ON THE SECURITY OF TWO RING SIGNCRYPTION SCHEMES

S. Sree Vivek*, S. Sharmila Deva Selvi and C. Pandu Rangan*
Theorectical Computer Science Lab, Department of Computer Science
Indian Institute of Technology Madras, Chennai-600036, India

Keywords: Identity-based, Ring signcryption, Bilinear pairing, Cryptanalysis.

Abstract: Ring signcryption is a cryptographic primitive, that allows an user to send a message in confidential, authentic and anonymous way, i.e. the recipient of the message is convinced that the message is valid and it comes from one of the ring member, but does not know the actual sender. In this paper, we show attacks on ring signcryption schemes by Li et al. (Li et al., 2008b) and Chung et al. (Chung et al., 2006). We demonstrate anonymity and confidentiality attack on the scheme by Li et al. (Li et al., 2008b) and confidentiality attack on the scheme by Chung et al. (Chung et al., 2006).

1 INTRODUCTION

Ring signature is a cryptographic primitive that enables an user to sign a message in an anonymous way by forming a ring(group) of users. The user forms the ring without getting any acceptance or acknowledgment from the users included in the ring. The verifier of the ring signature will get convinced that the signature is generated by one of the ring members without knowing which ring member has actually generated the signature. This primitive was first introduced by Rivest et al. (Rivest et al., 2001). Due to its elegance and wide spread application, ring signatures have widely attracted the research community. Since its introduction in 2001, a lot of ring signature schemes were proposed (Rivest et al., 2001) (Abe et al., 2002) (Zhang and Kim, 2002) (Herranz and Sáez, 2004) (Bender et al., 2006).

Message security and sender authentication for communication in the open channel is an essential and important requirement. A technique for answering such a requirement was proposed by Yulien Zheng in 1997 (Zheng, 1997). The solution given by Zheng achieves confidentiality and authentication in single logical step called signcryption. After the development of signcryption primitive, a number of efficient signcryption schemes were proposed in literature till date.

*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

In scenarios where a user want to communicate a message confidentially with sender authentication and without disclosing his identity, ring signcryption is a good solution which achieves this functionality in an efficient way. Ring signcryption is a primitive which offers the services provided by both ring signature and signcryption. A number of ring signcryption schemes (Huang et al., 2005) (Yu Fang Chung, 2008) (Wang et al., 2007) (Yu et al., 2008) (Zhang et al., 2008)(Li et al., 2008b) (Li et al., 2008a) (Zhun and Zhang, 2008) (Zhang et al., 2009) were proposed in the recent past.

In this paper, we show the security weaknesses in the identity-based ring signcryption scheme by Li et al. (Li et al., 2008b) and the PKI based ring signcryption scheme by Chun et al. (Chung et al., 2006). First, we review Li et al. scheme (Li et al., 2008b) in section 3.1. Next, We show the attack on confidentiality of Li et al.'s scheme in section 3.2.2 and the attack on anonymity of Li et al.'s scheme in section 3.2.1. Then, we review Chung et al.'s scheme in section 4.1. Also, we demonstrate the attack on anonymity of Chung et al.'s scheme in section 4.2.

Bilinear Pairing. Since both the schemes are based on bilinear pairing, we review the basis of 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 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 $P, Q, R \in \mathbb{G}_1$,

Sree Vivek S., Deva Selvi S. and Rangan C. (2009).
ON THE SECURITY OF TWO RING SIGNCRYPTION SCHEMES.
In *Proceedings of the International Conference on Security and Cryptography*, pages 219-224
DOI: 10.5220/0002205702190224

- $\hat{e}(P+Q,R) = \hat{e}(P,R)\hat{e}(Q,R)$
- $\hat{e}(P,Q+R) = \hat{e}(P,Q)\hat{e}(P,R)$
- $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$

- ***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 SIGNCRYPTION SCHEME (IBRSS)

2.1 Generic Scheme

A generic identity-based ring signcryption scheme consists of the following four algorithms.
Let $\mathcal{U}$ be the set of ring members and $U_\psi \in \mathcal{U}$ be the actual sender.

- ***Setup(*κ*).*** Given a security parameter κ, the private key generator (*PKG*) uses this algorithm to generate the master private key *Msk* and system public parameters *params*. Here the *params* are made public to the user and *Msk* is kept secret by the *PKG*.
- ***Extract(*ID_i*).*** Given an identity ID_i by user U_i to PKG, the PKG uses this algorithm to generate the corresponding private key S_i. *PKG* sends the private key S_i to ID_i through a secure channel.
- ***Signcrypt(*$m, \mathcal{U}=\{ID_1,\ldots,ID_n\}, ID_\psi, S_\psi, ID_B$*)*** . On input of a message $m \in \mathcal{M}$, a set of ring members $\mathcal{U}$, the identity of the actual sender ID_ψ, the private key S_ψ of the actual sender ID_ψ, the receiver identity ID_B to this algorithm by the actual sender ID_ψ, this algorithm outputs the ring signcryption σ of message m from $\mathcal{U}$ to U_B.
- ***Unsigncrypt(*$\sigma, \mathcal{U}, ID_B, S_B$*).*** On providing the ring signcryption σ, the set of ring members $\mathcal{U}$, the receiver identity ID_B and the private key of the receiver S_B as input to this algorithm by ID_B, the *Unsigncrypt* algorithm recovers the plaintext m, if σ is a valid signcryption of m from $\mathcal{U}$ to ID_B and outputs m to the user with identity ID_B. Else, the algorithm outputs "*INVALID*".

We further assume that the validity of the consistency constraint that, if $\sigma = Signcrypt(m, \mathcal{U}, ID_\psi, S_\psi, ID_B)$, then $m = Unsigncrypt\ (\sigma, ID_B, S_B)$.

2.2 Security Model

In this section we formally define the security model for identity-based ring signcryption scheme.

Confidentiality:

An identity-based ring signcryption (IBRSS) is indistinguishable against adaptive chosen ciphertext attack (IND-IBRSS-CCA2) if there exists no polynomially bounded adversary that has non-negligible advantage in the following game:

1. ***Setup Phase.*** The challenger $\mathcal{C}$ runs the *Setup* algorithm with the security parameter κ and sends the system parameters *params* to the adversary $\mathcal{A}$ and keeps the master private key *Msk* secret. $\mathcal{A}$ chooses a target identity ID_T and gives ID_T to $\mathcal{C}$. It is assumed that $\mathcal{A}$ never queries the *KeyExtractOracle* for the private key of ID_T during the entire confidentiality game.
2. ***First Phase.*** During the *FirstPhase* of training $\mathcal{A}$ makes polynomially bounded number of requests to the oracles controlled by $\mathcal{C}$. The description of the oracles and the responses provided by the oracles in the first phase are listed below:
   - ***Key Extract Oracle.*** $\mathcal{A}$ submits an identity ID_i to $\mathcal{C}$ and requests the private key of ID_i. $\mathcal{C}$ returns the private key S_i of ID_i to $\mathcal{A}$.
   - ***Signcrypt Oracle.*** $\mathcal{A}$ submits a message m, a set of ring members $\mathcal{U}$, the actual sender $ID_\psi \in \mathcal{U}$, a receiver identity ID_B to $\mathcal{C}$. $\mathcal{C}$ generates σ, the ring signcryption of m from $\mathcal{U}$ to ID_B and returns σ to $\mathcal{A}$.
   - ***Unsigncrypt Oracle.*** $\mathcal{A}$ produces a ring signcryption σ, the set of ring members $\mathcal{U}$, a receiver identity ID_B to $\mathcal{C}$. The challenger $\mathcal{C}$ retrieves the private key $S_B = Keygen(ID_B)$ and recovers m from σ and checks whether σ is a valid ring signcryption of m from $\mathcal{U}$ to ID_B. If σ is valid then $\mathcal{C}$ returns m to $\mathcal{A}$. Else, $\mathcal{C}$ returns "*INVALID*" to $\mathcal{A}$.

   $\mathcal{A}$ adaptively queries all the above oracles, i.e. the current oracle requests may depend on the responses obtained from the previous oracle queries.
3. ***Challenge.*** $\mathcal{A}$ chooses two plaintext $\{m_0, m_1\} \in \mathcal{M}$, a set of n ring members $\mathcal{U}$ and the target receiver identity ID_T(chosen by $\mathcal{A}$ during the *SetupPhase* on which $\mathcal{A}$ wants to be challenged) and give this to $\mathcal{C}$. $\mathcal{C}$ now chooses a bit $b \in_R \{0,1\}$ and computes the challenge ring signcryption σ^* of m_b from $\mathcal{U}$ to ID_T. $\mathcal{C}$ sends σ to $\mathcal{A}$.

4. ***Second Phase.*** $\mathcal{A}$ performs polynomially bounded number of oracle queries as in *FirstPhase*, with the restrictions that,
   - $\mathcal{A}$ cannot make *KeyExtract* query for any user in the ring $\mathcal{U}$.
   - $\mathcal{A}$ cannot make *KeyExtract* query for ID_T.
   - $\mathcal{A}$ should not query for *Unsigncrypt* oracle with $(\sigma^*, \mathcal{U}, ID_T)$ as input.
5. ***Guess.*** Finally, $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$. The success probability of $\mathcal{A}$ is defined as,

$$Succ_{\mathcal{A}}^{IND-IBRSS-CCA2}(\kappa) = \frac{1}{2} + \varepsilon$$

We require that ε to be negligible with respect to κ and ε is called the advantage for the adversary in the attack.

Unforgeability:

An identity-based ring signcryption scheme (IBRSS) is said to be existentially unforgeable against adaptive chosen messages attacks (EUF-IBRSS-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game:

1. ***Setup Phase.*** The challenger $\mathcal{C}$ runs the *Setup* algorithm with a security parameter κ and generates the system parameters *params* and the master private key *Msk*. $\mathcal{C}$ gives the system parameters to the adversary $\mathcal{A}$ and keeps *Msk* secret. $\mathcal{A}$ then chooses a set of ring members $\mathcal{U}_T = \{U_1, U_2, \ldots, U_{n^*}\}$ and gives $\mathcal{U}_T$ to $\mathcal{C}$. It should be noted that $\mathcal{A}$ is not allowed to query the private key of ring members $\mathcal{U}_T$.
2. ***Training Phase.*** After the *SetupPhase*, $\mathcal{A}$ performs a polynomially bounded number of oracle queries as in *FirstPhase* of section 2.2. The queries may be adaptive, i.e. the current query may depend on the responses to the previous oracle queries.
3. ***Forgery.*** After getting sufficient training from $\mathcal{C}$, $\mathcal{A}$ produces new $(\sigma, \mathcal{U}, ID_B)$ (i.e. σ was not produced by the signcryption oracle), where the private key of ID_B) was not queried in the *TrainingPhase*. $\mathcal{A}$ wins the game if the result of the *Unsigncrypt* $(\sigma, \mathcal{U}, ID_B)$ is some message m and σ is a valid signcryption of $m \in \mathcal{M}$ from the ring $\mathcal{U}_T$ to ID_B.

3 LI ET AL. RING SIGNCRYPTION SCHEME (Li et al., 2008b) (LRSS)

3.1 Review of the Scheme

Li et al. given an efficient identity-based ring signcryption scheme in (Li et al., 2008b). This scheme does not use any pairing computation in ring signcryption generation and uses only two pairing for ring unsigncryption. This scheme is identity-based and it comprises of four algorithms namely: *LRSS.Setup*, *LRSS.Extract*, *LRSS.Signcrypt* and *LRSS.Unsigncrypt*, which we describe below.

- ***LRSS.Setup.*** The setup algorithm is run by the PKG. Given a security parameter κ as input, this algorithm performs the following,
  - Chooses $\mathbb{G}_1$ an additive cyclic group, $\mathbb{G}_2$ a multiplicative cyclic group, both of the same prime order q, $\hat{e}$ an admissible bilinear pairing given by $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Defines 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 master private key $s \in_R \mathbb{Z}_q^*(Msk = s)$ and sets master public key $P_{pub} = sP$, where P is a generator of $\mathbb{G}_1$. Also, chooses a secure symmetric cipher (E, D). The system parameters *params* are $(\mathbb{G}_1, \mathbb{G}_2, n_1, \hat{e}, q, P, P_{pub}, E, D, H_1, H_2, H_3)$.
- ***LRSS.Extract.*** The PKG on getting the identity of any user ID_A as input, computes the private/public key pair $\langle Q_A, S_A \rangle$ as,
  - Public key $Q_A = H_1(ID_A) \in \mathbb{G}_1$.
  - private key $S_A = sQ_A$.
  - PKG sends S_A to the user through secure channel.
- ***LRSS.Signcrypt.*** User ID_ψ for generating a ring signcryption provides the message m, the set of ring members $\mathcal{U}$=$\{U_1, U_2, \ldots, U_n\}$, the identity of the actual sender $ID_\psi \in \mathcal{U}$, the private key S_i of ID_ψ and the receiver identity ID_B as input to the *LRSS.Signcrypt* algorithm. This algorithms generates a valid ring signcryption on m with ring members $\mathcal{U}$ as senders and ID_B as receiver. This is done by performing,
  - 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 $V = (h_\psi + r_\psi)S_\psi$.
– Finally, the *LRSS.Signcrypt* algorithm output the ring signcryption $\sigma = \{\mathcal{U}, X, c, \bigcup_{i=1}^{n}\{R_i\}, V\}$ to ID_ψ.

- ***LRSS.Unsigncrypt.*** For unsigncrypting any ring signcryption $\sigma = \{\mathcal{U}, X, c, \bigcup_{i=1}^{n}\{R_i\}, V\}$ from ID_ψ to ID_B, the receiver ID_B provides the ring signcryption σ, the receiver identity ID_B, private key $\S_B$ of receiver ID_B as input to *LRSS.Unsigncrypt* algorithm. Unsigncryption is carried out by doing the computations given below:
  – 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 $\hat{e}(P_{pub}, \sum_{i=1}^{n}(R_i + h_i Q_i)) \stackrel{?}{=} \hat{e}(P, V)$.
  – Returns the message m if σ is a valid signcryption on message m from ID_ψ to ID_B. Else, return "*INVALID*".

3.2 Attacks on the Identity-based Ring Signcryption Scheme LRSS

This section demonstrates two different attacks on (Li et al., 2008b). The first attack is on the anonymity of the and is given in section 3.2.1. The second attack is on the confidentiality the scheme and the details are given in 3.2.2.

3.2.1 Attack on Anonymity

We show that the ring signcryption scheme *LRSS* 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. This can be demonstrated as follows, Let m be any message and $\sigma = \{\mathcal{U} = \{ID_1, ID_2, \ldots, ID_n\}, X, c, \bigcup_{i=1}^{n}\{R_i\}, V\}$ be the ring signcryption on m from the ring $\mathcal{U}$ to ID_B and $ID_\psi \in \mathcal{U}$ be the actual sender. On seeing the ring signcryption σ anyone can do the following operations to identify the actual sender $ID_\psi \in \mathcal{U}$. It is to be noted that the private key of any $ID_i \in \mathcal{U}$ or ID_B is not required during this computation.

Anyone can do the following to identify the actual signer in the ring. For all values of i ($i = 1$ to n) perform the following.

$h_i = H_3(c\|\mathcal{U}\|R_i)$, ($c$, $\mathcal{U}$, R_i are taken from the cipher-text).

Check whether $\hat{e}(V, P) \stackrel{?}{=} \hat{e}(h_i Q_i + X, sP)$. (1)

If the check holds for some value of i then ID_i is the actual sender.

The following *Lemma* 1 and *Lemma* 2 will prove that the test given above (equation (1)) is valid.

Lemma 1. *Let $\mathcal{H}_\psi = X + h_\psi Q_\psi$ where U_ψ is the actual signer. Let $R' = \hat{e}(V, P)$, then $R' = \hat{e}(\mathcal{H}_\psi, P_{pub})$.*
Proof.

$$\begin{aligned}\mathcal{H}_\psi &= X + h_\psi Q_\psi \\ &= (r_\psi + h_\psi)Q_\psi \text{ and} \\ R' &= \hat{e}(V, P) \\ &= \hat{e}((r_\psi + h_\psi)S_\psi, P) \\ &= \hat{e}((r_\psi + h_\psi)Q_\psi, P_{pub}) \\ &= \hat{e}(\mathcal{H}_\psi, P_{pub}\end{aligned}$$

Lemma 2. *Let $\mathcal{H}_i = X + h_i Q_i$ where $U_i \in U$ is the not the actual signer. Let $R' = \hat{e}(V, P)$, then $R' \neq \hat{e}(\mathcal{H}_i, P_{pub})$.*
Proof.

$$\begin{aligned}H_\imath &= X + h_i Q_i \\ &= r_\psi Q_\psi + h_i Q_i \text{ and} \\ R' &= \hat{e}(V, P) \\ &= \hat{e}((r_\psi + h_\psi)S_\psi, P) \\ &= \hat{e}((r_\psi + h_\psi)Q_\psi, P_{pub}) \\ &\neq \mathcal{H}_i\end{aligned}$$

From *Lemma* 1 and *Lemma* 2 it is clear that $R' = \mathcal{H}_i$ iff $i = \psi$.

3.2.2 Attack on Confidentiality

The LRSS is not CCA2 secure. As per the security model of (Li et al., 2008b), during the *Challenge Phase* of confidentiality game, the adversary $\mathcal{A}$ provides two messages m_0 and m_1 and a set of ring members $\mathcal{U} = \{ID_1, ID_2, \ldots, ID_n\}$ including the actual sender ID_ψ to $\mathcal{C}$(Note that $\mathcal{A}$ does not know the actual sender ID_ψ). $\mathcal{C}$ selects randomly a bit b and builds the challenge ring signcryption $\sigma = \{\mathcal{U}, X, c, \bigcup_{i=1}^{n}\{R_i\}, V\}$ on message m_b from the ring $\mathcal{U}$ to ID_T. $\mathcal{A}$ is given access to the secret key of all users, except the target receiver ID_T and members of the ring $\mathcal{U}$. Now, $\mathcal{A}$ can perform the following,

- Set $X^* = X$ and $c^* = c$.
- Form a new ring $\mathcal{U}^* = \{U_1, U_2 \ldots, U_t\}$ with the property $\mathcal{U}^* \nsubseteq \mathcal{U}$ and also $\mathcal{A}$ knows the secret key of at least one U_j, $j \in \{1, 2, \ldots, t\}$. Let U_{ψ^*} be a user from ring $\mathcal{U}^*$, for which $\mathcal{A}$ knows the private key.
- For all $j \in \{1, 2, \ldots, t\}$, $j \neq \psi^*$, $\mathcal{A}$ chooses $a_j \in_R \mathbb{Z}_q^*$, computes $R_j = a_j P$ and h_j=$H_3(c\|\mathcal{U}\|R_j)$.

- Chooses a random $r_{\psi^*} \in \mathbb{Z}_q^*$ and computes $R_{\psi^*} = r_{\psi^*}Q_{\psi^*} - \sum_{j=1,2,j\neq\psi^*}^{n}\{R_j + h_jQ_j\}$.
- Computes $h_{\psi^*} = H_3(c\|\mathcal{U}\|R_\psi)$ and $V* = (h_{\psi^*}+r_{\psi^*})S_{\psi^*}$.
- Sets $\sigma^* = \{\mathcal{U}^*, X^*, c^*, \bigcup_{j=1}^{t}\{R_j\}, V^*\}$.
- σ^* is entirely different from the challenge signcryption σ and hence $\mathcal{A}$ can request the *Unsigncrypt* oracle for the unsigncryption of σ^* as if σ^* is a signcryption of m_b from ring $\mathcal{U}^*$ to receiver ID_T.

The challenger will correctly respond with m_b.

Hence, $\mathcal{A}$ can exactly find whether σ is a signcryption of m_0 or m_1 without solving any hard problem. Thus, breaking the confidentiality of the Li et al.'s identity-based ring signcryption scheme.

Correctness of σ^*:

$$\begin{aligned}\hat{e}(P_{pub}, \textstyle\sum_{j=1}^{t}(R_j + h_jQ_j)) &= \hat{e}((r_{\psi^*} + h_{\psi^*})Q_{\psi*}, P_{pub}) \\ &= \hat{e}((r_{\psi^*} + h_{\psi^*})S_{\psi*}, P) \\ &= \hat{e}(V^*, P)\end{aligned}$$

4 CHUNG ET AL.'S ANONYMOUS SIGNCRYPTION SCHEME (CAS)

In this section, we review the anonymous signcryption scheme given by Chung et al. (Chung et al., 2006) and demonstrate an attack on confidentiality of the scheme in (Chung et al., 2006).

4.1 Review of the Scheme

Let q denote a large prime number, E denote an elliptic curve, P denote a base point on the elliptic curve E with order q and H denote a dispersed row function with collision resistance, where q, E, P and H are public parameters, and $\mathbb{Z}_q$ is a finite field with q elements. Let $\mathcal{U}$ be the ring formed by $(U_1, U_2, \ldots, U_n)$, the private keys of $U_1, U_2, \ldots, U_n$ are $d_1, d_2, \ldots, d_n$ respectively. The corresponding public keys $Q_1, Q_2, \ldots, Q_n$ satisfies $Q_i = d_iP$, where $i = 1, 2, \ldots, n$. The private and public keys of verifier U_v are d_v and $Q_v = d_vP$ respectively.

CAS.Signcrypt: For sending a ring signcryption on a message m, from a ring $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ with $U_\psi \in \mathcal{U}$ as actual sender and U_v as receiver, U_ψ performs the following,

- Randomly selects $r, k \in_R [1, q-1]$
- Calculates $(x_\psi, y_\psi) = T_i = kP$, $(x_r, y_r) = R = rP$, and $(x_e, y_e) = T_e = rQ_v$.
- When $t = 1$ and $t - 1 = n$, let $t = \psi + 1, \psi + 2, \ldots, n, 1, \ldots, \psi - 1$, select $s_t \in_R [1, q-1]$ and compute $c_t = H(m||x_{t-1})$ and $(x_t, y_t) = T_t = s_tP + c_tQ_t$.
- Compute $c_\psi = H(m\|x_{\psi-1})$ and $s_\psi = k - d_\psi c_\psi (mod q)$.
- $m' = E_{x_e}(m)$, here x_e acts as a symmetric key.
- sends the encrypted text $\sigma = (m', c_1, s_1, s_2, \ldots, s_n, R)$ to the verifier U_v.

CAS.Unsigncrypt: On receiving a ring signcryption $\sigma = (m', c_1, s_1, s_2, \ldots, s_n, R)$, the receiver U_v to unsigncrypt σ uses his secret key d_v and perform the following computations,

- Let (x_r, y_r) = R, calculates $(x_d, y_d) = d_vR$ and $m''= E_{x_d}(m')$.
- Let $t = 1, 2, \ldots, n-1$, calculate $(x_t, y_t) = T_t = s_tP + c_tQ_t$ and $c_{t+1} = H(m''\|x_t)$.
- Verifier U_v calculates $(x_n, y_n) = T_n = s_nP + c_nQ_n$ and $c_1' = H(m''\|x_n)$.
- If $c_1' = c_1$ then $\sigma = (m', c_1, s_1, s_2, \ldots, s_n, R)$ is a valid anonymous signcryption from the group $\mathcal{U} = (U_1, U_2, \ldots, U_n)$; otherwise, return "*INVALID*".

4.2 Attack on Chung et al. Scheme (CAS)

In this section we demonstrate the attack on confidentiality of Chung et al. Scheme (Chung et al., 2006).

4.2.1 Attack on Confidentiality

The anonymous signcryption scheme CAS is not CCA2 secure. The attack on confidentiality is also similar to the attack proposed in 3.2.2. During the challenge phase of the confidentiality game of the ring signcryption scheme, the adversary $\mathcal{A}$ provides two messages m_0 and m_1, receiver U_v and a set of ring members $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ including the actual sender U_ψ to $\mathcal{C}$. $\mathcal{C}$ selects randomly a bit b and generates the challenge ring signcryption $\sigma = (m', c_1, s_1, s_2, \ldots, s_n, R)$ on message m_b. Here, $\mathcal{A}$ does not know the private key of the target user U_v and the private key of the ring members $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$. $\mathcal{A}$ generates a valid signcryption σ^* with a new set of ring member $\mathcal{U}^* = \{U_1, U_2, \ldots, U_t\}$ from the challenge signcryption σ as given below,

- Let $U_{\psi^*} \in \mathcal{U}^*$ be the actual sender and $\mathcal{A}$ knows the private key d_{ψ^*} corresponding to U_{ψ^*}.
- Sets $R^* = R$ and $(x_e^*, y_e^*) = T_e^* = T_e$.
- Calculates $(x_{\psi^*}, y_{\psi^*}) = T_i = k^*P$, where $k^* \in_R [1, q-1]$.

- When $j = 1$ and $j-1 = n$, let $j = \psi^* + 1, \psi^* + 2, \ldots, t, 1, \ldots, \psi^* - 1$, select $s_j^* \in_R [1, q-1]$ and compute $c_j^* = H(m_0 || x_{j-1}^*)$ and $(x_j^*, y_j^*) = T_j^* = s_j P + c_j Q_j$.
- Compute $c_{\psi^*} = H(m \| x_{\psi^*-1})$ and $s_{\psi^*} = k^* - d_{\psi^*} c_{\psi^*} (mod q)$.
- $m^* = m' = E_{x_e}(m_b)$.
- sends $\sigma^* = (m^*, c_1^*, s_1^*, s_2^*, \ldots, s_t^*, R^*)$ to the *Unsigncrypt* oracle with U_v as receiver.
- *Unsigncrypt* oracle returns m_0 if σ is a valid signcryption on m_0. In other words, if $m^* = m'$ is the encryption of m_0 then the signature generated as part of σ^* by $\mathcal{A}$ with m_0 is a valid signature and hence σ^* is a valid signcryption from $\mathcal{U}^*$ to receiver U_v . Else, m' is the encryption of m_1. Hence, if the output of *Unsigncrypt* oracle is m_0 if σ^* is a valid signcryption of m_0. Otherwise, $\mathcal{A}$ returns "INVALID". Thus $\mathcal{A}$ can distinguish whether σ is the signcryption of m_0 or m_1 without knowing the private key of the receiver U_v. Thus, breaking the confidentiality of Chung et al. scheme.

5 CONCLUSIONS

In this paper we have showed attacks on confidentiality and anonymity of Li et al.'s identity-based ring signcryption scheme. Also, we have showed the attack on confidentiality of Chung et al.'s anonymous signcryption scheme.

REFERENCES

Abe, M., Ohkubo, M., and Suzuki, K. (2002). 1-out-of-n signatures from a variety of keys. In *ASIACRYPT '02: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security*, pages 415–432, London, UK. Springer-Verlag.

Bender, A., Katz, J., and Morselli, R. (2006). Ring signatures: Stronger definitions, and constructions without random oracles. In *TCC 06*, volume 3876 of *Lecture Notes in Computer Science*, pages 60–79. Springer.

Chung, Y.-F., Wu, Z. Y., Lai, F., and Chen, T.-S. (2006). Anonymous signcryption in ring signature scheme over elliptic curve cryptosystem. In *JCIS 06*. Atlantis Press.

Herranz, J. and Sáez, G. (2004). New identity-based ring signature schemes. In *ICICS*, volume 3269 of *Lecture Notes in Computer Science*, pages 27–39. Springer.

Huang, X., Susilo, W., Mu, Y., and Zhang, F. (2005). Identity-based ring signcryption schemes: Cryptographic primitives for preserving privacy and authenticity in the ubiquitous world. In *AINA '05*, pages 649–654.

Li, F., Shirase, M., and Takagi, T. (2008a). Analysis and improvement of authenticatable ring signcryption scheme. In *ProvSec '08*.

Li, F., Xiong, H., and Yu, Y. (2008b). An efficient id-based ring signcryption scheme. In *International Conference on Communications, Circuits and Systems - 2008. ICCCAS 2008.*, pages 483–487. IEEE.

Rivest, R. L., Shamir, A., and Tauman, Y. (2001). How to leak a secret. In *ASIACRYPT '01*, pages 552–565.

Wang, L., Zhang, G., and Ma, C. (2007). A secure ring signcryption scheme for private and anonymous communication. In *NPC '07: Proceedings of the 2007 IFIP International Conference on Network and Parallel Computing Workshops*, pages 107–111, Washington, DC, USA. IEEE Computer Society.

Yu, Y., Li, F., Xu, C., and Sun, Y. (2008). An efficient identity-based anonymous signcryption scheme. *Wuhan University Journal of Natural Sciences*, Volume: 13, Number: 6, December, 2008:670–674.

Yu Fang Chung, Zhen Yu Wu, T. S. C. (2008). Ring signature scheme for ecc-based anonymous signcryption. In *Computer Standards & Interfaces Journal*.

Zhang, F. and Kim, K. (2002). Id-based blind signature and ring signature from pairings. In *ASIACRYPT '02: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security*, pages 533–547, London, UK. Springer-Verlag.

Zhang, J., Gao, S., Chen, H., and Geng, Q. (2009). A novel id-based anonymous signcryption scheme. In *APWeb/WAIM '09*, volume 5446 of *Lecture Notes in Computer Science*, pages 604–610. Springer.

Zhang, M., Yang, B., Zhu, S., and Zhang, W. (2008). Efficient secret authenticatable anonymous signcryption scheme with identity privacy. In *PAISI, PACCF and SOCO '08: Proceedings of the IEEE ISI 2008 PAISI, PACCF, and SOCO international workshops on Intelligence and Security Informatics*, pages 126–137. Springer-Verlag.

Zheng, Y. (1997). Digital signcryption or how to achieve cost(signature & encryption) $<<$ cost(signature) + cost(encryption). In *CRYPTO '97*, pages 165–179.

Zhun, L. and Zhang, F. (2008). Efficient idbased ring signature and ring signcryption schemes. In *International Conference on Computational Intelligence and Security, 2008. CIS '08.*, volume 2, pages 303–307.