_i^* \end{aligned} \tag{8}$$

Since $C = C_i^*$, so the forged multi-signature (C_i^*,δ_i^*) generated by U_i, is the valid multi-signature for message m. This completes the proof of the theorem.

3.3 Outsider forgery attack

In this Section, outsider forgery attack on the Lin et al.'s digital multi-signature scheme is discussed, i.e. an outsider can generate a forged multi-signature (C^*,δ^*) corresponding to the valid multi-signature (C,δ) on a message m without knowing the secret keys of all signers. The proposed attack comprises two steps as given below:

Step 1.An attacker randomly selects a set of integers $\{k_1', k_2', \cdots, k_k'\}$ and computes $k' = \sum_{i=1}^{k} k_i'$ and $C' = \sum_{i=1}^{k} k_i' G$.

Step 2.The attacker calculates the values $C^* = C - C'$ and $\delta^* = \delta - k'$, where (C,δ), is the intercepted valid multi-signature, and instead of (C,δ), the forged signature (C^*,δ^*) is sent to the verifier. The validity of the proposed outsider forgery attack is explained in the *Theorem 3* given below.

Theorem 3.*The forged multi-signature (C^*,δ^*) generated by step 1 and step 2 pretends to be a valid multi-signature for a message m.*

*Proof.*On receiving the forged multi-signature (C^*,δ^*), the verifier carries out the following derivations

$$\begin{aligned} &\delta^* G + H(m)Q \\ &= (\delta - k')G + H(m)\sum_{i=1}^{k} Q_i \\ &= \delta G - k'G + H(m)\sum_{i=1}^{k} Q_i \\ &= \sum_{i=1}^{k} \delta_i G - \sum_{i=1}^{k} k_i' G + H(m)\sum_{i=1}^{k} Q_i \\ &= \sum_{i=1}^{k} (k_i - H(m)d_i)G - \sum_{i=1}^{k} k_i' G + H(m)\sum_{i=1}^{k} d_i G \\ &= \sum_{i=1}^{k} k_i G - H(m)\sum_{i=1}^{k} d_i G - \sum_{i=1}^{k} k_i' G + H(m)\sum_{i=1}^{k} d_i G \\ &= \sum_{i=1}^{k} k_i G - \sum_{i=1}^{k} k_i' G \\ &= C - C' \\ &= C^* \end{aligned} \tag{9}$$

Therefore the forged multi-signature (C^*,δ^*) can not be detected by the verifier. Hence the theorem is proved.

4 Conclusion

In this paper, the authors presented three attacks on the Lin et al.'s digital multi-signature scheme and they are extraction of the signer's secret pair, insider forgery attack and the outsider forgery attack. It has been shown that an attacker can computes secret pairs of the signers using a technique of solving the linear Diophantine equation. It has also been shown that any malicious signer can generate a forged signature that reflects the signature final multi-signature. Finally, it has been proved that the Lin et al.'s digital multi-signature is also forgeable by an outsider.

References

[1] Chung, Y.F., Huang, K.H., Lai, F., and Chen, T.S.: ID-based digital signature scheme on the elliptic curve cryptosystem, Computer Standards and Interfaces, **29**, 601-604 (2007).

[2] Le, D.P., and Gabillon, A.: A new multisignature scheme based on strong Diffie-Hellman assumption, In: Proceedings of the third International Conference on Pairing-based Cryptography, Stanford University, USA, (2009).

[3] Biao, W., Xiaodong, Y., and Guang, Y.: An Identity-Based Multisignature Scheme from the Weil Pairing. In: Proceedings of the International Conference on Computer Design and Applications, **5**, 585-587 (2010).

[4] Gui, W-X., and Zhang, X-P.: ID-based designed-verifier multisignature without trusted PKG, In: Proceedings of the Third International Conference on Information and Computing, 213-215 (2010).

[5] Harn, L., and Ren, J.: Efficient identity-based RSA multisignatures, Computers and Security, **27**, 12-15 (2010).

[6] Islam, S. H., and Biswas, G. P.: Certificateless strong designated verifier multisignature scheme using bilinear pairings, In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics, 540-546 (2012).

[7] Islam, S. H., and Biswas, G. P.: Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings, Journal of King Saud University - Computer and Information Sciences, **26**, 89-97 (2014).

[8] Harn, L.: Digital multi-signature with distinguished signing authorities, Electronics Letters, **35**, 294-295 (1999).

[9] Shieh, S. P., Lin, C. T., Yang, W. B., and Sun, H. M.: Digital multi-signature schemes for authenticating delegates in mobile code systems, IEEE Transactions on Vehicular Technology, **49**, 164-173 (2000).

[10] Chang, C. C., Lin, I. C., and Lam, K. Y.: An ID-based multisignature scheme without reblocking and predetermined signing order, Computer Standards and Interfaces, **27**, 407-413 (2005).

[11] Bellare, M., and Neven, G.: Identity-based multi-signatures from RSA, In: Proceedings of the Topics in cryptology CT-RSA, LNCS, **4377**, 145-162 (2007).

[12] Wu, T. C., and Hsu, C. L.: Cryptanalysis of digital multi-signature schemes for authenticating delegates in mobile code systems, IEEE Transactions on Vehicular Technology, **52**, 462-465 (2003).

[13] Qian, H., Cao, Z., Wang, L., and Guo, G.: Cryptanalysis of Chang-Lin-Lam's ID-based Multi-signature Scheme, In: Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06), Springer-Verlag, **2**, 113-116 (2006).

[14] Liu, D., Luo, P., and Da, Y. Q.: Attack on digital multi-signature scheme based on elliptic curve cryptosystem, Journal of Computer Science and Technology, **22**, 92-94 (2007).

[15] Shim, K. A.: Forgery attacks on the ID-based multi-signature scheme without reblocking and predetermined signing order, Computer Standards and Interfaces, **30**, 121-123 (2008).

[16] Li, Z. C., Hui, L.C.K., Chow, K.P., Tsang, W. W., and Chan, H. W.: Cryptanalysis of Harn digital multi-signature scheme with distinguished signing authorities, Electronics Letters, **36**, 314-315 (2000).

[17] Chen, T. S., Huang, K. H., and Chung, Y. F.: Digital multi-signature scheme based on the Elliptic Curve cryptosystem, Journal of Computer Science and Technology, **19**, 570-573 (2000).

[18] Chung, Y. F., Huang, K. H., Lai, F., and Chen, T. S.: ID-based digital signature scheme on the elliptic curve cryptosystem, Computer Standards and Interfaces, **29**, 601-604 (2000).

[19] Tzeng, S. F., and Hwang, M. S.: Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem, Computer Standards and Interfaces, **26**, 61-71 (2004).

[20] Shao, Z.: Improvement of digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem, Computer Standards and Interfaces, **27**, 61-69 (2004).

[21] Zhang, J., Chen, D., and Wang, Y.: On the Security of a Digital Signature with Message Recovery Using Self-certified Public Key, In: Proceedings of the International Conference on Applied Mathematics and Computer Science (AMCOS'05), **29**, 343-346 (2005).

[22] Lin, S., Wang, B., and Li, Z.: Digital multi-signature on the generalized conic curve over Z_n, Computers and Security, **28**, 100-104 (2009).

[23] Hankerson, D., Menezes, A., and Vanstone, S.: Guide to elliptic curve cryptography, Springer-Verlag, New York, USA, (2004).

[24] Mordell, L. J.: History of the Theory of Numbers Volume II: Diophantine Analysis, New York, Academic Press, (1969).

[25] Dickson, L. E.: Diophantine Equations, Bronx, New York, Chelsea Publishing, (1992).

S. K. Hafizul Islam completed his Ph.D in Computer Science and Engineering from Indian School of Mines, Dhanbad, India, under the prestigious INSPIRE Fellowship Ph.D Program (funded by DST, Govt. of India) and Information Security Education and Awareness (ISEA) program (funded by Department of Information Technology (DIT), Ministry of Communication and Information Technology, Govt. of India, No. MIT (2)/2006-08/189/CSE). Dr. Islam received his B.Sc (Hons.) in Mathematics and M.Sc in Applied Mathematics from Vidyasagar University, West Bengal, India in 2004 and 2006, and M.Tech from Indian School of Mines, Dhanbad in 2009, respectively. Dr. Islam is currently holding the position of Assistant Professor in the Department of Computer Science & Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India. His research interest includes Cryptography, Network/Information Security and Computer Networks.

G. P. Biswas received B.Sc (Engg.) and M.Sc (Engg.) degrees in Electrical & Electronics Engineering and Computer Science & Engineering, respectively. He completed his PhD degree in Computer Science & Engineering from Indian Institute of Technology, Kharagpur, India. He is currently working as a Professor in the Department of Computer Science & Engineering, Indian school of Mines, Dhanbad, Jharkhand, India. His main research interests include Cryptography, Computer Network and Security, Cellular Automata, VLSI Design.