Cryptanalysis of Attribute-based Ring Signcryption Scheme

Hu Xiong, Ji Geng, Zhiguang Qin, and Guobin Zhu
(Corresponding author: Hu Xiong)
School of Computer Science and Engineering & University of Electronic Science and Technology of China[1]
No. 4, North Jianshe Road, Chenghua District, Chengdu, Sichuan 610054, China
(Email: xionghu.uestc@gmail.com)
(Received Apr. 8, 2013; revised and accepted Nov. 3, 2014)

Abstract

Signcryption can offer authentication and confidentiality simultaneously with better efficiency than traditional signature-then-encryption approach. Ring signature enables a user to conscribe arbitrarily a group of ring members and sign a message on behalf of the ring (which includes himself) without revealing his real identity. By integrating the notion of signcryption and ring signature, ring signcryption has been initialized to leak secrets in an authenticated and confidential way anonymously. Recently, Guo *et al.* (Guo Z, Li M, Fan X. Attribute-based ring signcryption scheme. *Security and Communication Networks*, vol. 6, no. 6, pp. 790-796, 2013) proposed a ring signcryption scheme in attribute-based cryptography. Furthermore, they claimed that their scheme can satisfy confidentiality and unforgeability in the random oracle model. Unfortunately, by giving concrete attacks, we indicate that Guo *et al.*'s attribute-based ring signcryption scheme doesn't provide confidentiality and unforgeability.

Keywords: Attribute-based cryptography; cryptanalysis; ring signcryption; provable security

1 Introduction

To offer authenticity and confidentiality simultaneously with better efficiency than traditional "sign-then-encrypt" approach, Zheng [24] initially formalized the notion of signcryption. Since Zheng's pioneering work, dozens of signcryption schemes have been proposed following various research lines. Firstly, the existing signcryption scheme can be classified as RSA-based [10], IF-based [20], elliptic curves-based [21, 25], pairing-based [4], lattice-based [12] according to the underlying keys. Secondly, ID-based [3, 5, 6], certificateless [2, 7], self-certified [13] and certificate-based [15] signcryption also have been proposed to simplify the public key certificates in the traditional public key infrastructure. Thirdly, the extensions of signcryption have been proposed by integrating the pure signcryption with other cryptographic primitives, such as ring signcryption [1, 22], group signcryption [11], threshold unsigncryption [14, 23] and proxy signcryption [17, 18]. The survey of signcryption and related applications can be found in [8].

As one of the extension of signcryption, ring signcryption was initially formalized by Huang *et al.* [1] and allows a signer conscripts a group of ring members and signcrypts one message on behalf of the ring without revealing his real identity. Furthermore, the procedure of signcryption does not need the cooperation of other ring members. Thus, ring signcryption can be applied in some concrete applications where authenticity, confidentiality and anonymity receive concern simultaneously. On the other hand, to use biometric-based identities in the Identity-based cryptosystem, attribute-based cryptography has been proposed in 2005 [19]. Recently, Guo et al. [9] introduced ring signcryption in the attribute-based cryptography by integrating the notion of attribute-based ring signature [16] and attribute-based encryption [19]. In an attribute-based signcryption, a signer can get its private key for attributes set ω from a trusted private key generator. Then, this signer can signcrypt message on behalf of a subset $\omega' \subseteq \omega$. Here, all users with this attributes subset ω' can be considered as the ring. After that, a concrete attribute-based ring signcryption based on bilinear pairings has also been suggested in this paper. They claimed that their scheme can achieve unforgeability and confidentiality in the random oracle model. However, in this paper, we show that their scheme cannot provide confidentiality and unforgeability at all by giving concrete attacks. Furthermore, the basic reason behind our attack has also been analyzed.

The rest of this paper is organized as follows. In Section 2, we review the Guo-Li-Fan attribute-based ring signcryption scheme. After that, we explain why their scheme can not provide unforgeability and confidentiality in Sections 3 and 4 respectively. Finally, the conclusions are given in Section 5.

2 Overview of the Guo-Li-Fan Scheme

We describe Guo-Li-Fan's attribute-based ring signcryption scheme [9] as follows. In their scheme, the signer can signcrypt a message on behalf of d attributes, where d will be defined in the **Setup** algorithm. We then review Lagrange interpolation as follows. Given d points $q(1), \cdots, q(d)$ on a $d-1$ degree polynomial, $q(i)$ for any $i \in \mathbb{Z}_p$ can be computed by adopting Lagrange interpolation technique. Assume S be a set in $\mathbb{Z}_p$ with d-elements and the Lagrange coefficient $\Delta_{i,S}$ for $i \in \mathbb{Z}_p$ as follows.

$$\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-i}{i-j}$$

Setup(κ): Given a security parameter κ, the trusted private key generator (PKG) first defines the set of universal attributes $\mathcal{U}$ in $\mathbb{Z}_p$, where $|\mathcal{U}| = l$. After that, a $d-1$ default attributes set from $\mathbb{Z}_p$ is given as $\Omega = \{\Omega_1, \cdots, \Omega_{d-1}\}$. Furthermore, PKG selects a pairing $e : G_1 \times G_1 \rightarrow G_2$ where the order of G_1 and G_2 is prime $p > 2^\kappa$, and a generator g of G_1. PKG then chooses $t_1, \cdots, t_l, t_{l+1}, \cdots, t_{l+d-1} \in \mathbb{Z}_p$ randomly and computes $T_i = g^{t_i}$ where $1 \leq i \leq l+d-1$. PKG also picks $\alpha \in \mathbb{Z}_p$ at random and computes $Y = e(g,g)^\alpha$. Finally, PKG selects three cryptographic hash functions: $H_1 : G_2 \rightarrow \{0,1\}^{|M|} \times \mathbb{Z}_p^* \times G_1$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, and $H_3 : \{0,1\}^{|M|} \times \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$, where $|M|$ denotes the length of the ciphertext. The public parameters PK are published as follows:

$$PK = (G_1, G_2, e, g, \{T_i\}_{i=1}^{l+d-1}, Y, H_1, H_2, H_3).$$

The master secret key MK is denoted as $MK = (\alpha, \{t_i\}_{i=1}^{l+d-1})$.

Key Extract(MK, ω): Given the user with attribute set $\omega \subseteq \mathcal{U}$, the PKG generates the private key for ω as follows:

- A $d-1$ degree polynomial $q(x)$ is picked at random such that $q(0) = \alpha$.
- Generates a new attribute set $\hat{\omega} = \omega \cup \Omega$ and computes $D_i = g^{\frac{q(i)}{t_i}}$ for each $i \in \hat{\omega}$.
- Outputs the private key D_i for each $i \in \hat{\omega}$.

Signcryption(m, ω_S, ω_R): To signcrypt a message m to a receiver $\mathcal{R}$, the sender $\mathcal{S}$ follows the steps below:

- Chooses a subset ω_S' with d elements from $\hat{\omega}_S$ (where f attributes $\{i_1, \cdots, i_f\}$ are chosen from ω_S to signcrypt the message, and $d-f$ attributes are chosen from default attributes set Ω).
- The sender $\mathcal{S}$ randomly chooses $r \in \mathbb{Z}_p^*$, and set $s = H_3(m, r)$, $U = g^s$, and $X = Y^s = e(g,g)^{\alpha \cdot s}$. $\mathcal{S}$ then computes $E_i = T_i^s$ for each $i \in \omega_S'$ and for each $j \in \omega_R$.
- Let $\omega_S' = \{1, \cdots, d\}$, and chooses $k \in \omega_S'$ randomly. Defines the elements in set $\omega_S' \cup \omega_R$ to be the ring. For $l \in \omega_S' \cup \omega_R$ and $l \neq k$, chooses $U_l \in \mathbb{Z}_p^*$ at random and computes $h_l = H_2(m, U_l, X, \omega_S' \cup \omega_R, l)$, where $|\omega_S' \cup \omega_R| = n_R + d$. For $l = k$, chooses r_k from $\mathbb{Z}_p^*$ randomly and computes

$$\begin{aligned} U_k &= E_k^{r_k} / \prod_{l \in \omega_S' \cup \omega_R, l \neq k} U_l \cdot E_l \\ &= g^{t_k \cdot r_k \cdot s} / \prod_{l \in \omega_S' \cup \omega_R, l \neq k} U_l \cdot g^{t_l \cdot h_l \cdot s} \\ h_k &= H_2(m, U_k, X, \omega_S' \cup \omega_R, k) \\ V &= E_k^{r_k + h_k} \end{aligned}$$

- Compute $y = (m \| r \| V) \oplus H_1(X)$.
- Finally, the ciphertext CT is denoted as $CT = (y, \omega_S', \omega_R, U, \{U_l\}_{l=1}^{n_R+d}, \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R})$.

UnsigncryptionCT: After receiving the ciphertext CT, $\mathcal{R}$ decrypts the ciphertext as follows.

- For $CT = (y, \omega_S', \omega_R, U, \{U_l\}_{l=1}^{n_R+d}, \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R})$, select a subset $\omega_{R'}$ with d-elements subset from attribute set ω_R.
- Computes

$$\begin{aligned} X' &= \prod_{j \in \omega_{R'}} e(D_j, E_j)^{\Delta_{j,S}(0)} \\ &= \prod_{j \in \omega_{R'}} e(g^{\frac{q(j)}{t_j}}, g^{t_j \cdot s})^{\Delta_{j,S}(0)} \\ &= e(g,g)^{\alpha \cdot s} \end{aligned}$$

  and retrieves m', r', V' as $(m' \| r' \| V') = y \oplus H_1(X')$.
- Computes $s' = H_3(m', r')$ and verifies whether $U \stackrel{?}{=} g^{s'}$ holds or not.
- For $l \in \{1, \cdots, n_R + d\}$, computes $h_l' = H_2(m, U_l, X, \omega_S' \cup \omega_R, l)$ and verifies

$$e(g, \prod_{l=1}^{n_R+d} U_l \cdot g^{t_l \cdot h_l' \cdot s'}) \stackrel{?}{=} e(g, V')$$

  holds or not. If so, $\mathcal{R}$ accepts CT as the valid ring signcryption on the message m'; $\mathcal{R}$ rejects otherwise.

Note that the original scheme in [9] has several typos. In the Step 1 of **Signcryption** algorithm, instead of writing Chooses a subset ω_S' with d elements from $\hat{\omega}_S$, it was written as Chooses a subset ω_S' with d elements from ω_S. In the Step 2 of **Signcryption** algorithm, instead of writing for each $i \in \omega_S'$, it was written as for each $i \in \omega_{S'}$. In the Step 3 of **Signcryption** algorithm, instead of writing $g^{t_k \cdot r_k \cdot s} / \prod_{l \in \omega_S' \cup \omega_R, l \neq k} U_l \cdot g^{t_l \cdot h_l \cdot s}$, it was written as $g^{t_k \cdot r_k \cdot s} / \prod_{l \in \omega_S' \cup \omega_R, l \neq k} U_l \cdot g^{t_l \cdot h_i \cdot s}$. We have corrected these typos to maintain consistency of the scheme.

3 On the Unforgeability of the Guo-Li-Fan Scheme

In this section, we show that the Guo-Li-Fan's certificate-based ring signcryption scheme is not secure against forgery attacks. After receiving a valid ciphertext $CT = (y, \omega'_S, \omega_R, U, \{U_l\}_{l=1}^{n_R+d}, \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R})$, the adversary $\mathcal{A}$ can forge a valid ciphertext $CT^* = (y^*, \omega'_S, \omega_R, U^*, \{U_l^*\}_{l=1}^{n_R+d}, \{E_i^*\}_{i=1}^{d}, \{E_i^*\}_{i=1}^{n_R})$ on message m^* as follows:

- $\mathcal{A}$ randomly chooses $r^* \in \mathbb{Z}_p^*$, and set $s^* = H_3(m^*, r^*)$, $U^* = g^{s^*}$, and $X^* = Y^{s^*} = e(g,g)^{\alpha \cdot s^*}$. $\mathcal{S}$ then computes $E_i^* = T_i^{s^*}$ for each $i \in \omega'_S$ and for each $j \in \omega_R$.
- Let $\omega'_S = \{1, \cdots, d\}$, and chooses $k \in \omega'_S$ randomly. Defines the elements in set $\omega'_S \cup \omega_R$ to be the ring. For $l \in \omega'_S \cup \omega_R$ and $l \neq k$, chooses $U_l^* \in \mathbb{Z}_p^*$ at random and computes $h_l^* = H_2(m^*, U_l^*, X^*, \omega'_S \cup \omega_R, l)$, where $|\omega'_S \cup \omega_R| = n_R + d$. For $l = k$, chooses r_k^* from $\mathbb{Z}_p^*$ randomly and computes

$$\begin{aligned} U_k^* &= (E_k^*)^{r_k^*} / \prod\nolimits_{l \in \omega'_S \cup \omega_R, l \neq k} U_l^* \cdot E_l^* \\ &= g^{t_k \cdot r_k^* \cdot s^*} / \prod\nolimits_{l \in \omega'_S \cup \omega_R, l \neq k} U_l^* \cdot g^{t_l \cdot h_l^* \cdot s^*} \\ h_k^* &= H_2(m^*, U_k^*, X^*, \omega'_S \cup \omega_R, k) \\ V^* &= (E_k^*)^{r_k^* + h_k^*} \end{aligned}$$

- Compute $y^* = (m^* \| r^* \| V^*) \oplus H_1(X^*)$.
- Finally, the ciphertext CT^* on message m^* is denoted as $CT^* = (y^*, \omega'_S, \omega_R, U^*, \{U_l^*\}_{l=1}^{n_R+d}, \{E_i^*\}_{i=1}^{d}, \{E_i^*\}_{i=1}^{n_R})$.

The ring signcryption is correct because of the following:

- X^* can be reconstructed as follows:

$$\begin{aligned} X^* &= \prod\nolimits_{j \in \omega_{R'}} e(D_j, E_j^*)^{\Delta_{j,S}(0)} \\ &= \prod\nolimits_{j \in \omega_{R'}} e(g^{\frac{q(j)}{t_j}}, g^{t_j \cdot s^*})^{\Delta_{j,S}(0)} \\ &= e(g,g)^{\alpha \cdot s^*} \end{aligned}$$

- After retrieving $(m^* \| r^* \| V^*) = y^* \oplus H_1(X^*)$, it is easy to verify that $s^* = H_3(m^*, r^*)$ and $U^* = g^{s^*}$.
- Finally, it is obvious that

$$e(g, \prod_{l=1}^{n_R+d} U_l^* \cdot g^{t_l \cdot h_l^* \cdot s^*}) \stackrel{?}{=} e(g, V^*),$$

where $h_l^* = H_2(m^*, U_l^*, X^*, \omega'_S \cup \omega_R, l)$ for $l \in \{1, \cdots, n_R + d\}$.

The basic reason of our attack works is that the private key of the signer has not been mentioned in the **Signcryption** algorithm. Thus, anyone can generate valid ciphertext on any message on behalf of the ring without the knowledge of any ring member's private key by executing **Signcryption** algorithm directly.

4 On the Confidentiality of the Guo-Li-Fan Scheme

In this section, we show that the Guo-Li-Fan's certificate-based ring signcryption scheme cannot offer confidentiality. After receiving a valid ciphertext $CT = (y, \omega'_S, \omega_R, U, \{U_l\}_{l=1}^{n_R+d}, \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R})$ generated by a user $\mathcal{S}$. Here, ω'_S denotes $\mathcal{S}$'s attributes subset and depicts the ring. Assume that the adversary $\mathcal{A}$ is one of the member in the ring, and therefore $\mathcal{A}$ has the private key D_j for $j \in \omega'_S$ corresponding to the attributes sets ω'_S with d elements according to the definition in [9, 16].

Thus, $\mathcal{A}$ can decrypt the ciphertext CT as follows.

$$\begin{aligned} X &= \prod\nolimits_{j \in \omega'_S} e(D_j, E_j)^{\Delta_{j,S}(0)} \\ &= \prod\nolimits_{j \in \omega'_S} e(g^{\frac{q(j)}{t_j}}, g^{t_j \cdot s})^{\Delta_{j,S}(0)} \\ &= e(g,g)^{\alpha \cdot s}. \end{aligned}$$

Then, $\mathcal{A}$ can obtain m by executing $(m \| r \| V) = y \oplus H_1(X)$.

The basic reason about our attack works is that the blind factor $X = Y^s = e(g,g)^{\alpha \cdot s}$ is computed independent of the receiver's public key. Thus, any of the ring member can decrypt the ciphertext by computing the blinded factor using its own private key.

5 Conclusions

In this paper, we identified security flaws in Guo-Li-Fan's attribute-based ring signcryption scheme proposed in [9]. Our results showed that this signcryption scheme fails to provide unforgeability and confidentiality. Specifically, anyone can forge the valid ciphertext without the knowledge of the ring member's private key. On the other hand, any ring member can decrypt the ciphertext which should only be decrypted by the receiver. Furthermore, the basic reason about our attack has also been analyzed. We remark that it is still an open problem to construct a provably-secure and efficient attribute-based ring signcryption scheme.

Acknowledgments

The authors thank the editors and the anonymous referees for their valuable comments and suggestions. This work is partially supported by National Natural Science Foundation of China under Grant Nos. 61003230, 61370026, 61300191 and 61103206, the Fundamental Research Funds for the Central Universities under Grant No. ZYGX2013J073 and ZYGX2012J077, and the Applied Basic Research Program of Sichuan Province under Grant No. 2014JY0041.

References

[1] M. Barbosa and P. Farshim, "Identity-based ring signcryption schemes: Cryptographic primitives for preserving privacy and authenticity in the ubiquitous world," in *19th International Conference on Advanced Information Networking and Applications (AINA'05)*, pp. 649–654, Taipei, Taiwan, Mar. 2005.

[2] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, pp. 369–372, Tokyo, Japan, Mar. 2008.

[3] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *11th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'05)*, pp. 515–532, Chennai, India, Dec. 2005.

[4] X. Boyen, "Multipurpose identity-based signcryption: a swiss army knife for identity-based cryptography," in *Proceedings of Advances in Cryptology (CRYPTO'03)*, pp. 383–399, Santa Barbara, California, USA, Aug. 2003.

[5] H. Chen, Y. Li, and J. Ren, "A practical identity-based signcryption scheme," *International Journal of Network Security*, vol. 15, no. 6, pp. 484–489, 2013.

[6] L. Chen and J. M. Lee, "Improved identity-based signcryption," in *8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'05)*, pp. 362–379, Les Diablerets, Switzerland, Jan. 2005.

[7] L. Cheng and Q. Wen, "An improved certificateless signcryption in the standard model," *International Journal of Network Security*, vol. 17, no. 3, pp. 229-237, 2015.

[8] A. W. Dent and Y. Zheng, *Practical Signcryption*, Springer, 2010.

[9] Z. Guo, M. Li, and X. Fan, "Attribute-based ring signcryption scheme," *Security and Communication Networks*, vol. 6, no. 6, pp. 790–796, 2013.

[10] J. M. Lee and W. Mao, "Two birds one stone: signcryption using RSA," in *Proceedings of Topics in Cryptology (CT-RSA'03)*, LNCS, vol. 2612, pp. 211–226, Apr. 2003.

[11] D. J. Kwak, S. J. Moon, G. Wang, and R. H. Deng, "A secure extension of the kwakc-moon group signcryption scheme," *Computers & Security*, vol. 25, no. 6, pp. 435–444, 2006.

[12] F. Li, F. T. B. Muhaya, M. K. Khan, and T. Takagi, "Lattice-based signcryption," *Concurrency and Computation: Practice and Experience*, vol. 25, no. 14, pp. 2112–2122, 2013.

[13] F. Li, X. Xin, and Y. Hu, "A pairing-based signcryption scheme using self-certified public keys," *International Journal of Computers and Applications*, vol. 29, no. 3, pp. 278–282, 2007.

[14] F. Li, X. Xin, and Y. Hu, "Id-based signcryption scheme with (t, n) shared unsigncryption," *International Journal of Network Security*, vol. 3, no. 2, pp. 155–159, 2006.

[15] J. Li, X. Huang, M. Hong, and Y. Zhang, "Certificate-based signcryption with enhanced security features," *Computers and Mathematics with Applications*, vol. 64, no. 6, pp. 1587–1601, 2012.

[16] J. Li and K. Kim, "Attribute-based ring signatures," *Cryptology ePrint Archive*, 2008.

[17] H. Y. Lin, T. S. Wu, S. K. Huang, and Y. S. Yeh, "Efficient proxy signcryption scheme with provable cca and cma security," *Computers & Mathematics with Applications*, vol. 60, no. 7, pp. 1850–1858, 2010.

[18] C. Pan, S. Li, Q. Zhu, C. Wang, and M. Zhang, "Notes on proxy signcryption and multi-proxy signature schemes," *International Journal of Network Security*, vol. 17, no. 1, pp. 29-33, 2015

[19] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology (EUROCRYPT'05)*, pp. 457–473, Aarhus, Denmark, May 2005.

[20] R. Steinfeld and Y. Zheng, "A signcryption scheme based on integer factorization," in *Third International Workshop on Information Security (ISW'00)*, pp. 308–322, Wollongong, Australia, Dec. 2000.

[21] M. Toorani and A. A. B. Shirazi, "Cryptanalysis of an elliptic curve-based signcryption scheme," *International Journal of Network Security*, vol. 10, no. 1, pp. 51–56, 2010.

[22] H. Xiong, J. Hu, and Z. Chen, "Security flaw of an ecc-based signcryption scheme with anonymity," *International Journal of Network Security*, vol. 15, no. 4, pp. 317–320, 2013.

[23] Bo Yang, Y. Yu, F. Li, and Y. Sun, "Provably secure identity-based threshold unsigncryption scheme," in *4th International Conference on Autonomic and Trusted Computing (ATC'07)*, pp. 114–122, Hong Kong, China, July 2007.

[24] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost(encryption)," in *Proceedings of Advances in Cryptology (CRYPTO'97)*, pp. 165–179, Santa Barbara, California, USA, Aug. 1997.

[25] Y. Zheng and H. Imai, "How to construct efficient signcryption scheme on elliptic curves," *Information Processing Letters*, vol. 68, no. 5, pp. 277–233, 1998.

Hu Xiong is an associate professor at University of Electronic Science and Technology of China (UESTC). He received his Ph.D degree from UESTC in 2009. His research interests include: cryptographic protocol, and network security.

Ji Geng is a professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China. He received his Ph.D degree from UESTC in 2014. His research interests include:

information security and system software.

Zhiguang Qin is the dean and professor in the School of Computer Science and Engineering, UESTC. He received his PH.D. degree from UESTC in 1996. His research interests include: information security and computer network.

Guobin Zhu is an assistant professor at University of Electronic Science and Technology of China (UESTC). He received his Ph.D degree from UESTC in 2014. His research interests include: network security and applied cryptography.