Analysis and Improvements of Two Identity Based Anonymous Signcryption Schemes for Multiple Receivers

Huaqun Wang[1,2], Yuqing Zhang[3], Bo Qin [2]
1.School of Information Engineering, Dalian Ocean University, Dalian, China;
2.Universitat Rovira i Virgili, Dept. of Comp. Eng. and Maths
UNESCO Chair in Data Privacy, Tarragona, Catalonia;
3. National Computer Network Intrusion Protection Center, GUCAS, Beijing, China;
wanghuaqun8@gmail.com

***Abstract*—Anonymous signcryption provides anonymity of the sender with the advantages of signcryption. When a sender wants to send a message to multiple receivers in the confidential and authenticated way, multi receiver signcryption is needed. In 2010, Zhang et al. proposed an identity based anonymous signcryption scheme for multiple receivers which is proved secure in the standard model. At the same time, Lal et al. designed another identity based anonymous signcryption scheme for multiple receivers in the random oracle model. Unfortunately, we show that the two schemes do not satisfy the semantic security. Then we improve their corresponding anonymous signcryption schemes that remedy the weaknesses of the above two schemes. Our proposed schemes satisfy the semantic security, unforgeability, signcrypter identity's ambiguity, and public authenticity.**

***Keywords*-signcryption; multi-receiver; cryptanalysis; anonymity**

I. INTRODUCTION

In 1997, the concept of digital signcryption was proposed by Zheng [1]. This cryptographic primitive can perform signature and encryption simultaneously at a lower computational costs and communication overheads. It's efficient than the signature-then-encryption approach. After that, many efficient signcryption schemes and security models were presented [2], [3], [4]. Signcryption can be applied in the fields that demand high speed and low communication overload. In 2002, Baek et al. proposed a sound security model for signcryption that admits rigorous formal proofs for the confidentiality and unforgeability of signcryption [3].

Anonymous signcryption or ring signcryption is a novel cryptographic primitive motivated from ring signature [4]. It is an important cryptographic model that can realize the signcrypter identities' ambiguity. The receiver in an anonymous signcryption scheme only knows that the message is produced by one member of a designated group, but he cannot know more information about the actual signcrypter's identity. Some identity-based ring signcryption schemes have been proposed [5], [6], [7], [8]. The concept of multi-receiver setting was first formalized by Bellare et al. [9]. Duan et al. consider the situation where there are not only multiple receivers but also multiple senders [10]. Regretful, Tan showed that Duan et al.'s scheme is in fact not secure against adaptive chosen ciphertext attacks under their defined security model in 2008 [11]. In 2009, Lal et al. proposed the first anonymous identity based signcryption scheme for multiple receivers in the random oracle model [12]. In 2010, Zhang et al. designed another identity based anonymous signcryption scheme for multiple receivers which was proved secure in the standard model [13]. We denote "identity based anonymous signcryption scheme for multiple receivers" as IASMR for short in this paper.

Cryptanalysis is the art of defeating cryptographic security systems, and gaining access to the contents of encrypted messages, without being given the cryptographic key. Through cryptanalysis, we find that both Zhang et al.'s scheme [13] and Lal et al.'s scheme [12] are insecure. Our analysis show that these two IASMR schemes do not satisfy the semantic security. To make up for these flaws, two improved IASMR schemes are also proposed in this paper. The analysis shows that the two improved IASMR schemes are secure.

The rest of the paper is organized as follows. In section II, we give preliminaries and security requirements. In section IV, we describe both Zhang et al.'s IASMR scheme and Lal et al.'s IASMR scheme. Then, the corresponding attack methods are also presented in this section. In section IV, we improve Zhang et al.'s IASMR scheme and give its security analysis. In section V, we improve Lal et al.'s IASMR scheme and give its security analysis. Finally, we conclude this paper in section VI.

II. PRELIMINARIES AND SECURITY REQUIREMENTS

Bilinear pairings and some difficult assumptions are given as the preliminaries. Then, we present the formal definition and the security requirements of IASMR scheme. IASMR scheme.

A. Preliminaries

Let $\mathcal{G}$ and $\mathcal{G}_T$ be two (multiplicative) cyclic groups with the same prime order p. Let $e : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_T$ is a bilinear map with the following properties:

(1) Bilinearity: For all $u, v \in \mathcal{G}$ and $a, b \in \mathcal{Z}_p^*$, $e(u^a, v^b) = e(u, v)^{ab}$;

(2) Non-degeneracy: There exists $g \in \mathcal{G}$, such that $e(g, g) \neq 1$;

(3) Computability: It is efficient to compute $e(u, v)$ for all $u, v \in \mathcal{G}$.

Then, we give the difficult problems on $\mathcal{G}_1$ and $\mathcal{G}_2$ as follows.

Definition 1 Definition 1(Discrete Logarithm Problem (DLP)) Given $(g, g^a) \in \mathcal{G}^2$ where g is a generator of $\mathcal{G}$, the DLP problem is to compute a from g^a.

Definition 2(Computational Diffie-Hellman Problem (CDH)). Given $(g, g^a, g^b) \in \mathcal{G}^3$ where g is a generator of $\mathcal{G}$, the CDH problem is to compute g^{ab}.

Definition 3(Decision Bilinear Diffie-Hellman problem (DBDH)). Given $(g, g^a, g^b, g^c, Z) \in \mathcal{G}^4 \times \mathcal{G}_T$, the DBDH problem is to decide whether $Z \stackrel{?}{=} e(g, g)^{abc}$ holds.

We choose the group $\mathcal{G}$ and $\mathcal{G}_T$ that satisfy that DLP, CDH and $DBDH$ are difficult.

Let H be a hash function $H : \{0,1\}^* \rightarrow \{0,1\}^n$. We say that algorithm $\mathcal{A}$ has advantage ϵ in breaking the collision-resistance of H if

$$Pr[A = (m_0, m_1) : m_0 \neq m_1, H(m_0) = H(m_1)] \geq \epsilon$$

where the probability is over the random bits of $\mathcal{A}$.

Definition 4(Collision-Resistant Hashing). A hash family H is (t, ϵ)-collision-resistant if no t-time adversary has advantage at least ϵ in breaking the collision-resistance of H.

In practice, of course, one would use a standard hash function such as SHA-256 and assume that it is collision-resistant.

B. Security requirements

First, we give the formal definition of IASMR scheme as follows.

Definition 5 (IASMR scheme) [12] An IASMR scheme consists of the following algorithms:

1) Setup. Given a security parameter k, key generation center (KGC) runs this algorithm to generate the master secret key S and system public parameter $params$ which includes the system public key.
2) Extract. Given the identity ID_i, KGC runs this algorithm to generate its private key d_i.
3) Signcrypt. A user ID_s runs this algorithm to send a message m to n receivers with identities $ID_{1'}, ID_{2'}, \cdots, ID_{n'}$ which includes the actual signcrypter identity ID_s. Finally, ID_s outputs the ciphertext C.
4) Unsigncrypt. Upon receiving the ciphertext C, the receiver ID_r runs this algorithm to recover m if the message was properly signcrypted, otherwise rejected.

Second, a secure IASMR scheme must satisfy the properties: signcrypter identity's ambiguity, semantic security and unforgeability.

Definition 6(Signcrypter identity's ambiguity). An IASMR scheme is unconditionally anonymous if for any group of n members with identities in the signer list L, the probability to identify the actual signcrypter is not more than random guess, *i.e.*, the adversary outputs the identity of actual signcrypter with probability $\frac{1}{n}$ if he is not a member of L, and with probability $\frac{1}{n-1}$ if he is a member of L.

Definition 7 (Semantic security) An IASMR scheme satisfies the property of indistinguishability against adaptive chosen ciphertext attack (IND-IASMR-CCA2) if no polynomially bounded adversary has a non-negligible advantage in the following game.

1) Setup. The challenger $\mathcal{C}$ runs the Setup algorithm with a security parameter k and obtains public parameters $param$ and a master secret key S. He sends $params$ to the adversary and keeps S secret.
2) First Stage. The adversary $\mathcal{A}$ performs a polynomially bounded number of queries. These queries may be made adaptively, *i.e.*, each query may depend on the answers to the previous queries.
   a) Extract queries. The adversary requests the private key of an identity ID_u and receives the extracted private key $d_u = Extract(ID_u)$.
   b) Signcryption queries. The adversary produces a signer list $L = \{ID_1, \cdots, ID_n\}$, a receiver list $L' = \{ID'_1, \cdots, ID'_{n'}\}$ and a plaintext m (Note that the adversary should not have asked the private key that corresponds to the identities in the receiver list L'). $\mathcal{C}$ computes $d_i = Extract(ID_i)$ $(i \in \{1, \cdots, n\})$ and $\sigma = Signcrypt(m, d_i, L, L')$, then he sends σ to the adversary.
   c) Unsigncryption queries. The adversary produces a signer list $L = \{ID_1, \cdots, ID_n\}$, a receiver list $L' = \{ID'_1, \cdots, ID'_{n'}\}$ and a ciphertext σ. $\mathcal{C}$ computes $d'_i = Extract(ID'_i)$ $(i \in \{1, \cdots, n'\})$ randomly and sends the result of $Unsigncrypt(\sigma, d'_i, L, L')$ to the adversary. This result may be the symbol $\perp$ if σ is an invalid ciphertext.
3) Challenge. The adversary chooses two plaintexts, m_0 and m_1, a signer list $L_s = \{ID_{c1}, \cdots, ID_{cn'}\}$, and a receiver list $L_r = \{ID_{r1}, \cdots, ID_{rn''}\}$ on which he wishes to be challenged. He cannot have asked the private key that corresponds to the identities in the receiver list L_r in the first stage. $\mathcal{C}$ chooses randomly a bit γ and computes $d_i = Extract(ID_i)(i \in \{1, \cdots, n\})$ and $\sigma^* = Signcrypt(m_\gamma, d_i, L_s, L_r)$. Finally, $\mathcal{C}$ sends σ^* to the adversary.
4) Second stage. The adversary asks a polynomial num-

ber of queries adaptively again as in the first stage. It is not allowed to extract the private key corresponding to the identities in the receiver list L_r and it is not allowed to make an unsigncryption query for σ^* under the receiver list.

5) Guess. Finally, the adversary produces a bit γ' and wins the game if $\gamma' = \gamma$.

Definition 8(Unforgeability). An IASMR scheme is said to be secure against an existential forgery for adaptive chosen message attacks (EUF-IASMR-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.

1) Setup. The challenger $\mathcal{C}$ runs the Setup algorithm with a security parameter k and obtains the public parameters $params$ and a master key S. He sends $params$ to the adversary and keeps S secret.
2) Queries. The adversary performs a polynomially bounded number of queries adaptively just like in the previous definition 7.
3) Forgery. Finally, the adversary produces a new triple (σ, L, L') (*i.e.*, a triple that was not produced by the signcryption oracle) where all of the private keys of signers in the signer list were not asked. The adversary wins the game if the result of Unsigncrypt (σ, L, L') is a valid message m and (m, L) have never been asked.

III. Two IASMR schemes and analysis

First, we review Zhang et al.'s IASMR scheme and Lal et al.'s IASMR scheme. Second, we analyze their schemes and propose the corresponding attack methods.

A. Review of Zhang et al.'s IASMR scheme

Zhang et al.'s IASMR scheme consists of four phases: *Setup, Extract, Signcrypt, Unsigncrypt*.

1) Setup. Let $H : \mathcal{G}_T \rightarrow \{0,1\}^{l_t}$, $H_u : \{0,1\}^* \rightarrow \{0,1\}^{n_u}$, $H_m : \{0,1\}^{l_t} \times \{0,1\}^* \times \mathcal{G}_T \rightarrow \{0,1\}^{n_m}$ be three collision-resistant hash functions for some $n_u, n_m \in \mathcal{Z}$, where l_t is the length of plaintext. Select a pairing $e : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_T$ where the order of $\mathcal{G}, \mathcal{G}_T$ is p. Let g be generators of $\mathcal{G}$. Randomly select $\alpha \in \mathcal{Z}_p$, $g_2, h \in \mathcal{G}$ and compute $g_1 = g^\alpha$. It also selects the random elements: $u', m', u_i, m_j \in \mathcal{G}$, where $i = 1, \cdots, n_u, j = 1, \cdots, n_m$. Let $V_U = \{u_i\}, V_M = \{m_j\}$. The public parameters are $params = (\mathcal{G}, \mathcal{G}_T, e, g, g_1, g_2, u', V_U, m', V_M, H, H_u, H_m)$ and the master secret key is $S = g_2^\alpha$.
2) Extract. Let $\mathcal{U}$ be a bit string of length n_u, representing an identity and let $\mathcal{U}_{[i]}$ be the i-th bit of $\mathcal{U}$. Define $U' \subseteq \{1, \cdots, n_u\}$ to be the set of indices such that $\mathcal{U}_{[i]} = 1$. Randomly select $r_u \in \mathcal{Z}_p^*$ and compute the private key of the identity $\mathcal{U}$: $d_u = (g_2^\alpha (u' \prod_{i \in U'} u_i)^{r_u}, g^{r_u})$.
3) Signcrypt. Let $L = \{ID_1, \cdots, ID_n\}$ be the list of n identities including the actual signer $\mathcal{U}_s$. Let $L' = \{ID'_1, \cdots, ID'_{n'}\}$ be the receiver list and m be a bit string representing a message. $\mathcal{U}_s$ picks random $r_1, r_2, \cdots, r_n, r_m \in \mathcal{Z}_p$ and computes $U_j = u' \prod_{i \in U'_j} u_i$ (for $j = 1, 2, \cdots, n$), $U'_j = u' \prod_{i \in U''_j} u_i$ (for $j = 1, 2, \cdots, n'$) and follows the steps below:
   a) Compute $\omega = e(g_1, g_2)^{r_m}$, $c = m \bigoplus H(\omega)$;
   b) Compute $\sigma_1 = \{R_1 = g^{r_1}, \cdots, R_{s-1} = g^{r_{s-1}}, R_s = g^{r_s} d_{s_2}, R_{s+1} = g^{r_{s+1}}, \cdots, R_n = g^{r_n}\}$;
   c) Compute $\sigma_2 = \{R'_j = U_j'^{r_m} | j = 1, 2, \cdots, n'\}$, $\sigma_3 = g^{r_m}$;
   d) Compute $M = H_m(m, L, \omega)$, $\sigma_4 = d_{s_1} (\prod_{j=1}^n U_j^{r_j}) (m' \prod_{j \in M'} m_j)^{r_m}$ ($M' \subset \{1, 2, \cdots, n_m\}$ be the set of indices j such that $m[j] = 1$, where $m[j]$ is the jth bit of M).

   The ciphertext is $\sigma = (c, \sigma_1, \sigma_2, \sigma_3, \sigma_4, L)$.
4) Unsigncrypt. Receiving a ciphertext $\sigma = (c, \sigma_1, \sigma_2, \sigma_3, \sigma_4, L)$, the receiver ID_j in L' decrypts the ciphertext as follows.
   a) Compute $\omega = \frac{e(d'_{j_1}, \sigma_3)}{e(d'_{j_2}, R'_j)}$, $m = c \bigoplus H(\omega)$, $M = H_m(m, L, \omega)$;
   b) Accept the message if the following equality holds: $e(\sigma_4, g) = e(g_1, g_2)(\prod_{j=1}^n e(U_j, R_j)) e(m' \prod_{j \in M'} m_j, \sigma_3)$

B. Security analysis of Zhang et al.'s IASMR scheme

Let the attacker be $\mathcal{A}$. In the phase of challenge, suppose $\mathcal{A}$ chooses two plaintexts m_0 and m_1, a signer list L and a receiver list L'. Challenger $\mathcal{C}$ flips a γ and signcrypts m_γ. At last, $\mathcal{C}$ gets the ciphertext σ and sends it to $\mathcal{A}$. $\mathcal{A}$ gets the signcryption $\sigma = (c, \sigma_1, \sigma_2, \sigma_3, \sigma_4, L)$ of the message m_γ which was sent to the receiver set L' by the sender set L. $\mathcal{A}$ can construct another signcryption σ' on the same message m_γ as follows.

Based on $\sigma = (c, \sigma_1, \sigma_2, \sigma_3, \sigma_4, L)$, $\mathcal{A}$ computes $\hat{\sigma} = (\hat{c}, \hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3, \hat{\sigma}_4, \hat{L})$ as follows:

$$\hat{c} = c, \hat{\sigma}_1 = \{R_i g | i = 1, 2, \cdots, n\}, \hat{\sigma}_2 = \sigma_2$$

$$\hat{\sigma}_3 = \sigma_3, \hat{\sigma}_4 = \sigma_4 \prod_{j=1}^{n} U_j, \hat{L} = L$$

The forged signcryption $\hat{\sigma} = (\hat{c}, \hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3, \hat{\sigma}_4, \hat{L})$ can pass the unsigncryption. The receiver ID'_j performs the procedures as follows.

1) Compute $\hat{\omega} = \frac{e(d'_{j_1}, \hat{\sigma}_3)}{e(d'_{j_2}, \hat{R}_j)}$, $\hat{m} = \hat{c} \bigoplus H(\hat{\omega})$, $\hat{M} = H_m(\hat{m}, \hat{L}, \hat{\omega})$;
2) Verify whether $e(\hat{\sigma}_4, g) \stackrel{?}{=} e(g_1, g_2)(\prod_{j=1}^n e(U_j, \hat{R}_j)) e(m' \prod_{j \in M'} m_j, \hat{\sigma}_3)$ holds.

The forged ciphertext can pass the verification. From the computation of $\hat{\sigma}$, we can get:

$$\hat{\omega} = \frac{e(d'_{j_1}, \hat{\sigma}_3)}{e(d'_{j_2}, \hat{R}_j)} = \frac{e(d'_{j_1}, \sigma_3)}{e(d'_{j_2}, R'_j)} = \omega$$

$$\hat{m} = \hat{c} \bigoplus H(\hat{\omega}) = c \bigoplus H(\omega) = m_\gamma$$

$$\hat{M} = H_m(\hat{m}, \hat{L}, \hat{\omega}) = H_m(m_\gamma, L, \omega) = M$$

We can get

$$\begin{aligned}
& e(\hat{\sigma}_4, g) \\
= \; & e(\sigma_4 \prod_{j=1}^{n} U_j, g) = e(\sigma_4, g) e(\prod_{j=1}^{n} U_j, g) \\
= \; & e(g_1, g_2)(\prod_{j=1}^{n} e(U_j, R_j)) e(m' \prod_{j \in M'} m_j, \sigma_3) e(\prod_{j=1}^{n} U_j, g) \\
= \; & e(g_1, g_2)(\prod_{j=1}^{n} e(U_j, R_j g)) e(m' \prod_{j \in M'} m_j, \sigma_3) \\
= \; & e(g_1, g_2)(\prod_{j=1}^{n} e(U_j, \hat{R}_j)) e(m' \prod_{j \in M'} m_j, \hat{\sigma}_3)
\end{aligned}$$

Thus, the forged different ciphertext σ' of the message m_γ is valid.

In the phase of Second stage, $\mathcal{A}$ sends σ' to the challenger $\mathcal{C}$. $\mathcal{C}$ sends the plaintext m_γ to $\mathcal{A}$. In the phase of Guess, $\mathcal{A}$ compares m_γ with m_0. If they are equal, output 0; otherwise, output 1. Thus, Zhang et al.'s IASMR scheme does not satisfy the semantic security.

C. Review of Lal et al.'s IASMR scheme

Lal et al.'s IASMR scheme consists of four phases: *Setup, Extract, Signcrypt, Unsigncrypt*.

1) Setup. Given a security parameter k, two groups $\mathcal{G}$ and $\mathcal{G}_T$ of order p, a bilinear map $e : \mathcal{G} \times \mathcal{G} \to \mathcal{G}_T$, a generator g of $\mathcal{G}$, KGC chooses his master key $s \in \mathcal{Z}_p^*$ and computes the public key $P_{pub} = g^s$. It also picks $R \in \mathcal{G}$ and computes $h = e(R, P_{pub})$. It chooses three hash functions $H_1 : \{0,1\}^* \to \mathcal{G}$, $H_2 : \mathcal{G}_T \to \{0,1\}^t$ and $H_3 : \{0,1\}^t \times \mathcal{G} \to \mathcal{Z}_p^*$. The system public parameters are $params = \{\mathcal{G}, \mathcal{G}_T, p, g, e, R, h, P_{pub}, H_1, H_2, H_3\}$
2) Extract. On receiving an identity ID, KGC computes the user's public key $Q_{ID} = H_1(ID)$ and the corresponding private key $D_{ID} = Q_{ID}^s$.
3) Signcrypt. Suppose the sender ID_S wants to send a message m anonymously to n' different receivers $L' = \{ID'_1, \cdots, ID'_{n'}\}$. ID_S performs the following procedures:
   a) Choose a set of users $L = \{ID_1, \cdots, ID_n\}$ ($ID_S \in L$).
   b) Pick $x_i \in \mathcal{Z}_p^*$ and compute $R_i = g^{x_i}$ for $i = 1, \cdots, S-1, S+1, \cdots, n$.
   c) Pick $x_S \in \mathcal{Z}_p^*$ and compute $\alpha = \sum_{i=1}^{n} x_i, \omega = h^\alpha, c = H_2(\omega) \bigoplus m$.
   d) Compute $U = g^\alpha, T_j = (RQ'_j)^\alpha$ for $j = 1, 2, \cdots, n'$.
   e) Compute $h_i = H_3(c, R_i)$ $(i = 1, \cdots, S-1, S+1, \cdots, n)$ and $R_S = Q_S^{x_S} (\prod_{i \neq S} R_i Q_i^{h_i})^{-1}$.
   f) Compute $Z = D_S^{x_S + h_S}$ where $h_S = H_3(c, R_S)$.

   The ciphertext is $\sigma = (c, U, Z, R_1, \cdots, R_n, T_1, \cdots, T_{n'}, L, L')$.
4) Unsigncrypt. Upon receiving $\sigma = (c, U, Z, R_1, \cdots, R_n, T_1, \cdots, T_{n'}, L, L')$, the receiver $ID'_j \in L'$ decrypts σ as follows:
   a) Compute $h_i = H_3(c, R_i)$ for $i = 1, \cdots, n$.
   b) If $e(Z, P) = e(P_{pub}, \prod_{i=1}^{n} R_i Q_i^{h_i})$, it computes $\omega' = e(P_{pub}, T_i) e(U, D'_j)^{-1}$ and recovers the plaintext $m = c \bigoplus H_2(\omega')$. Otherwise, it outputs $\perp$ as failure.

D. Security analysis of Lal et al.'s IASMR scheme

Let the attacker be $\mathcal{A}$. In the phase of challenge, suppose $\mathcal{A}$ chooses two plaintexts m_0 and m_1, a signer list L and a receiver list L'. Challenger $\mathcal{C}$ flips a γ and signcrypts m_γ. At last, $\mathcal{C}$ gets the ciphertext $\sigma = (c, U, Z, R_1, \cdots, R_n, T_1, \cdots, T_{n'}, L, L')$ and sends it to $\mathcal{A}$. $\mathcal{A}$ gets the ciphertext $\sigma = (c, U, Z, R_1, \cdots, R_n, T_1, \cdots, T_{n'}, L, L')$ of the message m_γ which was sent to receiver set L' by the sender set L. $\mathcal{A}$ can construct another signcryption $\sigma' = (\hat{c}, \hat{U}, \hat{Z}, \hat{R}_1, \cdots, \hat{R}_n, \hat{T}_1, \cdots, \hat{T}_{n'}, \hat{L}, \hat{L}')$ on the same message m_γ as follows:

$$\hat{c} = c, \hat{U} = Ug, \hat{Z} = Z, \hat{R}_i = R_i, \hat{T}_j = T_j Q'_j$$

$$\hat{L} = L, \hat{L}' = L', 1 \leq i \leq n, 1 \leq j \leq n'$$

Then, $\hat{\sigma}$ is also a valid different ciphertext of the same message m_γ. $\hat{\sigma}$ can pass the unsigncryption phase.

According to the forge process, we can get:

For $i = 1, \cdots, n$, $\hat{h}_i = H_3(\hat{c}, \hat{R}_i) = H_3(c, R_i) = h_i$, then

$$\begin{aligned}
e(\hat{Z}, P) &= e(Z, P) \\
&= e(P_{pub}, \prod_{i=1}^{n} R_i Q_i^{h_i}) e(P_{pub}, \prod_{i=1}^{n} R_i Q_i^{h_i}) \\
&= e(P_{pub}, \prod_{i=1}^{n} \hat{R}_i Q_i^{\hat{h}_i}) e(P_{pub}, \prod_{i=1}^{n} \hat{R}_i Q_i^{\hat{h}_i})
\end{aligned}$$

$$\begin{aligned}
\hat{\omega} &= e(P_{pub}, \hat{T}_j) e(\hat{U}, D'_j)^{-1} \\
&= e(P_{pub}, T_j Q'_j) e(Ug, D'_j)^{-1} \\
&= e(P_{pub}, T_j) e(U, D'_j)^{-1} e(P_{pub}, Q'_j) e(g, D'_j)^{-1} \\
&= e(P_{pub}, T_j) e(U, D'_j)^{-1} \\
&= \omega'
\end{aligned}$$

Afterwards,

$$\hat{m} = \hat{c} \bigoplus H_2(\hat{\omega}) = c \bigoplus H_2(\omega') = m_\gamma$$

Thus, $\hat{\sigma}$ is also a valid another ciphertext on the same message m_γ.

In the phase of Second stage, $\mathcal{A}$ sends σ' to the challenger $\mathcal{C}$. $\mathcal{C}$ sends the plaintext m_γ to $\mathcal{A}$. In the phase of Guess, $\mathcal{A}$ compares m_γ with m_0. If they are equal, output 0; otherwise, output 1. Lal et al.'s IASMR scheme does not satisfy the semantic security.

IV. Our improved Zhang et al.'s IASMR scheme and analysis

A. Our improved Zhang et al.'s IASMR scheme

Our improved IASMR scheme also consists of four phases: *Setup, Extract, Signcrypt* and *Unsigncrypt*. The phases of *Setup* and *Extract* are the same with Zhang et al.'s scheme. We only described the phases of *Signcrypt* and *Unsigncrypt*.

1) Signcrypt. Let $L = \{ID_1, \cdots, ID_n\}$ be the list of n identities including the actual signer $\mathcal{U}_s$. Let $L' = \{ID'_1, \cdots, ID'_{n'}\}$ be the receiver list and m be a bit string representing a message. $\mathcal{U}_s$ picks random $r_1, r_2, \cdots, r_n, r_m \in \mathcal{Z}_p$ and computes $U_j = u' \prod_{i \in U'_j} u_i$ (for $j = 1, 2, \cdots, n$), $U'_j = u' \prod_{i \in U''_j} u_i$ (for $j = 1, 2, \cdots, n'$) and follows the steps below:
   a) Compute $\omega = e(g_1, g_2)^{r_m}$, $c = m \bigoplus H(\omega)$;
   b) Compute $R_1 = g^{r_1}, \cdots, R_{s-1} = g^{r_{s-1}}, R_s = g^{r_s} d_{s_2}, R_{s+1} = g^{r_{s+1}}, \cdots, R_n = g^{r_n}$. We denote $\sigma_1 = \{R_1, \cdots, R_{s-1}, R_s, R_{s+1}, \cdots, R_n = g^{r_n}\}$
   c) Compute $\sigma_2 = \{R'_j = U'^{r_m}_j | j = 1, 2, \cdots, n'\}$, $\sigma_3 = g^{r_m}$
   d) Compute $M = H_m(m, L, \omega, \sigma_1, \sigma_2, \sigma_3)$,
   $$\sigma_4 = d_{s_1} (\prod_{j=1}^{n} U_j^{r_j})(m' \prod_{j \in M'} m_j)^{r_m}$$
   where $M' \subset \{1, 2, \cdots, n_m\}$ denotes the set of indices j such that $m[j] = 1$, where $m[j]$ is the jth bit of M.

   The ciphertext is $\sigma = (c, \sigma_1, \sigma_2, \sigma_3, \sigma_4, L)$.
2) Unsigncrypt. Receiving a ciphertext $\sigma = (c, \sigma_1, \sigma_2, \sigma_3, \sigma_4, L)$, the receiver ID_j in L' decrypts the ciphertext as follows.
   a) Compute $\omega = \frac{e(d'_{j_1}, \sigma_3)}{e(d'_{j_2}, R'_j)}$, $m = c \bigoplus H(\omega)$, $M = H_m(m, L, \omega, \sigma_1, \sigma_2, \sigma_3)$;
   b) Accept the message if the following equality holds: $e(\sigma_4, g) = e(g_1, g_2)(\prod_{j=1}^{n} e(U_j, R_j)) e(m' \prod_{j \in M'} m_j, \sigma_3)$.

B. Analysis of our improved Zhang et al.'s IASMR scheme

Compared with Zhang et al.'s IASMR scheme, the improved IASMR scheme makes the Hash function H_m act on the values of $(m, L, \omega, \sigma_1, \sigma_2, \sigma_3)$. The weak in the original scheme lies in the fact that σ_1 and σ_4 are linear. So, the forged ciphertext can pass the verification. Our improvement breaks the linearity. Thus, it can resist our attack.

Our improved Zhang et al.'s IASMR scheme can also satisfy the security properties: correctness, signcrypter identity's ambiguity, semantic security and unforgeability. The proof processes are very similar with Zhang et al.'s IASMR scheme. We omit them here due to the page limits.

V. Our improved Lal et al.'s IASMR scheme and analysis

A. Our improved Lal et al.'s IASMR scheme

Our improved IASMR scheme also consists of four phases: *Setup, Extract, Signcrypt* and *Unsigncrypt*. The phases of *Setup* and *Extract* are the same with Lal et al.'s scheme. We only describe the phases of *Signcrypt* and *Unsigncrypt*.

1) Signcrypt. Suppose the sender ID_S wants to send a message m anonymously to n' different receivers $L' = \{ID'_1, \cdots, ID'_{n'}\}$. ID_S performs the following procedures.
   a) Choose a set of users $L = \{ID_1, \cdots, ID_n\}$ ($ID_S \in L$).
   b) Pick $x_i \in \mathcal{Z}_p^*$ and compute $R_i = g^{x_i}$ for $i = 1, \cdots, S-1, S+1, \cdots, n$.
   c) Pick $x_S \in \mathcal{Z}_p^*$ and compute $\alpha = \sum_{i=1}^{n} x_i, \omega = h^\alpha, c = H_2(\omega) \bigoplus m$
   d) Compute $U = g^\alpha, T_j = (RQ'_j)^\alpha$ for $j = 1, 2, \cdots, n'$. Denote $T = \{T_j, j = 1, 2, \cdots, n'\}$.
   e) Compute $h_i = H_3(c, R_i, U, T, L, L')$ for $i = 1, \cdots, S-1, S+1, \cdots, n$ and $R_S = Q_S^{x_S} (\prod_{i \neq S} R_i Q_i^{h_i})^{-1}$.
   f) Compute $Z = D_S^{x_S + h_S}$ where $h_S = H_3(c, R_S, U, T, L, L')$.

   The ciphertext is $\sigma = (c, U, Z, R_1, \cdots, R_n, T_1, \cdots, T_{n'}, L, L')$.
2) Unsigncrypt. Upon receiving $\sigma = (c, U, Z, R_1, \cdots, R_n, T_1, \cdots, T_{n'}, L, L')$, the receiver $ID'_j \in L'$ decrypts σ as follows.
   a) Computes $h_i = H_3(c, R_i, U, T, L, L')$ for $i = 1, \cdots, n$
   b) If $e(Z, P) = e(P_{pub}, \prod_{i=1}^{n} R_i Q_i^{h_i})$, computes $\omega' = e(P_{pub}, T_i) e(U, D'_j)^{-1}$ and recovers the plaintext $m = c \bigoplus H_2(\omega')$. Otherwise it outputs $\perp$ as failure.

B. Analysis of our improved Lal et al.'s IASMR scheme

Compared with Lal et al.'s IASMR scheme, the improved IASMR scheme makes the Hash function H_3 act on the values of (c, R_i, U, T, L, L'). The weak in Lal et al.'s scheme lies in the fact that U and T_j are linear. So, the forged ciphertext has the same ω with the original ciphertext. Our improvement breaks the linearity. Thus, it can resist our attack.

Our improved Lal et al.'s IASMR scheme can also satisfy the security properties: correctness, signcrypter identity's ambiguity, semantic security and unforgeability. The proof processes are very similar with Lal et al.'s IASMR scheme. We omit them here due to the page limits.

Notes: Our improved IASMR schemes are provable secure under the assumptions of DLP, CDH, DBDH are computational difficult. Due to the page limits, we omit the proof process in this paper.

VI. Conclusion

We analyze Zhang et al.'s IASMR scheme and Lal et al.'s IASMR scheme. We propose the attack methods. Our attack shows that their schemes can not satisfy the semantic security. We improve the two IASMR schemes. The improved schemes satisfy the security properties: correctness, signcrypter identity's ambiguity, semantic security and unforgeability.

Acknowledgment

This work was partly supported by Natural Science Foundation of Liaoning Province (No. 20102042), by China Post-doctor Science Fund (No. 20110490061) and by Program for Liaoning Excellent Talents in University (No. LJQ2011078), by the NSF of China through projects (No. 61003214), by the Fundamental Research Funds for Shaanxi Provincial Education Department through Scientific Research Program (No. 2010JK727), by the Spanish Government through projects TSI2007-65406-C03-01 "E-AEGIS", TIN2011-27076-C03-01 "CO-PRIVACY" and CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", by the Government of Catalonia under grant 2009 SGR 1135, by the European Commission under FP7 project "DwB".

References

[1] Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption)$\leq$ cost(signature)+cost(encryption). Crypto 1997, LNCS 1294, Springer-Verlag, Berlin, 1997, pp. 165-179.

[2] J. An, Y. Dodis and T. Rabin. On the security of joint signature and encryption. Eurocrypt 2002. LNCS 2332, Springer Verlag, Berlin, 2002, pp.83-107.

[3] J. Baek, R. Steinfeld and Y. Zheng Y. Formal proofs for the security of signcryption. PKC 2002, LNCS 2274, Springer-Verlag, Berlin, 2002, pp. 80-98.

[4] B. Libert and J. Quisquator. A new identity based signcryption scheme from pairings. IEEE Information Theory Workshop 2003, pp.155-158.

[5] X. Huang, W. Su, Y. Mu. Identity-based ring signcryption scheme: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world. ACISP 2003, LNCS 2727, Springer-Verlag, Berlin, 2003, pp. 649-654.

[6] F. Li, H. Xiong, Y. Yu. An efficient id-based ring signcryption scheme. ICCCAS 2008, 2008, pp. 483-487.

[7] Z. Zhu, Y. Zhang and F. Wang. An efficient and provable secure identity based ring signcryption scheme. Computer Standards and Interfaces. 2009, 31(6): 1092-1097.

[8] J. Zhang, S. Gao, H. Chen and G. Qin. A novel ID-based anonymous signcryption scheme. APWeb/WAIM 2009, LNCS 5446, Springer-Verlag, Berlin, 2009, pp. 604-610.

[9] M. Bellare, A. Boldyreva and S. Micali. Public-key encryption in a multi-user setting: security proofs and improvements . EUROCRYPT 2000 , LNCS 1807, Springer-Verlag, Berlin, 2000, pp. 259-274.

[10] S. Duan and Z. Cao. Efficient and provably secure multi-receiver identity-based signcryption. ACISP 2006, LNCS 4058, Springer-Verlag, Berlin, pp.195C206.

[11] C. Tan. On the security of provably secure multi-receiver ID-based signcryption scheme. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E91-A (7), 2008, pp. 1836-1838.

[12] S. Lal, P. Kushwah. Anonymous ID based signcryption scheme for multiple receivers. Cryptology ePrint Archive: Report 2009/345 (2009), http: //eprint. iacr. org/2009/345

[13] B. Zhang and Q. Xu. An ID-Based anonymous signcryption scheme for multiple receivers secure in the standard model. AST/UCMA/ISA/ACN 2010, LNCS 6059, Springer-Verlag, Berlin, 2010, pp. 15-27.