Cryptanalysis of Ring Signature and Ring Signcryption Schemes

S. Sharmila Deva Selvi, S. Sree Vivek*, C. Pandu Rangan*

{sharmila,svivek,prangan}@cse.iitm.ac.in,
Indian Institute of Technology Madras
Theoretical Computer Science Laboratory
Department of Computer Science and Engineering
Chennai, India

Abstract. Ring signature and ring signcryption are cryptographic primitives, that allow an user to sign and signcrypt a message respectively without revealing their identity, i.e. the verifier or the unsigncrypter are convinced that the message is valid and authentic but is handicapped of knowing the identity of the actual signer or signcrypter. In this paper we consider two schemes, one is a ring signature scheme and the other one is a ring signcryption scheme. We demonstrate an attack to show that both of them lack anonymity.

[**Keywords:**] **Ring Signature, Ring Signcryption, Anonymity, Cryptanalysis, Bilinear Pairing.**

1 Introduction

Ring signature is a cryptographic primitive that enables an user to sign a message on behalf of a group of users without revealing his identity and without getting any acknowledgment from other users in the group. The group of users or the ring is formed by the signer in an arbitrary manner and even the other users may not be aware of the fact that they are being included in a ring. The verifier gets convinced that one of the ring members has signed the message, but he will not be able to identify the actual signer of the message. This primitive was first introduced by Rivest et al. in [8]. Due to its elegance and wide spread application ring signatures have attracted the research community widely. Since its introduction in 2001, a lot of schemes were proposed. Signcryption is another cryptographic primitive which offers authentication and confidentiality simultaneously with a very low cost than performing sign and encrypt independently on a message.
Ring signcryption was introduced to make it possible for an user to signcrypt a message and specify a set of possible signcryptors without revealing which

* Work supported by Project No. CSE/05-06/076/DITX/CPAN on Protocols for Secure Communication and Computation sponsored by Department of Information Technology, Government of India

member actually produced the signcryption. Thus a ring signcrypted message provides both authentication and confidentiality. Ring signatures (resp. signcryption) have no group managers, no setup procedure, no revocation procedures and no coordination: any user can choose any set of possible signers (resp.signcryptors) that includes himself and signs (resp.signcrypt) any message by using his secret key as well as other peoples public keys, without getting any approval or assistance from them. Ring signatures (resp.signcryption) is used to provide a graceful way to leak trustworthy secrets in an anonymous way.

In this paper, we demonstrate an attack on a ring signature scheme and a ring signcryption scheme and expose that they do not provide anonymity, which is the most desired property. The ring signature scheme is proposed by Chandana et.al in [4]. They have proposed an identity based ring signature scheme that has applications where the ad-hoc group size is small and all the members would disclose their private keys in a collusion attack. They have taken VANET (Vehicular Ad-hoc Networks) as the platform where the above conditions apply. The idea of the authors is to ring sign a message, that employs a designated verifier to verify it. Thus producing ambiguity between the actual signer and the designated verifier. We show that a person who gets a valid ring signature can identify the actual signer by performing some special test.

The second scheme is an identity based ring signcryption scheme proposed by Li et.al [6]. They claim their scheme is efficient, when compared to that of Huang et.al's [5] identity based ring signcryption scheme. Unfortunately, the change made by Li et.al to [5] did not help in improving the efficiency, instead it lost the anonymity of the signer. We also show this in our paper.

Definition 1. ***Bilinear Pairing***

Let $\mathbb{G}_1$ be an additive cyclic group generated by P, with prime order q, and $\mathbb{G}_2$ be a multiplicative cyclic group of the same order q. A bilinear pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following properties.

- ***Bilinearity.*** *For all $P, Q, R \in \mathbb{G}_1$,*
  - $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$
  - $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$
  - $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$
- ***Non-Degeneracy.*** *There exist $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq I_{\mathbb{G}_2}$, where $I_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$.*
- ***Computability.*** *There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}_1$.*

2 Identity Based Ring Signature Scheme of Chandana et al.[4]

2.1 Review of the Scheme

In 2006, Chandana et al. proposed an identity-based ring signature scheme. They claim their scheme provides enhanced security, i.e. it resists full key exposure attack. If the ring is very small all the ring members can collide and find the actual signer by exposing all their secret keys. They have extended the identity based ring signature scheme of Chow et al. [3]. We show that their extension makes the scheme insecure. Chandana et al.'s scheme consists of the following four algorithm.

Setup. Given a security parameter κ the PKG (Private Key Generator) chooses $\mathbb{G}_1$ an additive cyclic group, $\mathbb{G}_2$ a multiplicative cyclic group, $\hat{e}$ an admissible bilinear pairing given as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and chooses two hash functions $H : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. Chooses $x \in_R \mathbb{Z}_q^*$ as the master secret key and sets $P_{pub} = xP$ as the master public key, where P is a random generator of $\mathbb{G}_1$. The system parameters *params* are $(\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, P_{pub}, H, H_0)$.

KeyGen. The PKG computes the following for each user with identity ID_A.

- The user public key is computed as $Q_A = H(ID_A) \in \mathbb{G}_1$.
- The corresponding secret key $D_A = xQ_A$.
- The TA sends D_A to the user via a secure authenticated channel.

Sign. Let L=$\{ID_1$,ID_2,$\ldots$,$ID_n\}$ be the set of all identities of n users. The actual signer indexed by A (with public key Q_A and secret key D_A) carries out the following steps to generate an ID-based ring signature on behalf of the group L. The designated verifiers identity is ID_B.

- Choose $U_i \in_R \mathbb{G}_1$, compute h_i=$H_0(m\|L\|U_i)$ $\forall i \in \{1,2,..n\}\backslash\{A\}$.
- Choose $r'_A \in_R \mathbb{Z}_q^*$, compute $U_A = r'_A Q_A$-$\sum_{i=1,i\neq A}^{n}\{U_i + h_iQ_i\}$.
- Compute $W_A = \hat{e}(r'_A Q_B, S_A)$.
- Compute $W = r'_A Q_A$
- Compute $h_A = H_0(m\|L\|U_A\|W_A)$ and $V = (h_A$+$r'_A)D_A$.
- Output the signature on m as $\sigma = \{\bigcup_{i=1}^{n}\{U_i\}, V, W, L\}$.

Verify. Given a signature $\sigma = \{\bigcup_{i=1}^{n}\{U_i\}, V, W, L\}$ for the message m and a set of identities L, the designated verifier can check the validity of it as described below.

- The designated verifier computes the h_i value independently for each user U_i, as $h_i = H_0((m\|L\|U_i\|\hat{e}(W, S_B))$.
- Checks whether $\hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i + h_iQ_i)) \stackrel{?}{=} \hat{e}(P, V)$.
- If the above verification equality is satisfied for one of the identifiers ID_i, then the message has been correctly signed by the i^th member of the ordered set L and the verification step must return a value *true*.

2.2 Attack on Identity Based Ring Signature Scheme of Chandana et al. [4]

In the above scheme, the authors claim that only the designated verifier can verify the signature. Here too if the designated verifier exposes his secret key the actual signer is in trouble but the signature is ambiguous with respect to the signer and the designated verifier. But, the major weakness in the scheme is, anyone who gets the signature $\sigma = \{\bigcup_{i=1}^{n}\{U_i\}, V, W, L\}$, can identify the signer by performing the following steps.

- Compute $U' = \sum_{i=1}^{n} U_i - W$.
- Compute $H' = \sum_{i=1}^{n} H_0(m \| L \| U_i) Q_i$.
- Compute $H = U' + H'$.
- Check whether $H \overset{?}{=} H_0(m \| L \| U_i) Q_i$ for all value of i.
- If the check holds for some i then ID_i is the sender.

We provide the proof of correctness for this attack.
If ID_A is the actual sender, then

$$\begin{aligned} U' &= \sum_{i=1}^{n} U_i - W \\ &= \sum_{i=1, i \neq A}^{n} U_i + U_A - r'_A Q_A \end{aligned}$$

Substituting the value for U_A we get,

$$\begin{aligned} U' &= \sum_{i=1, i \neq A}^{n} U_i + r'_A Q_A - \sum_{i=1, i \neq A}^{n} \{U_i + h_i Q_i\} - r'_A Q_A \\ &= \sum_{i=1, i \neq A}^{n} U_i + r'_A Q_A - \sum_{i=1, i \neq A}^{n} U_i - \sum_{i=1, i \neq A}^{n} h_i Q_i\} - r'_A Q_A \\ &= - \sum_{i=1, i \neq A}^{n} h_i Q_i \end{aligned}$$

since, $H' = \sum_{i=1}^{n} H_0(m \| L \| U_i) Q_i$, we get

$$\begin{aligned} U' + H' &= - \sum_{i=1, i \neq A}^{n} h_i Q_i + \sum_{i=1}^{n} H_0(m \| L \| U_i) Q_i \\ &= H_0(m \| L \| U_A) Q_A \end{aligned}$$

Thus the actual signer A can be identified.
Note : In [2] Sherman Chow has claimed that [4] does not provide enhanced privacy, instead the privacy level is reduced. He has pointed out a trivial weakness which can be exploited, that the hash value computed by the actual signer A, while signing is $h_A = (m||L||U_A||W_A)$, which is constructed in a different way from the other hash values $h_i = H_0(m||L||U_i)$, where $i = \{1, 2, \ldots, n\} \backslash \{A\}$ and all h_i's can be computed by the knowledge of publicly available values. The attack proposed in [2] is to compute all h'_i's as $h'_i = H_0(m||L||U_i)$ for $i = \{1, 2, \ldots, n\}$ and if there exists a j such that $h'_j \neq h_j$, one can conclude that ID_j is the real signer, without using the private key of the designated verifier. Computing $h'{}_j$ is feasible but the other value h_j is not available in the signature (i.e. there is no reference value with which the computed value can be checked). So, it is not a trivial case to identify the actual signer as explained by Sherman Chow. Thus we argue that our's is the exact way to identify the signer in Chandana et.al.'s ring signature.

3 Identity Based Ring signcryption Scheme of Li et al.[6]

3.1 Review of the Scheme

Li et al., in [6] claims that their scheme is an efficient identity based ring signcryption scheme. Their scheme does not use pairing during the ring signcryption generation and uses only two pairing while unsigncrypting it. In-spite of these efficiency enhancements in [6], we show that their scheme is void of sender anonymity. The identity based ring signcryption in [6] consists of four algorithms namely: *Setup*, *Extract*, *Signcrypt* and *Unsigncrypt*, which we describe below.

Setup. Given a security parameter κ the PKG chooses $\mathbb{G}_1$ an additive cyclic group, $\mathbb{G}_2$ a multiplicative cyclic group, both of prime order q, $\hat{e}$ an admissible bilinear pairing given as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and chooses two hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^{n_1}$ and $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. Chooses $s \in_R \mathbb{Z}_q^*$ as the master secret key and sets $P_{pub} = sP$ as the master public key, where P is a random generator of $\mathbb{G}_1$. It also chooses a secure symmetric cipher (E, D). The system parameters *params* are $(\mathbb{G}_1, \mathbb{G}_2, n_1, \hat{e}, q, P, P_{pub}, E, D, H_1, H_2, H_3)$.

Extract. Given an identity ID_A, the PKG computes the following for the user.

- The user public key is computed as $Q_A = H_1(ID_A) \in \mathbb{G}_1$.
- The corresponding secret key $S_A = sQ_A$.
- The PKG sends S_A to the user via a secure authenticated channel.

Signcrypt. Let $\mathcal{U}$=$\{U_1$,U_2,...,$U_n\}$ be a set of n users. Let ID_i be U_i's identity. To signcrypt a message m to the receiver ID_B on behalf of the group $\mathcal{U}$, the actual signcrypter, indexed by A performs the following steps.

- Chooses $r_A \in_R \mathbb{Z}_q^*$ and computes $X = r_A Q_A$.
- Computes $k = H_2(\hat{e}(r_A S_A, Q_B)$.
- Computes $c = E_k(m)$.
- For all $i \in \{1, 2, \ldots, n\}$, $i \neq A$, chooses $a_i \in_R \mathbb{Z}_q^*$, computes $R_i = a_i P$ and h_i=$H_3(c \| \mathcal{U} \| R_i)$.
- Computes $R_A = X - \sum_{i=1, i \neq s}^{n} \{R_i + h_i Q_i\}$.
- Computes $h_A = H_3(c \| \mathcal{U} \| R_A)$ and $V = (h_A$+$r_A)S_A$.
- Output the cipher-text on m as $\sigma = \{\mathcal{U}, X, c, \bigcup_{i=1}^{n}\{R_i\}, V\}$.

Unsigncrypt. The receiver can unsigncrypt $\sigma = \{\mathcal{U}, X, c, \bigcup_{i=1}^{n}\{R_i\}, V\}$ as follows.

- Computes $k = H_2(\hat{e}(X, S_B))$.
- Recovers the message $m = D_k(c)$.
- Computes h_i=$H_0(c \| \mathcal{U} \| R_i)$ for all $i \in \{1, 2, ..n\}$.
- Checking whether $\hat{e}(P_{pub}, \sum_{i=1}^{n}(R_i + h_i Q_i)) \stackrel{?}{=} \hat{e}(P, V)$.
- Accept the message m if the above check is true, reject otherwise.

3.2 Attack on Identity Based Ring Signcryption Scheme of Li et al. [6]

We show that the ring signcryption scheme proposed by Li et al. in [6] does not provide anonymity. Any passive observer including the receiver, who is in possession of a ring signcryption can identify the sender in this scheme. The cipher-text produced by the scheme is $\sigma = \{\mathcal{U}, X, c, \bigcup_{i=1}^{n}\{R_i\}, V\}$. Anyone who has the cipher-text can do the following to identify the sender.

For all values of i ($i = 1$ to n) perform the following.

- Check whether $\hat{e}(V, P) \stackrel{?}{=} \hat{e}(h_i Q_i + X, sP)$, where h_i=$H_0(c \| \mathcal{U} \| R_i)$ (c, $\mathcal{U}$, R_i are taken from the cipher-text).

- If the check holds then ID_i is the sender.

We provide the proof of correctness for this attack.
If ID_i is the actual sender i.e, $i = A$ then

$$\begin{aligned}\hat{e}(h_iQ_i + X, sP) &= \hat{e}(h_AQ_A + r_AQ_A, sP)\\ &= \hat{e}((h_A + r_A)Q_A, sP)\\ &= \hat{e}((h_A + r_A)sQ_A, P)\\ &= \hat{e}((h_A + r_A)S_A, P).\\ &= \hat{e}(V, P)\end{aligned}$$

If ID_i is not the actual sender i.e, $i \neq A$ then

$$\begin{aligned}\hat{e}(h_iQ_i + X, sP) &= \hat{e}(h_iQ_i + r_AQ_A, sP)\\ &\neq \hat{e}(V, P)\end{aligned}$$

4 Conclusion

In this paper, we show the lack of anonymity in a ring signature schemes and a ring signcryption scheme, which is a key feature of both ring signature and ring signcryption. We conclude that, anonymity in ring signature and ring signcryption should not be established by the symmetric looks of the signed message with respect to the members of the ring or by probability arguments that they are all equally likely with probability 1/n. Anonymity should be treated rigorously using the definitions given in [7] and [1].

References

1. Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In *TCC*, volume 3876 of *Lecture Notes in Computer Science*, pages 60–79. Springer, 2006.
2. Sherman S. M. Chow. Blind signature and ring signature schemes: Rehabilitation and attack. In *Computer Standards & Interfaces*, doi:10.1016/j.csi.2008.09.002, 2008.
3. Sherman S. M. Chow, Siu-Ming Yiu, and Lucas Chi Kwong Hui. Efficient identity based ring signature. In *ACNS*, pages 499–512, 2005.
4. Chandana Gamage, Ben Gras, Bruno Crispo, and Andrew Tanenbaum. An identity-based ring signature scheme with enhanced privacy. In *Securecomm and Workshops 2006 - Journal*, pages 1–5, 2006.
5. Xinyi Huang, Willy Susilo, Yi Mu, and Futai Zhang. Identity-based ring signcryption schemes: Cryptographic primitives for preserving privacy and authenticity in the ubiquitous world. In *AINA*, pages 649–654, 2005.
6. Fagen Li, Hu Xiong, and Yong Yu. An efficient id-based ring signcryption scheme. In *International Conference on Communications, Circuits and Systems - 2008. ICCCAS 2008.*, pages 483–487. IEEE, 2008.
7. Miyako Ohkubo and Masayuki Abe. On the definition of anonymity for ring signatures. In *VIETCRYPT*, volume 4341 of *Lecture Notes in Computer Science*, pages 157–174. Springer, 2006.
8. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *ASIACRYPT*, pages 552–565, 2001.