Insecurity of a Certificate-free Ad Hoc Anonymous Authentication

Yan Xu[1], Liusheng Huang[2], Miaomiao Tian[2], and Hong Zhong[1]
(Corresponding author: Hong Zhong)

School of Computer Science and Technology, Anhui University[1]
Hefei 230027, China
School of Computer Science and Technology, University of Science and Technology of China[2]
Hefei 230601, China
(Email: xuyan@ahu.edu.cn)
(Received Apr. 14, 2015; revised and accepted July 30 & Nov. 27, 2015)

Abstract

The ring signature scheme is a simplified group signature scheme for no manager while preserving unconditionally anonymous of the signer. Certificateless cryptography is introduced for eliminating the use of certificates in Public Key Infrastructure and solving the key-escrow problem in ID-based cryptogratography. Recently, Qin et al. proposed the first RSA-based certificateless ring signature scheme which was proved unforgeable in random oracle model. In this paper, we demonstrated that this scheme was not secure against the Type I adversary.

Keywords: Certificateless cryptography, ring signature, RSA

1 Introduction

In 2001, Rivest et al. [11] formally introduced the concept of the ring signature in which the verifier can be convinced that the message was authenticated by a ring including the signer while keeping the signer unconditionally anonymous. Anonymity and spontaneity are inherent properties of the ring signature. Anonymity allows anyone to verify the validity of the ring signature without revealing the signer's identity. Spontaneity means that the signer can generate the ring signature without any help or cooperation from the other ring members. The ring signature allows the signer to decide all ring members. The ring signature scheme in [11] is based on RSA cryptosystem. Abe et al. [1] proposed the first ring signature scheme based on discrete logarithm problem. These ring signature schemes are all based on traditional Public Key Infrastructure which requires a great amount of computing time and storage to manage the certificates. In order to avoid the heavy burden of certificate management, Shamir [12] introduced Identity-based public key cryptography (ID-PKC). In 2002, Zhang et al. [16] proposed the first ID-based ring signature scheme. Nguyen [9] proposed the first ring signature with a constant number of pairing computations and a constant size signature. Au et al. [3] proposed the first secure ring signature scheme in standard model. Herranz [7] and Tsang et al. [14] respectively provided the ID-based ring signature schemes from RSA. However, ID-based cryptography usually suffers from the inherent key escrow problem.

In 2003, Al-Riyami and Paterson [2] introduced the concept of certificateless public key cryptography (CL-PKC) which not only avoids the key escrow problem but also moves the digital certificates. In CL-PKC, there is a third party called Key Generate Center (KGC) to issue the users partial private keys with their identities. However, the KGC has no right to access the full private key which is generated by combining the partial private key and a secret value chosen by the user itself. The public keys are computed by the secret value and then published by users. The CL-PKC has attracted a lot of further studies [6, 8, 13]. Yum et al. [15] proposed a general construction of certificateless signature (CLS) scheme which was a less efficient scheme. Zhang and Mao [17] designed the first RSA-based CLS scheme.

In 2007, two certificatelss ring signature (CL-RS) schemes [5, 18] were proposed independently. Chang et al. [4] constructed a more efficient (t,n) threshold ring signture scheme. The above CL-RS schemes are all based on bilinear pairings which is an expensive operation for the computational cost. Qin et al. [10] proposed the first RSA-based CL-RS scheme without bilinear parings and proved their scheme was secure in random oracle model. However, we found that Qin et al.'s scheme was vulnerable to a Type I adversary who can replace the public key of any signer.

2 Preliminaries

2.1 Security Model of the Certificateless Ring Signature Scheme

There are two kinds of adversaries in the security model of CL-RS scheme. Type I adversary $\mathcal{A}_1$ can replace the public key of any user at his will but is not able to visit the partial private key. Type II adversary $\mathcal{A}_2$ models the malicious-but-passive KGC who generates the partial private keys for users, but cannot replace any users' public keys. We define two games, **Game 1** for $\mathcal{A}_1$, and **Game 2** for $\mathcal{A}_2$.

- **Game 1**: Let S_1 be the challenger to interactive with $\mathcal{A}_1$
  1) **Initialization:** S_1 runs **Setup** and **MasterKeyGen** algorithms to get the system parameters *mpk* and the master key pair *msk*. Then S_1 publics *mpk* while keeping *msk* secret. S_1 maintains three lists L_1, L_2, L_3 initiated empty. (1) L_1 records the identities whose partial private keys have been required by $\mathcal{A}_1$ in **PartialKeyGen** queries. (2)L_2 records the identities whose public keys have been replaced by $\mathcal{A}_1$. (3) L_3 records the identities who have been corrupted by $\mathcal{A}_1$ in **Corruption** queries.
  2) **Query:** $\mathcal{A}_1$ adaptively performs a polynomially bounded number of queries.
     - **UserKeyGen:** On input a user's identity ID, if ID has not been created, S_1 run **UserKeyGen** to generate (upk_{ID}, usk_{ID}), upk_{ID} is returned.
     - **PartialKeyGen:** $\mathcal{A}_1$ requests the partial private key of the user *ID*. If $ID \notin L_1$, S_1 first sets $L_1 = L_1 \cup ID$ and then runs **PartialKeyGen**. Otherwise S_1 does nothing. Finally psk_{ID} is returned.
     - **ReplaceKey**: On input *ID* and upk^*_{ID}, if ID has been requested in **UserKeyGen**, S_1 first sets $L_2 = L_2 \cup ID$ and then updates the public key of ID as upk^*_{ID}. Otherwise nothing is carried out.
     - **Corruption**: $\mathcal{A}_1$ requests the full private key of the user with identity ID.
       a. If $ID \in L_2$, S_1 cannot output the full private key of ID whose public key is replaced, S_1 returns $\perp$.
       b. Otherwise, S_1 first sets $L_3 = L_3 \cup ID$, and then returns the partial private key psk_{ID} as well as the user secret value usk_{ID}.
     - **Ring-Sign:** On input a message m, a ring R containing the identities and the public keys of ring members, S_1 outputs a ring signature σ.
  3) **Forgery:** At the end of the simulation, $\mathcal{A}_1$ outputs (R^*, m^*, σ^*) as the forgery. We say that $\mathcal{A}_1$ wins the game:
     - (R^*, m^*) has never been required for the verification.
     - $Verify(R^*, m^*, \sigma^*) = 1$ and $(L^*_{ID} \cap L_1 \cap L_2) \cup (L^*_{ID} \cap L_3) = \emptyset$ for L^*_{ID} is the set of ring members' identities.

- **Game 2**: Let S_2 be the challenger to interactive with $\mathcal{A}_2$
  1) **Initialization:** As with the initialization of **Game 1**, except that S_2 sends the master key pair (mpk, msk) to $\mathcal{A}_2$. In **Game 2**, lists L_2, L_3 are maintained by S_2.
  2) **Query:** $\mathcal{A}_2$ makes the queries of **UserKeyGen**, **Corruption** and **Ring-Sign** in the same way as in **Game 1**.
  3) **Forgery:** At the end of the simulation, $\mathcal{A}_2$ outputs (R^*, m^*, σ^*) as the forgery. We say that $\mathcal{A}_2$ wins the game:
     - (R^*, m^*) has never been required for the verification $Verify(R^*, m^*, \sigma^*) = 1$
     - $L^*_{ID} \cap L_3 = \emptyset$ for L^*_{ID} is the set of ring members' identities.

Definition 1. (Unforgeability). *A CL-RS scheme is unforgeable if the advantage of any polynimail bounded adversary in the* ***Game 1*** *and* ***Game 2*** *is negligible.*

3 Cryptanalysis of Qin *et al.* CL-RS Scheme

3.1 The Qin *et al.* 's CL-RS Scheme

- **Setup:** On input 1^k as a security parameter, the KGC randomly selects two k-bit prime number p, q and computes $N = pq$. The KGC picks two prime numbers e, d satisfying $\gcd(e, \varphi(n)) = 1$ and $ed = 1 \bmod \varphi(n)$, where $\varphi(n)$ denotes the Euler totient function. Finally, the KGC chooses two hash functions H_1, H_2 which satisfy $H_1 : \{0,1\}^* \to Z^*_N$ and $H_2 : \{0,1\}^* \to \{0,1\}^l$. The KGC publishes the public parameters $mpk = \{N, e, H_1, H_2\}$ while keeping the master key $msk = \{p, q, d\}$ secret.

- **PartialKeyGen:** For the user with $ID \in \{0,1\}^*$, the KGC computes its partial private key $psk_{ID} = H_1(ID)^d$.

- **UserKeyGen:** The user ID selects $x_{ID} \in Z_{2^{|N|/2-1}}$ as its secret value usk_{ID} and sets its public key $upk_{ID} = H_1(ID)^{x_{ID}}$, where $|N|$ denotes the binary length of N.

- **Ring-Sign:** Let $R = L_{ID} \cup L_{upk}$, $L_{ID} = \{ID_1, \cdots, ID_n\}$ denotes the set of ring members' identities with the corresponding set of public keys $L_{upk} = \{upk_{ID1}, \cdots, upk_{IDn}\}$. To sign a message $m \in \{0,1\}^*$ on behalf of the ring, the signer ID_π performs the following steps by using its full private key $SK_{ID\pi} = (psk_{ID\pi}, usk_{ID\pi})$.
  - Selects two random numbers $r_{\pi 1}, r_{\pi 2} \in Z_{2^{|N|/2-1}}$.
  - Computes $R_{\pi 1} = H_1(ID_\pi)^{r_{\pi 1}} \bmod N, R_{\pi 2} = H_1(ID_\pi)^{r_{\pi 2}} \bmod N$.
  - Randomly chooses $u_{i1}, c_i \in Z_N^*, u_{i2} \in Z_{2^{|N|/2-1}}$ pairwise different, for $i \in [1,n], i \neq \pi$. Then ID_π computes $R_{i1} = u_{i1}^e H_1(ID_i)^{c_i} \bmod N, R_{i2} = H_1(ID_i)^{u_{i2}} upk_{IDi}^{c_i} \bmod N$.
  - Computes $c_0 = H_2(m||L_{ID}||L_{upk}||(R_{i1}, R_{i2})i \in [1,n])$.
  - Generates a polynomial f over $GF(2^k)$ with degree $n-1$ such that $c_0 = f(0), c_i = f(i)$ for $i \in [1,n], i \neq \pi$.
  - Computes $c_\pi = f(\pi)$, $u_{\pi 1} = (psk_{ID\pi})^{r_{\pi 1} - c_\pi} \bmod N$, $u_{\pi 2} = r_{\pi 2} - x_{ID\pi} c_\pi$.
  - Outputs the ring signature on message m as $\sigma = (m, f, (u_{i1}, u_{i2})i \in [1,n])$.
- **Verify:** Given a CL-RS $\sigma = (m, f, (u_{i1}, u_{i2})i \in [1,n])$ on message m, the verifier executes as follows:
  - Checks if f is a polynomial over $GF(2^k)$ with degree $n-1$.
  - Computes $c_i = f(i), R_{i1} = u_{i1}^e H_1(ID_i)^{c_i} \bmod N, R_{i2} = H_1(ID_i)^{u_{i2}} upk_{IDi}^{c_i} \bmod N$ for $i \in [1,n]$.
  - Accepts the signature if and only if the following equation holds $f(0) = H_2(m||L_{ID}||L_{upk}|| (R_{i1}, R_{i2})i \in [1,n])$.

3.2 Attack of Qin *et al.*'s CL-RS Scheme by TypeI Adversary

Qin *et al.* proved their scheme is secure against the two types of adversaries in CL-RS scheme. However, we found that the Type I adversary can forge the ring signature. $\mathcal{A}_1$ forges ID_π's signature as follows:

1) $r_{\pi 1}, r_{\pi 2}, R_{\pi 1}, R_{\pi 2}, \{c_i, u_{i1}, u_{i2}, R_{i1}, R_{i2}\}_{(i \in [1,n], i \neq \pi)}, f$ are generated as Qin *et al.*'s scheme.

2) $\mathcal{A}_1$ computes $c_\pi = f(\pi)$. If $r_{\pi 1} - c_\pi$ is not divided by e, $\mathcal{A}_1$ operates the step **Ring-Sign** of Qin *et al.*'s scheme.

3) If $r_{\pi 1} - c_\pi = eh$, $\mathcal{A}_1$ sets $u_{\pi 1} = H(ID_\pi)^h \bmod N$, $u_{\pi 2} = r_{\pi 2} - x'_{ID\pi} c_\pi$, $\sigma = (m, f, (u_{i1}, u_{i2})i \in [1,n])$ as the forged signature.

The forged signature can pass the verification:

$$
\begin{aligned}
R_{\pi 1} &= u_{\pi 1}^e H_1(ID_\pi)^{c_\pi} \\
&= H_1(ID_\pi)^{eh} H_1(ID_\pi)^{c_\pi} \\
&= H_1(ID_\pi)^{r_{\pi 1} - c_\pi} H_1(ID_\pi)^{c_\pi} \\
&= H_1(ID_\pi)^{r_{\pi 1}} \bmod N \\
R_{\pi 2} &= H_1(ID_\pi)^{u_{\pi 2}} (upk'_{ID\pi})^{c_\pi} \\
&= H_1(ID_\pi)^{r_{\pi 2} - x'_{ID\pi} c_\pi} H_1(ID_\pi)^{x'_{ID\pi} c_\pi} \\
&= H_1(ID_\pi)^{r_{\pi 2}} \bmod N \\
f(0) &= H_2(m||L_{ID}||L_{upk}||(R_{i1}, R_{i2})i \in [1,n])
\end{aligned}
$$

For the reason that $r_{\pi 1}$ is a random number, c_π is generated by polynomial f decided by random numbers $c_i (i \in [1,n], i \neq \pi)$ and hash function H_2 which could treated as a random number. The probability that $r_{\pi 1} - c_\pi$ dividing by e holds is $1/e$ which is no negligible. In conclusion, the Type I adversary can forge the CL-RS in a non-negligible probability.

4 Conclusion

Certificateless public key cryptography could eliminate the use of certificates in Public Key Infrastructure and solve the key-escrow problem in ID-based public key cryptography. Certificateless ring signature schemes can provide anonymous authentication for ad hoc networks. Recently, Qin et al. proposed a RSA-based CL-RS scheme which was proved unforgeable in random oracle model. However, we found that the scheme was not secure against the Type I adversary. In the future, we will design a more efficient CL-RS scheme without bilinear pairing. The novel scheme should be unforgeable in random oracle model.

Acknowledgements

This work is supposed by the National Nature Science Fundation of China (No.61173188, 61572001), China Postdoctoral Science Foundation (No.2015M570545), Anhui Provincial Natural Science Foundation (No.201508085QF132), the Educational Commission of Anhui Province, China(KJ2015A326), and the Open Project of Co-Innovation Center for Information Supply & Assurance Technology, Anhui University (No.ADXXBZ2014-9). All authors thank referees for their valuable suggestions.

References

[1] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in *Advances in Cryptology (Asiacrypt'02)*, pp. 415–432, Springer, 2002.

[2] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology (Asiacrypt'03)*, pp. 452–473, Springer, 2003.

[3] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, "ID-based ring signature scheme secure in the standard model," in *Advances in Information and Computer Security*, pp. 1–16, Springer, 2006.

[4] S. Chang, D. S. Wong, Y. Mu, and Z. Zhang, "Certificateless threshold ring signature," *Information Sciences*, vol. 179, no. 20, pp. 3685–3696, 2009.

[5] S. S. Chow and W. Yap, "Certificateless ring signatures," *IACR Cryptology ePrint Archive*, vol. 2007, pp. 236, 2007.

[6] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Systems Journal*, DOI: 10.1109/JSYST.2015.2428620, 2015.

[7] J. Herranz, "Identity-based ring signatures from rsa," *Theoretical Computer Science*, vol. 389, no. 1, pp. 100–117, 2007.

[8] S. Horng, S. Tzeng, P. Huang, and et al., "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Information Sciences*, vol. 317, no. 1, pp. 48–66, 2015.

[9] L. Nguyen, "Accumulators from bilinear pairings and applications," in *Topics in Cryptology (CT-RSA'05)*, pp. 275–292, Springer, 2005.

[10] Z. Qin, H. Xiong, G. Zhu, and Z. Chen, "Certificate-free ad hoc anonymous authentication," *Information Sciences*, vol. 268, pp. 447–457, 2014.

[11] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology (Asiacrypt'01)*, pp. 552–565, Springer, 2001.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, pp. 47–53, Springer, 1985.

[13] M. Tian, W. Yang, and L. Huang, "Cryptanalysis and improvement of a certificateless multi-proxy signature scheme," *Fundamenta Informaticae*, vol. 129, no. 4, pp. 365–375, 2014.

[14] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong, "A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity," in *Proceedings of 4th International Conference on Provable Security (ProvSec'10)*, LNCS 6402, pp. 166–183, Springer, 2010.

[15] D. H. Yum and P. J. Lee, "Generic construction of certificateless signature," in *Information Security and Privacy*, pp. 200–211, Springer, 2004.

[16] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in *Advances in Cryptology (Asiacrypt'02)*, pp. 533–547, Springer, 2002.

[17] J. Zhang and J. Mao, "An efficient rsa-based certificateless signature scheme," *Journal of Systems and Software*, vol. 85, no. 3, pp. 638–642, 2012.

[18] L. Zhang, F. Zhang, and W. Wu "A provably secure ring signature scheme in certificateless cryptography," in *Provable Security*, pp. 103–121, Springer, 2007.

Yan Xu received her Ph.D degrees from University of Science and Technology of China in 2015. She is a lecturer at Anhui University. Her research interests include digital signature, cryptography.

Liusheng Huang is currently a professor and Ph.D supervisor in School of Computer Science and Technology at University of Science and Technology of China. His research interests include information security, wireless sensor network and distributed computing. He is author or coauthor of more than 100 research papers and six books.

Miaomiao Tian received his Ph.D degrees from University of Science and Technology of China in 2014. He is a postdoctor at University of Science and Technology of China. His research interests include information security, cryptography, digital signature.

Hong Zhong received her Ph.D degrees from University of Science and Technology of China in 2005. She is a professor and Ph.D supervisor in School of Computer Science and Technology at Anhui University. Her research interests include information security, cryptography.