Chapter 4
Improvement of an ID-Based Threshold Signcryption Scheme

Wei Yuan, Liang Hu, Xiaochun Cheng, Hongtu Li, Jianfeng Chu and Yuyu Sun

Abstract Signcryption can realize the function of encryption and signature in a reasonable logic step, which can lower computational costs and communication overheads. In 2008, Fagen Li et al. proposed an efficient secure id-based threshold signcryption scheme. The authors declared that their scheme had the attributes of confidentiality and unforgeability in the random oracle model. However, our previous analysis shows that scheme is insecure against malicious attackers. Further, we propose a probably-secure improved scheme to correct the vulnerable and give the unforgeability and confidentiality of our improved scheme under the existing security assumption.

Keywords Identity-based · Signcryption · Bilinear pairing · Cryptanalysis

W. Yuan · L. Hu · H. Li · J. Chu (✉) · Y. Sun
Department of Computer Science and Technology, Jilin University, Changchun, China
e-mail: chujf@jlu.edu.cn

W. Yuan
e-mail: yuanwei1@126.com

L. Hu
e-mail: hul@mails.jlu.edu.cn

H. Li
e-mail: li_hongtu@hotmail.com

Y. Sun
e-mail: sunyy@ccu.edu.cn

X. Cheng
The School of Computing Science, Middlesex University, London, UK
e-mail: xiaochun.cheng@gmail.com

Y. Sun
Software Institue, Changchun University, Changchun, China

X. He et al. (eds.), *Computer, Informatics, Cybernetics and Applications*,
Lecture Notes in Electrical Engineering 107, DOI: 10.1007/978-94-007-1839-5_4,

4.1 Introduction

Encryption and signature are the two basic cryptographic tools offered by public key cryptography for achieving confidentiality and authentication. Signcryption can realize the function of encryption and signature in a reasonable logic step which is proposed by Zheng [1]. Comparing to the traditional way of signature then encryption or encryption then signature, signcryption can lower the computational costs and communication overheads. As a result, a number of signcryption schemes [2–8] were proposed following Zheng's work. The security notion for signcryption was first formally defined in 2002 by Baek et al. [9] against adaptive chosen ciphertext attack and adaptive chosen message attack. The same as signature and encryption, signcryption meets the attributes of confidentiality and unforgeability as well. In 1984, Shamir [10] introduced identity-based public key cryptosystem, in which a user's public key can be calculated from his identity and defined hash function, while the user's private key can be calculated by a trusted party called Private Key Generator (PKG). The identity can be any binary string, such as an email address and needn't to be authenticated by the certification authentication. As a result, the identity-based public key cryptosystem simplifies the program of key management to the conventional public key infrastructure. In 2001, Boneh and Franklin [11] found bilinear pairings positive in cryptography and proposed the first practical identity-based encryption protocol using bilinear pairings. Soon, many identity-based [12–18] schemes were proposed and the bilinear pairings became important tools in constructing identity-based protocols. Group-oriented cryptography [19] was introduced by Desmedt in 1987. Elaborating on this concept, Desmedt and Frankel [20] proposed a (t, n) threshold signature scheme based RSA system [21]. In such a (t, n) threshold signature scheme, any to out of n signers in the group can collaboratively sign messages on behalf of the group for sharing the signing capability. Identity-based signcryption schemes combine the advantages of identity-based public key cryptosystem and Signcryption. The first identity-based threshold signature scheme was proposed by Baek and Zheng [22]. Then Duan et al. [23] proposed an identity-based threshold signcryption scheme in the same year by combining the concepts of identity based threshold signature and encryption together. However, in Duan et al.'s scheme, the master-key of the PKG is distributed to a number of other PKGs, which creates a bottleneck on the PKGs. In 2005, Peng and Li proposed an identity-based threshold signcryption scheme [24] based on Libert and Quisquater's identity-based signcryption scheme [25]. However, Peng and Li's scheme dose not provide the forward security. In 2008, another scheme was proposed by Fagen Li et al. [26], which is more efficient comparing to previous scheme.

In this chapter, we show that the threshold signcryption scheme of Fagen Li et al. is vulnerable if the attacker can replaces the group public key or even the attacker can intercept the intermediate messages. Further, we propose a probably-secure improved scheme to correct the vulnerable and give the unforgeability and confidentiality of our improved scheme under the existing security assumption.

4.2 The Improvement of Fagen Li et al.' Scheme

The scheme involves four roles: the PKG, a trust dealer, a sender group $U_A = \{M_1, M_2, \ldots, M_n\}$ with identity ID_A and a receiver Bob with identity ID_B.

Setup: given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order q (with G_1 additive and G_2 multiplicative), a generator P of G_1, a bilinear map $e : G_1 \times G_1 \to G_2$, a secure symmetric cipher (E,D) and hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : G_2 \to \{0,1\}^{n_1}$, $H_3 : \{0,1\}^* \times G_1 \times \{0,1\}^* \times G_1 \to Z_q^*$. The PKG chooses a master-key $s \in_R Z_q^*$ and computes $P_{pub} = sP$. The PKG publishes system parameters $\{G_1, G_2, n_1, e, P, P_{pub}, E, D, H_1, H_2, H_3\}$ and keeps the master-key s secret. **Extract**: Given an identity ID, the PKG computes $Q_{ID} = H_1(ID)$ and the private key $S_{ID} = sQ_{ID}$. Then PKG sends the private key to its owner in a secure way.

Keydis: suppose that a threshold t and n satisfy $1 \le t \le n < q$. To share the private key S_{ID_A} among the group U_A, the trusted dealer performs the steps below.

1) Choose $F_1, \ldots, F_{t-1}$ uniformly at random from G_1^*, construct a polynomial $F(x) = S_{ID_A} + xF_1 + \cdots + x^{t-1}F_{t-1}$
2) Compute $S_i = F(i)$ for $i = 0, \ldots, n$. ($S_0 = S_{ID_A}$). Send S_i to member M_i for $i = 1, \ldots, n$ secretly.
3) Broadcast $y_0 = e(S_{ID_A}, P)$ and $y_j = e(F_j, P)$ for $j = 1, \ldots, t-1$.
4) Each M_i then checks whether his share S_i is valid by computing $e(S_i, P) = \prod_{j=0}^{t-1} y_j^{i^j}$. If S_i is not valid, M_i broadcasts an error and requests a valid one.

Signcrypt: let $M_1, \ldots, M_t$ are the t members who want to cooperate to signcrypt a message m on behalf of the group U_A.

1) Each M_i chooses $x_i \in_R Z_q^*$, computes $R_{1i} = x_i P$, $R_{2i} = x_i P_{pub}$, $\tau_i = e(R_{2i}, Q_{ID_B})$ and sends (R_{1i}, τ) to the clerk C.
2) The clerk C (one among the t cooperating players) computes $R_1 = \prod_{i=1}^{t} R_{1i}$, $\tau = \prod_{i=1}^{t} \tau_i$, $k = H_2(\tau)$, $c = E_k(m)$, and $h = H_3(m, R_1, k, Q_{ID_A})$.
3) Then the clerk C sends h to M_i for $i = 0, \ldots, t$.
4) Each M_i computes the partial signature $W_i = x_i P_{pub} + h\eta_i S_i$ and sends it to the clerk C, where $\eta = \prod_{j=1, j\neq i}^{t} -j(i-j)^{-1} \bmod q$.
5) Clerk C verifies the correctness of partial signatures by checking if the following equation holds: $e(P, W_i) = e(R_{1i}, P_{pub})(\prod_{j=0}^{t-1} y_j^{i^j})^{h\eta_i}$

If all partial signatures are verified to be legal, the clerk C computes $W = \sum_{i=1}^{t} W_i$; otherwise rejects it and requests a valid one.

6) The final threshold signcryption is $\sigma = (c, R_1, W)$.

Unsigncrypt: when receiving σ, Bob follows the steps below.

1) Compute $\tau = e(R_1, S_{ID_B})$ and $k = H_2(\tau)$.

2) Recover $m = D_k(c)$
3) Compute $h = H_3(m, R_1, k, Q_{ID_A})$ and accept σ if and only if the following equation holds: $e(P, W) = e(P_{pub}, R_1 + hQ_{ID_A})$

4.3 Security Analysis of Our Improved Scheme

In this section, we will give a formal proof on Unforgeability and Confidentiality of our scheme under CDH problem and DBDH problem.

Theorem 1 (Unforgeability) *Our improved scheme is secure against chosen message attack under the random oracle model if CDH problem is hard.*

Proof Suppose the challenger C wants to solve the CDH problem. That is, given (aP, bP) C should computes abP.

C chooses system parameters $\{G_1, G_2, n_1, e, P, P_{pub}, E, D, H_1, H_2, H_3\}$, sets $P_{pub} = aP$, and sends parameters to the adversary E (the hash functions H_1, H_2, H_3 are random oracles).

H_1query: C maintains a list L_1 to record H_1queries.L_1 has the form of $(ID, \alpha, Q_{ID}, S_{ID})$. Suppose the adversary Eve can make H_1 queries less than q_{H_1} times. C selects a random number $j \in [1, q_{H_1}]$. If C receives the j-th query, he will return $Q_{ID_j} = bP$ to Eve and sets $(ID_j, \perp, Q_{ID_j} = bP, \perp)$ on L_1. Else C selects $\alpha_i \in Z_q^*$ computes $Q_{ID_i} = \alpha_i P$, $S_{ID_i} = \alpha_i P_{pub}$, returns Q_{ID_i} to E and sets $(ID_i, \alpha_i, Q_i, S_i)$ on L_1.

H_2query: C maintains a list L_2 to record H_2queries.L_2 has the form of (τ, k). If C receives a query about τ_i, selects $k_i \in Z_q^*$, returns k_i to E, and sets (τ_i, k_i) on L_2.

H_3query: C maintains a list L_3 to record H_3 queries. L_3 has the form of (m, R, k, Q, h). If C receives a query about $(m_i, R_{1i}, k_i, Q_{ID_i})$, selects $h_i \in Z_q^*$, returns h_i to Eve, and sets $(m_i, R_{1i}, k_i, Q_{ID_i}, h_i)$ on L_3.

Signcrypt query: if C receives a query about Signcrypt with message m_i, identity ID_i

1. Select $x_i \in Z_q^*$, $W_i \in G_1$
2. Look-up L_1, L_2, set $Q_{ID_i} = \alpha_i P$ in L_1, $k_i = k_i$ in L_2, and compute $R_i = x_i Q_{ID_i}$
3. Set $h_i = H_3(m_i, R_i, k_i, Q_{ID_i})$.
4. Return (h_i, W_i) to Eve.

Finally, Eve output a forged signcryption (m, h_i, W_i, Q_{ID_i}). If $Q_{ID_i} \neq Q_{ID_j}$, Eve fails. Else, if $Q_{ID_i} = Q_{ID_j}$, Eve succeeds in forging a signcryption.

As a result, C gains two signcryption ciphertexts which meet:

$$e(P, W_i) = e(P_{pub}, R_i + h_i Q_{ID_i})$$

$$e(P, W_j) = e(P_{pub}, R_j + h_j Q_{ID_j})$$

Thus,

$$e\big(P,(W_i-W_j)\big)=e\big(P_{pub},(R_i+h_iQ_{ID_i})-(R_j+h_jQ_{ID_j})\big) \tag{4.1}$$

Note $Q=Q_{ID_i}=Q_{ID_j}$, (4.1) can be expressed as

$$e\big(P,(W_i-W_j)\big)=e\big(P_{pub},(R_i-R_j)+(h_i-h_j)Q\big) \tag{4.2}$$

$$\because P_{pub}=aP, Q_{ID_j}=bP$$

(4.2) can be expressed as $e\big(P,(W_i-W_j)\big)=e\big(aP,((\alpha_i-\alpha_j)+(h_i-h_j))bP\big)$

$$\therefore W_i-W_j=\big((\alpha_i-\alpha_j)+(h_i-h_j)\big)abP$$

Hence, the CDH problem $abP=\frac{W_i-W_j}{(\alpha_i-\alpha_j)+(h_i-h_j)}$ can be computed by C with aP and bP.

Theorem 2 (Confidentiality) *Our improved scheme is secure against adaptive chosen ciphertext and identity attack under the random oracle model if DBDH problem is hard.*

Proof Suppose the challenger C wants to solve the DBDH problem. That is, given (P,aP,bP,cP,τ), C should decide whether $\tau=e(P,P)^{abc}$ or not. If there exists an adaptive chosen ciphertext and identity attacker for our improved scheme, C can solve the DBDHP.

C chooses system parameters $\{G_1,G_2,n_1,e,P,P_{pub},E,D,H_1,H_2,H_3\}$, sets$P_{pub}=aP$, and sends parameters to the adversary E (the hash functions $H_1,H_2,H_3$are random oracles).

H_1 query: C maintains a list L_1 to record H_1 queries. L_1 has the form of $(ID,\alpha,Q_{ID},S_{ID})$. Suppose the adversary Eve can make H_1 queries less than q_{H_1} times. C selects a random number $j\in[1,q_{H_1}]$. If C receives the j-th query, he will return $Q_{ID_j}=bP$ to Eve and sets $(ID_j,\perp,Q_{ID_j}=bP,\perp)$ on L_1. Else C selects $\alpha_i\in Z_q^*$ computes $Q_{ID_i}=\alpha_iP$, $S_{ID_i}=\alpha_iP_{pub}$, returns Q_{ID_i} to E and sets (ID_i,α_i,Q_i,S_i) on L_1.

H_2 query: C maintains a list L_2 to record H_2 queries.L_2 has the form of (τ,k). If C receives a query about τ_i, selects $k_i\in Z_q^*$, returns k_i to E, and sets (τ_i,k_i) on L_2.

H_3 query: C maintains a list L_3 to record H_3 queries.L_3 has the form of (m,R,k,Q,h). If C receives a query about $(m_i,R_{1i},k_i,Q_{ID_i})$, selects $h_i\in Z_q^*$, returns h_i to Eve, and sets $(m_i,R_{1i},k_i,Q_{ID_i},h_i)$ on L_3.

Signcrypt query: if C receives a query about Signcrypt with message m_i, identity ID_i

1. Select $c_i\in Z_q^*$, $W_i\in G_1$
2. Look-up L_1, L_2, set$Q_{ID_i}=\alpha_iP$ in L_1, $k_i=k_i$ in L_2. Compute $R_i=c_iP$, if $ID_i\neq ID_j$. Else, if $ID_i=ID_j$, compute $R_i=cP$

3. Set $h_i = H_3(m_i, R_i, k_i, Q_{ID_i})$.
4. Return (h_i, W_i) to Eve.

After the first stage, Eve chooses a pair of identities on which he wishes to be challenged on (ID_i, ID_j). Note that Eve can not query the identity of ID_A. Then Eve outputs two plaintexts m_0 and m_1. C chooses a bit $b \in \{0, 1\}$ and signcrypts m_b. To do so, he sets $R_1^* = cP$, obtains $k^* = H_2(\tau)$ from the hash function H_2, and computes $c_b = E_{k_1^*}(m_b)$. Then C chooses $W^* \in G_1$ and sends the ciphertext $\sigma^* = (c_b, R_1^*, W^*)$ to Eve. Eve can performs a second series of queries like at the first one. At the end of the simulation, she produces a bit b' for which he believes the relation $\sigma^* = \text{Signcrypt}\ (m_{b'}, \{S_i\}_{i=1,\ldots,t}, ID_j)$holds. If $b = b'$, C outputs $\tau = e(R_1^*, S_{ID_j}) = e(cP, abP) = e(P, P)^{abc}$. Else, C outputs $\tau \neq e(P, P)^{abc}$. So C can solve the BDDH problem.

4.4 Conclusion

In this chapter, we show that the threshold signcryption scheme of Fagen Li et al. is vulnerable if the attacker can replaces the group public key. Then we point out that the receiver uses the senders' public key without any verification in the unsigncrypt stage cause this attack. Further, we propose a probably-secure improved scheme to correct the vulnerable and give the unforgeability and confidentiality of our improved scheme under the existing security assumption.

Acknowledgment The authors would like to thank the editors and anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China under Grant No. 60873235 and 60473099, the National Grand Fundamental Research 973 Program of China (Grant No. 2009CB320706), Scientific and Technological Developing Scheme of Jilin Province (20080318), and Program of New Century Excellent Talents in University (NCET-06-0300).

References

1. Zheng Y (1997) Digital signcryption or how to achieve cost (signature & Encryption) $\ll$ cost (signature) + cost (encryption), In: Proceedings of advances in CRYPTO'97, LNCS 1294. Springer, Berlin, pp 165–179
2. Bao F, Deng RH (1997) A signcryption scheme with signature directly verifiable by public key. PKC'98 LNCS, vol 1431. Springer, Berlin, pp 55–59
3. Chow SSM, Yiu SM, Hui LCK, Chow KP (2004) Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. ICISC'03 LNCS, vol 2971. Springer, Berlin, pp 352–269
4. Boyen X, Multipurpose identity based signcryption: a swiss army knife for identity based cryptography. CRYPT'03 LNCS, vol 2729. Springer, Berlin, pp 383–399
5. Mu Y, Varadharajan V (2000) Distributed signcryption. INDOCRYPT'00. LNCS, vol 1977. Springer, Berlin, pp 155–164

6. Yang G, Wong DS, Deng X (2005) Analysis and improvement of a signcryption scheme with key privacy. ISC'05. LNCS, vol 3650. Springer, Berlin, pp 218–232
7. SteinFeld R, Zheng Y (2000) A signcryption scheme based on integer factorization. ISW'00. LNCS, vol 1975. Springer, Berlin, pp 308–322
8. Libert B, Quisquater J (2004) Efficient signcryption with key prevacy from gap Diffie-Hellman groups. PKC'04. LNCS vol 2947. Springer, Berlin, pp 187–200
9. Baek J, Steinfeld R, Zheng Y (2002) Formal proofs for the security of signcryption. PKC'02. LNCS vol 2274. Springer, Berlin, pp 80–98
10. Shamir A (1984) Identity-based cryptosystems and signature schemes. CRYPTO'84. LNCS vol 196. Springer, Berlin, pp 47–53
11. Boneh D, Franklin M (2001) Identity-based encryption from well pairing. CRYPTO'01. LNCS vol 2139. Springer, Berlin, pp 213–229
12. Barreto PSLM, Libert B, Mccullagh N, Quisquater JJ (2005) Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. ASIACRYPT'05. LNCS, vol 3788. Springer, Berlin, pp 515–532
13. Li F, Hu X, Nie X (2009) A new multi-receiver ID-based signcryption scheme for group communication. ICCCAS'2009. IEEE Press, San Jose, pp 296–300
14. Han Y, Gui X (2009) Multi-recipient signcryption for secure group communication. ICIEA 2009, pp 161–165
15. Jin Z, Wen Q, Du H (2010) An improved semantically-secure identity-based signcryption scheme in the standard model. Comput Electr Eng 36(3):545–552
16. Huang X, Susilo W, Mu Y, Zhang E (2005) Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world. 19th international conference on advanced information networking and applications, Taiwan, pp 649–654
17. Liu Z, Hu Y, Zhang X, Ma H (2010) Certificateless signcryption scheme in the standard model. Inf Sci 180(3):452–464
18. Yu Y, Bo Y, Sun Y, Zhu S-l (2009) Identity based signcryption scheme without random oracles. Comput Stand Interfac 31(1):56–62
19. Desmedt Y (1987) Society and group oriented cryptography: a now concept. CRYPTO'87. LNCS, vol 293. Springer, Berlin, pp 120–127
20. Desmedt Y, Frankel Y (1991) Shared generation of authenticators and signatures. CRYPTO'91. LNCS, vol 576. Springer, Berlin, pp 457–469
21. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 2(2):120–126
22. Baek J, Zheng Y (2004) Identity-based threshold signature scheme from the bilinear pairings. International conference on information technology, Las Vegas, pp 124–128
23. Duan S, Cao Z, Lu R (2004) Robust ID-based threshold signcryption scheme from pairings. International conference on information security, Shanghai, pp 33–37
24. Peng C, Li X (2005) An identity-based threshold signcryption scheme with semantic security. Computational intelligence and security 2005. LNAI, vol 3902. Springer, Berlin, pp 173–179
25. Libert B, Quisquater JJ (2003) Anew identity based signcryption schemes from pairings. IEEE information theory workshop, Paris, pp 155–158
26. Li F, Yu Y (2008) An efficient and provably secure ID-based threshold signcryption scheme, ICCCAS. Springer, Xiamen, pp 488–492
27. Malone LJ (2002) Identity based signcryption. In: cryptology ePrint archive. Report, (14):098–106
28. Chow SSM, Yiu SM, Hui LCK, Chow KP (2004) Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. In: Lin J-I, Lee D-H (eds) ICISC 2003, LNCS, vol 2971. Springer, Berlin, pp 352–369
29. Boyen X (2003) Multipurpose identity based signcryption: a Swiss army knife for identity based cryptography. In: Boneh D (ed) CRYPTO 2003. LNCS, vol 2729. Springer, Berlin, pp 383–399