Universal Forgery on Shen et al.'s Linkable and Convertible ID-based Ring Signature Scheme

Shin-Jia Hwang
Department of Computer Science and Information Engineering,
Tamkang University, Tamsui, New Taipei City, 251, Taiwan, R.O.C.
Email: sjhwang@mail.tku.edu.tw

Abstract: Recently, Shen et al. proposes their ID-based ring signature scheme. Based on the scheme, they also propose their linkable and convertible ID-based ring signature scheme. However, a universal forgery is found for their ID-based ring signature scheme. Therefore, their linkable and convertible ID-based ring signature scheme is also insecure against universal forgeries.
Keywords: ID-based ring signature, convertible ring signatures, universal forgery

1 Introduction

Digital signature concept is first introduced by Diffie and Hellman [1]. Then Rivest et al. [2] proposed their digital signature scheme based factorization problem. Digital signature schemes should satisfy correctness, unforgeability, and nonrepudiation. Moreover, the digital signature on some message m can be verified by anyone using the public key of the signer. Therefore, verifiers have to know who the signer is. The signer's identity is not protected at all. However, the signer wishes to hide his/her identity but the signature is able to convince the verifier.

Ring signature schemes [3] are proposed to provide signer anonymity for the signers' identity privacy. In the ring signature scheme, the actual signer first randomly selects an ad hoc group as a ring. Then the actual signer generates the ring signature such that each ring member is also able to generate the ring signature. If the probability distributions of ring signatures generated by the ring members are the same, then the ring signature scheme is unconditionally signer anonymity.

Since the ring signature scheme provides signer anonymity protection for the actual signer, no one is convinced that the ring signatures are generated by the actual signer. To overcome this problem, the convertible ring signature schemes [4] provides a mechanism that the actual signer can transfer the ring signatures to ordinal signatures to show who the actual signer is. Moreover, the linkable ring signature schemes [5-7] just help the verifier being able to determine whether or not two ring signatures from the same ring are generated from the same unknown ring member.

Based on the concept of ID-based cryptosystems [8], many ID-based ring signature schemes [9-12] are proposed. In ID-based ring signature schemes, the actual signer only needs the identities of the ring members. It is convenient for the actual signer to generate ID-based ring signatures.

adfa, p. 1, 2011.

Recently, Shen et al. [13] proposed their linkable and convertible ID-based ring signature scheme. They announce that their schemes satisfies anonymity and unforgeability. Unfortunately, a universal forgery is found on their ID-based ring signature scheme, therefore, their linkable and convertible scheme is insecure against te universal forgery. In the following section, the universal forgery is presented after the review of Shen et al.' ID-based ring signature scheme.

2 Our Security Analysis on Shen et al.'s Linkable and Convertible ID-based Ring Signature Scheme

To propose their linkable and convertible ID-based ring signature scheme, Shen et al. [13] first proposed their ordinary ID-based ring signature scheme. This scheme is reviewed first, then our attack on the scheme is presented. In Shen et al.'s scheme, there is a trusted party, the key generator center (KGC), is responsible to generate the pubic system parameters and public functions. Any user U_i has to submit their identity ID_i to KGC for his/her registration. Then the user obtains his/her private key from the KGC through secure channels.

KGC first chooses a public prime number q and constructs a public bilinear pairing e: $G_1 \times G_1 \rightarrow G_2$, where $(G_1, +)$ is an addition group with the prime order q and $(G_2, \bullet)$ is a multiplication group with the prime order q. The bilinear pairing should satisfy three requirements:

Bilinearity: For any $P, Q, R \in G_1$, $e(P+Q, R)= e(P, R)e(Q, R)$ and $e(P, R+Q)= e(P, R)e(P, Q)$,

Non-degeneracy: There exist some $P, Q \in G_1$ such that $e(P, Q) \neq 1$, and

Efficient computation: There is some polynomial-time algorithm to perform the pairing function e [13].

Then KGC selects a public generator $P \in G_1$ and constructs two public hash functions $H_1:\{0, 1\}^* \rightarrow G_1$ and $H_2:\{0, 1\}^* \rightarrow Z_q^*= \{1, 2, 3, \ldots, q-1\}$. Then KGC randomly chooses its private key $x \in Z_q^*$ and computes its public key $P_{pub}= xP$.

For the registered user U_i with ID_i, KGC generates and securely sends his/her private key $S_i=xH_1(ID_i)$ to him/her. Then U_i's signature can be validated by using $H_1(ID_i)$.

Without losing generality, suppose that the signer U_0 wants to generate a ring signature on the message m. The signer U_0 performs the following procedure to generation ring signature on the message m with n randomly choosing ring members to protect who the actual signer is.

Step 1: Choose the ring members $U_1, U_2, U_3, \ldots,$ and, U_{n-1}.

Step 2: Choose a random secrete integer $t \in Z_q^*$ and $A \in G_1$, and compute $P'=tP$ and $c_{0+1}=H_2(L||m||e(A,P))$, where $L= (ID_0, ID_1, ID_2, \ldots, ID_{n-1})$.

Step 3: Select an random element $R_i \in G_1$ and compute $c_{i+1 \bmod n}= H_2(L||m||e(R_i,P)e(c_iH_1(ID_i), P_{pub}+P'))$ for i= 1, 2, 3, 4, …, n-1.

Step 4: Compute $R_0= A-c_0(S_0+tH_1(ID_0))$.

Then the ring signature on the message m is $\sigma=(P', c_0, (R_0, R_1, R_2,\ldots, R_{n-1})$.

To verify the ring signature $\sigma=(P', c_0, (R_0, R_1, R_2,\ldots, R_{n-1})$ on the message m, the verifier computes $c_{i+1 \bmod n}= H_2(L||m||e(R_i,P)e(c_iH_1(ID_i), P_{pub}+P'))$ for i= 0, 1, 2, …, n-1 and then checks whether or not the computed c_0 is equal to the given c_0 in the ring signature σ. If the computed and the given c_0 are the same, the ring signature is legal.

Our Universal Forgery

The forgery procedure shows that Shen et al.'s scheme is universally forgeable. Suppose that the forger wants to forge the ring signature on the message m for the ring $\{ID_0, ID_1, ID_2, \ldots, ID_{n-1}\}$, the forger performs the forgery procedure.

Step 1: Choose a random secrete integer $k\in Z_q^*$ and $A\in G_1$, and compute $P''= kP$ and $c_{0+1}=H_2(L||m||e(A,P))$, where $L= (ID_0, ID_1, ID_2, \ldots, ID_{n-1})$.

Step 2: Select an random element $R_i\in G_1$ and compute $c_{i+1 \bmod n}= H_2(L||m|| e(R_i,P)e(c_iH_1(ID_i), P''))$ for i= 1, 2, 3, 4, …, n-1.

Step 3: Compute $R_0= A-kc_0H_1(ID_0)$ and $P'= P''-P_{pub}$.

Then the forged ring signature on the message m is $\sigma= (P', c_0, (R_0, R_1, R_2,\ldots, R_{n-1})$ which passes the verification. It is easy to see that the $e(A,P)= e(R_0+ kc_0H_1(ID_0), P)= e(R_0, P)e(kc_0H_1(ID_0), P)= e(R_0, P)e(c_0H_1(ID_0), kP)= e(R_0, P)e(c_0H_1(ID_0), P'')= e(R_0, P)e(c_0H_1(ID_0), P_{pub}+P')$. It is also easy to find that $c_{i+1 \bmod n}= H_2(L||m|| e(R_i, P)e(c_iH_1(ID_i), P''))= H_2(L||m|| e(R_i,P)e(c_iH_1(ID_i), P_{pub}+P'))$ for i= 0, 1, 2, …, n-1.

Because our forgery can be applied on any message the forger wants, our forgery is a universal forgery. Moreover, our forgery needs no collection of signatures and message pairs, so our forgery is universal with known public key attacks.

3 Conclusions

Although Shen et al. proposed their efficient construction to propose ID-based ring signature schemes, their scheme is insecure against universal forgery. Moreover, Shen et al.'s linkable and convertible ID-based ring signature scheme is also universally forgeable with known public key attacks. Our future research is to find the way to overcome our forgery.

References

1. W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, pp. 644- 654, 1976.
2. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of ACM*, Vol. 21, No. 2, pp. 120-126, 1978.
3. Ronald L. Rivest, Adi Shamir, and Yael Tauman, "How to Leak a Secret," *Advances in Cryptology — ASIACRYPT 2001*, LNCS 2248, New York: Springer, 2001, pp 552-565.
4. K-C. Lee, H-A. Wen, and Tzonelih Hwang. "Convertible Ring Signature," *IEE Proceedings on Communications*, Vol. 152. No. 4. Pp. 411-414, 2005.

5. Joseph K. Liu, Victor K. Wei, and Duncan S. Wong, "Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract)," *Information Security and Privacy*, LNCS 3108, New York: Springer, 2004, pp 325-335.
6. Ik Rae Jeong, Jeong Ok Kwon, and Dong Hoon Lee, "Ring Signature with Weak Linkability and Its Applications," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 20, No. 8, pp. 1145-1148, 2008.
7. Eiichiro Fujisaki and Koutarou Suzuki, "*Traceable Ring Signatures*," IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol.E91-A No.1 pp.83-93, 2008.
8. Adi Shamir, "Identity-based Cryptosystem and Signature Scheme," *Advances in Cryptology —Proceedings of CRYPTO 84*, LNCS 196, New York: Springer, 1985, pp. 47-53.
9. Fangguo Zhang and Kwangjo Kim, "ID-Based Blind Signature and Ring Signature from Pairings," *Advances in Cryptology—ASIACRYPT 2002*, LNCS 2501, New York: Springer, 2002, pp. 533-547.
10. Javier Herranz and Germán Sáez, "New Identity-Based Ring Signature Schemes," *Information and Communications Security*, LNCS 3269, New York: Springer, 2004, pp. 27-39.
11. Sherman S. M. Chow, Siu-Ming Yiu, and Lucas C. K. Hui, "Efficient Identity Based Ring Signature," *Applied Cryptography and Network Security*, LNCS 3531, New York: Springer, 2005, pp. 499-512.
12. Jianhong Zhang, "An Efficient Identity-Based Ring Signature Scheme and Its Extension," Computational Science and Its Applications – ICCSA 2007, LNCS 4706, New York: Springer, 2007, pp. 63-74.
13. Xunxun Shen, Maozhi Xu, and Yanhui Zhao, "A Linkable and Convertible ID-based Ring Signature," 2011 International Conference on Computational and Information Sciences, Chengdu, Sichuan, China, Oct. 21 - 23, 2011, pp. 394-397.