Cryptanalysis of Ring Signature and Ring Signcryption Schemes

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

{svivek,sharmila,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 is 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 three schemes, the first one is a ring signature scheme and the second one is a ring signcryption scheme, we demonstrate attacks on them to show that, both schemes lack anonymity and the latter doesn't provide confidentiality. We also consider a secret authenticatable anonymous signcryption scheme with identity privacy as the third scheme in our paper, which is a ring signcryption scheme that allows the actual signcrypter to reveal his identity (if required in a dispute at a later point of time). We show that this scheme is void of indistinguishability because the ciphertext is distinguishable during the challenge phase of the confidentiality game.

[**Keywords:**] **Ring Signature, Ring Signcryption, Anonymity, Indistinguishability, Confidentiality, 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 signature and encryption sequentially on a message.

* 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

Ring signcryption was introduced to make it possible for an user to signcrypt a message and specify a set of possible signcrypters without revealing which 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. signcrypters) 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 attacks on a ring signature scheme and two ring signcryption schemes. The first scheme is a ring signature scheme which 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 review the scheme and show that a person who gets a valid ring signature can identify the actual signer by performing some special test in section 2.

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 of the scheme, instead it lost the anonymity of the signer. Also, as claimed by the authors the scheme does not provide insider security i.e, there is a weakness in the confidentiality of the scheme; we review the scheme and show these attacks in section 3.

The third scheme is an identity based secret authenticatable anonymous signcryption scheme with identity privacy proposed by Zhang et al. in [9]. This scheme is a variant of ring signcryption where the actual signer is capable of revealing his identity to the receiver of the ciphertext if required, in case of dispute. For achieving this property, the authors employ a zero knowledge interactive proof (ZKIP), where the actual signer interacts with the verifier to prove he is indeed the actual signer. This proof cannot be given by any of the possible signers in the ring because it involves the randomness used in the scheme during signcryption. In section 4, we provide the review of the scheme and show that this scheme is void of confidentiality because the ciphertext is distinguishable during the challenge phase of the confidentiality game.

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.*** *An efficient algorithm exists 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]

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 private keys. They have extended the identity based ring signature scheme of Chow et al. [3]. We show that their extension makes the scheme insecure.

2.1 Review of the Scheme

Chandana et al.'s identity-based ring signature scheme consists of a tuple of four algorithm, namely $Setup$, $KeyGen$, $Sign$ and $Verify$. Each of them is explained below.

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 private 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 does the following to generate the private/public key pair for each user U_i with identity ID_i.
- The user public key is computed as $Q_i = H(ID_i) \in \mathbb{G}_1$.
- The corresponding private key $D_i = xQ_i$.
- The PKG sends D_i to the user via a secure authenticated channel.

Sign. Let L=$\{ID_1$,ID_2,...,$ID_n\}$ be the set of all identities of n users. The actual signer indexed by ψ (with public key Q_ψ and private key D_ψ) 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.
- Chooses $R_i \in_R \mathbb{G}_1$, computes h_i=$H_0(m \| L \| R_i)$ $\forall i \in \{1, 2, ..n\} \backslash \{\psi\}$.
- Chooses $r_\psi \in_R \mathbb{Z}_q^*$, computes $R_\psi = r_\psi Q_\psi$-$\sum_{i=1, i \neq \psi}^{n} \{R_i + h_i Q_i\}$.
- Computes $W_\psi = \hat{e}(r_\psi Q_B, S_\psi)$.
- Computes $W = r_\psi Q_\psi$
- Computes $h_\psi = H_0(m \| L \| U_\psi \| W_\psi)$ and $V = (h_\psi + r_\psi) D_\psi$.
- Outputs the signature on m as $\sigma = \{\bigcup_{i=1}^{n} \{R_i\}, V, W, L\}$.

Verify. Given a signature $\sigma = \{\bigcup_{i=1}^{n} \{R_i\}, V, W, L\}$ 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 $h_i = H_0((m \| L \| R_i \| \hat{e}(W, S_B))$.
- Checks whether $\hat{e}(P_{pub}, \sum_{i=1}^{n} (R_i + h_i Q_i)) \stackrel{?}{=} \hat{e}(P, V)$.
- 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 private key the actual signer is in trouble but the signature is ambiguous with respect to the signer and the designated verifier. The major weakness in the scheme is, anyone who gets the signature $\sigma = \{\bigcup_{i=1}^{n}\{R_i\}, V, W, L\}$, can identify the signer by performing the following steps.

- Compute $R' = \sum_{i=1}^{n} R_i - W$.
- Compute $H' = \sum_{i=1}^{n} H_0(m\|L\|R_i)Q_i$.
- Compute $H = R' + H'$.
- Check whether $H \stackrel{?}{=} H_0(m\|L\|R_i)Q_i$ 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_ψ is the actual sender, then

$$\begin{aligned} R' &= \textstyle\sum_{i=1}^{n} R_i - W \\ &= \textstyle\sum_{i=1, i\neq\psi}^{n} R_i + R_\psi - r_\psi Q_\psi \end{aligned}$$

Substituting the value for R_ψ we get,

$$\begin{aligned} R' &= \textstyle\sum_{i=1, i\neq\psi}^{n} R_i + r_\psi Q_\psi - \sum_{i=1, i\neq\psi}^{n}\{R_i + h_i Q_i\} - r_\psi Q_\psi \\ &= \textstyle\sum_{i=1, i\neq\psi}^{n} R_i + r_\psi Q_\psi - \sum_{i=1, i\neq\psi}^{n} R_i - \sum_{i=1, i\neq\psi}^{n} h_i Q_i\} - r_\psi Q_\psi \\ &= -\textstyle\sum_{i=1, i\neq\psi}^{n} h_i Q_i \end{aligned}$$

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

$$\begin{aligned} R' + H' &= -\textstyle\sum_{i=1, i\neq\psi}^{n} h_i Q_i + \sum_{i=1}^{n} H_0(m\|L\|R_i)Q_i \\ &= H_0(m\|L\|R_\psi)Q_\psi \end{aligned}$$

Thus the actual signer ψ 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 ψ, while signing is $h_\psi = (m||L||R_\psi||W_\psi)$, which is constructed in a different way from the other hash values $h_i = H_0(m||L||R_i)$, where $i = \{1, 2, \ldots, n\}\backslash\{\psi\}$ and all h_i's can be computed with the knowledge of publicly available values. The attack proposed in [2] is to compute all h'_i's as $h'_i = H_0(m||L||R_i)$ 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 ours 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 three 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 private 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 private/public key pair for the user A.

- The user public key is computed as $Q_A = H_1(ID_A) \in \mathbb{G}_1$.
- The corresponding private 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 ψ performs the following steps.

- Chooses $r_\psi \in_R \mathbb{Z}_q^*$ and computes $X = r_\psi Q_\psi$.
- Computes $k = H_2(\hat{e}(r_\psi S_\psi, Q_B)$.
- Computes $c = E_k(m)$.
- For all $i \in \{1, 2, \ldots, n\}$, $i \neq \psi$, 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 $R_\psi = X - \sum_{i=1, i\neq\psi}^{n} \{R_i + h_i Q_i\}$.
- Computes $h_\psi = H_3(c \| \mathcal{U} \| R_\psi)$ and $V = (h_\psi + r_\psi) S_\psi$.
- 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 Attacks on the Identity Based Ring Signcryption Scheme of Li et al. [6]

This section demonstrates two different attacks on [6], one is on the anonymity of the ring signcryption and the other one is on the confidentiality of the ciphertext.

***Attack on Anonymity*:** 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 for some value of i then ID_i is the sender.

The proof of correctness for this attack is given below.
If ID_i is the actual sender i.e, $i = \psi$ then

$$\begin{aligned}\hat{e}(h_i Q_i + X, sP) &= \hat{e}(h_\psi Q_\psi + r_\psi Q_\psi, sP) \\ &= \hat{e}((h_\psi + r_\psi)Q_\psi, sP) \\ &= \hat{e}((h_\psi + r_\psi)sQ_\psi, P) \\ &= \hat{e}((h_\psi + r_\psi)S_\psi, P). \\ &= \hat{e}(V, P)\end{aligned}$$

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

$$\begin{aligned}\hat{e}(h_i Q_i + X, sP) &= \hat{e}(h_i Q_i + r_\psi Q_\psi, sP) \\ &\neq \hat{e}(V, P)\end{aligned}$$

***Attack on Confidentiality*:** As per the security model of [6], in the game to prove confidentiality, the adversary $\mathcal{A}$ is given access to the secret key of all the users, except the target identity ID_B. Now, $\mathcal{A}$ can compute the value $k = \hat{e}(V, Q_B)\hat{e}(S_\psi, h_\psi Q_B)^{-1}$, since he can identify the sender ID_ψ as given in the above attack, he has the sender secret key S_i and can decrypt the ciphertext $\sigma^* = \{\mathcal{U}, X, c^*, \bigcup_{i=1}^{n}\{R_i\}, V\}$ as $m = D_k(c^*)$. Thus, $\mathcal{A}$ can find whether σ^* is a signcryption of m_0 or m_1 with out solving any hard problem, hence breaking the confidentiality.

Even if $\mathcal{A}$ does not know the sender, he can decrypt the ciphertext, since he knows the secret key of all the users except the targeted identity ID_B, who is the receiver. $\mathcal{A}$ does the following to decrypt the challenge ciphertext $\sigma^* = \{\mathcal{U}, X, c^*, \bigcup_{i=1}^{n}\{R_i\}, V\}$:

- Finds the value of k with all the secret keys of the identities in the ring, one by one as $k_i = \hat{e}(V, Q_B)\hat{e}(S_i, h_i Q_B)^{-1}$, where $i = 1$ to n (it is to be noted that all h_i values are publicly computable).
- Tries to decrypt with each values of k_i as $m' = D_{k_i}(c^*)$.
- Since $\mathcal{A}$ knows the messages m_0 and m_1 he can identify whether $m' = m_0$ or m_1.

Thus, breaking the confidentiality of the scheme.

4 Identity Based Secret Authenticatable Anonymous Signcryption Scheme with Identity Privacy of Zhang et al.[9]

In [9], Zhang et al. proposed an identity based secret authenticatable anonymous signcryption scheme. The novelty they have projected in their scheme is a message can be signcrypted by a sender ID_A in such a way that the receiver ID_B can authenticate the ciphertext as generated from a member of the group but cannot identify the actual signcrypter. In case of a dispute, the actual signcrypter ID_A can prove that the ciphertext is generated by himself but others in the group who are considered to be potential signers cannot authenticate it. They have proved the security of the scheme in a formal model under recently studied computational assumptions in the random oracle model. They claim that, compared to the schemes in recent literature, their scheme provides higher efficiency and security than others with the same order of ciphertext size. In this section, we show that their scheme lacks confidentiality.

4.1 Review of the Scheme

The identity based secret authenticatable anonymous signcryption scheme as proposed in [9] has five algorithms namely *Setup*, *Extract*, *Signcrypt*, *Unsigncrypt* and *Authenticate*. All these algorithms are explained below.

Setup: Given security parameters k and l, the Private Key Generator(PKG) selects an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where the order of $\mathbb{G}_1$ and $\mathbb{G}_2$ is p. Let P be a generator of $\mathbb{G}_1$. It also chooses $s \in \mathbb{Z}_q^*$ as the master private key and computes $P_{pub} = sP$ as the corresponding master public key. It also chooses some secure hash functions: $H_0 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$, $H_1 : G2 \rightarrow \{0,1\}^l$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. The system public parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub}, H_0, H_1, H_2\}$.

Extract: For an user U_i identified by ID_i, the PKG computes user public key $Q_i = H_0(ID_i)$ and corresponding private key $D_i = sQ_i$ where s is the PKG's master private key. Then PKG sends D_i to U_i via a secure and authenticated channel.

Signcrypt: Let $\bigcup\{U_i\}$ $(i = 1, \ldots, n)$ be a set of users including the actual signcrypter ψ (identified by ID_ψ). To signcrypt a message m on behalf of the group $\bigcup\{U_i\}$ to receiver B (identified by ID_B, public key $Q_B = H_0(ID_B)$), the actual signcrypter indexed by ψ (i.e. its public/private key is (Q_ψ, D_ψ)), carries out the following:

- Chooses $r \in_R Z_q^*$ and computes $R = rP$, $R' = \hat{e}(P_{pub}, Q_B)^r$, $t = H_1(R')$, $c = m \oplus t$.
- For $i = 1, 2, \ldots, n$, $i \neq \psi$, chooses $a_i \in_R Z_q^*$ to compute $T_i = a_i P$ and computes $h_i = H_2(m, \bigcup\{U_i\}, t, T_i)$.
- Chooses $a_\psi \in_R Z_q^*$ and computes $T_\psi = a_\psi Q_\psi - \sum_{i=1, i\neq\psi}^{n}\{T_i + h_i Q_i\}$.
- Computes $h_\psi = H_2(m, \bigcup\{U_i\}, t, T_\psi)$ and $\sigma = (h_\psi + a_\psi)D_\psi$.
- Finally, outputs the ciphertext of message m as $C = (\bigcup\{U_i\}, c, R, h_1, h_2, \ldots, h_n, T_1, T_2, \ldots, T_n, \sigma)$.

Unsigncrypt: On receiving the ciphertext $C = (\bigcup\{U_i\}, c, R, h_1, h_2, \ldots, h_n, T_1, T_2, \ldots, T_n, \sigma)$, the receiver B uses his private key D_B to unsigncrypt the ciphertext as follows:

- Computes $t' = H_1(\hat{e}(R, D_B))$ and $m' = c \oplus t'$.
- For $i = 1$ to n, checks whether $h_i \stackrel{?}{=} H_2(m', \bigcup\{U_i\}, t', T_i)$.

– Checks whether $\hat{e}(P_{pub}, \sum_{i=1}^{n}(T_i + h_i Q_i)) \stackrel{?}{=} \hat{e}(P, \sigma)$.

For all $i \in \{1, 2, \ldots, n\}$ and $h_i = H_2(m', \bigcup\{U_i\}, t', T_i)$, if $\hat{e}(P_{pub}, \sum_{i=1}^{n}(T_i + h_i Q_i)) \stackrel{?}{=} \hat{e}(P, \sigma)$ then, m' is a valid message else output $\perp$.

Authenticate: If the actual signcrypter ID_ψ wants to give the verifier a proof that the ciphertext C was indeed produced by himself, he uses the following interactive zero-knowledge proof:

- ID_ψ chooses $x \in_R \mathbb{Z}_q^*$ and computes $\mu = \hat{e}(P, \sigma)^x$ and sends μ to the verifier.
- The verifier chooses $y \in_R \mathbb{Z}_q^*$ and sends it back to ID_ψ.
- ID_S computes $v = (x + y)(h_\psi + a_\psi)$ and sends v to the verifier.
- Finally, the verifier checks whether $\hat{e}(P_{pub}, Q_\psi)^v \stackrel{?}{=} \mu.\hat{e}(P, \sigma)^y$. If the above equality holds, the verifier shows that the ID_ψ is the actual signcrypter, otherwise it returns $\perp$.

4.2 Attack on Zhang et al. [9]

In this section, we show that the identity based secret authenticatable anonymous signcryption scheme of Zhang et al. fails in the indistinguishability game. In the challenge phase, the adversary $\mathcal{A}$ supplies the challenger $\mathcal{C}$ with two messages m_0 and m_1. $\mathcal{C}$ tosses a coin and takes the random output $b \in \{0, 1\}$ and signcrypts the message m_b and sends the challenge ciphertext C^* to $\mathcal{A}$. If the adversary is capable of distinguishing whether C^* is a ciphertext corresponding to m_0 or m_1, the confidentiality of the scheme is disproved.

The attack on indistinguishability said above holds good for [9] and hence we claim that the identity based secret authenticatable anonymous signcryption scheme fails in the challenge phase of the indistinguishability game. Next we show, how this attack is mounted on the scheme. The adversary $\mathcal{A}$ knows both the messages m_0, m_1 and the challenge ciphertext $C^* = (\bigcup\{U_i\}, c^*, R^*, h_1^*, h_2^*, \ldots, h_n^*, T_1^*, T_2^*, \ldots, T_n^*, \sigma^*)$, $\mathcal{A}$ does the following to distinguish C^*.

- Computes $t_0^* = m_0 \oplus c^*$.
- Computes all h_i^*'s as $h_i^* = H_2(m_0, \bigcup\{U_i\}, t^*, T_i^*)$, for $(i = 1$ to $n)$.
- Verifies $\hat{e}(\sigma^*, P) \stackrel{?}{=} \hat{e}(\sum_{i=1}^{n}(h_i^* Q_i + T_i^*), P_{pub}$.
- If the above verification holds, then C^* is a valid ciphertext of m_0, otherwise, $\mathcal{A}$ performs all the above steps with the message replaced with m_1.

One of the above verifications should hold because the ciphertext C^* is a valid signcryption of either m_0 or m_1.

Remark 1: It is to be noted that the weakness identified in the scheme is significant even though it can be fixed by simple measures. This attack is possible because $\mathcal{A}$ can compute h_i values and relate it to the corresponding message. As a consequence, a possible fix for the bug identified may be including the value $R^{'}$ in the hash functions, i.e compute $h_i = H_2(m, \bigcup\{U_i\}, t, T_i, R')$ for $(i = 1$ to $n)$ during signcryption as well as unsigncryption. The significance of including $R^{'}$ is, only the receiver can compute h_i's because computation of $R^{'}$ involves the secret key of the targeted user who is the receiver.

5 Conclusion

In this paper, we showed 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]. Also, we have showed that the second scheme is not insider secure as claimed by the authors. The third scheme which we considered is an identity based secret authenticatable anonymous signcryption scheme with identity privacy. This scheme does not provide ciphertext indistinguishability which is also another important feature of signcryption schemes. We also suggest a possible fix for the weakness in the scheme.

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.
9. Mingwu Zhang, Bo Yang, Shenglin Zhu, and Wenzheng Zhang. Efficient secret authenticatable anonymous signcryption scheme with identity privacy. In *ISI Workshops*, volume 5075 of *Lecture Notes in Computer Science*, pages 126–137. Springer, 2008.