An ID-based Anonymous Signcryption Scheme for Multiple Receivers

Bo Zhang[1] and Qiuliang Xu[2]
[1]*School of Information Science and Engineering*
University of Jinan, 250022, Jinan, Shandong, China
{zhangbo996@gmail.com}
[2]*School of Computer Science and Technology*
Shandong University, 250101, Jinan, Shandong, China

Abstract

Anonymous signcryption is a novel cryptographic primitive motivated from ring signature. It is an important method to realize the signcrypter identities' ambiguity. In this paper, we propose an identity-based anonymous signcryption scheme for multiple receivers in the standard model. The proposed scheme satisfies the semantic security, unforgeability and signcrypter identity's ambiguity. We also give the formal security proof on its semantic security under the hardness of Decisional Bilinear Diffie-Hellman problem and its unforgeability under the Computational Diffie-Hellman assumption.

Keywords: *signcryption, identity based, multi-receiver, anonymous signcryption*

1. Introduction

Encryption and signature are basic cryptographic tools to achieve private and authenticity. In 1997, Zheng [1] proposed the notion of signcryption, which can perform digital signature and public key encryption simultaneously at lower computational costs and communication overheads than sign- then-encrypt way to obtain private and authenticated communications in the open channel. Identity-based (ID-based) cryptosystems were introduced by Shamir [2] in 1984. Its main idea is that the public keys of a user can be easily derived from arbitrary strings corresponding to his identity information such as name, telephone number or email address. The corresponding private key can only be derived by a trusted Private Key Generator (PKG). By combining ID-based cryptology and signcryption, Malone-Lee [3] gave the first ID-based signcryption scheme. Since then, quite a few ID-based signcryption schemes [4,5,6,7,8] have been proposed.

In some network applications, we have to distribute same message to several different persons. A simple approach for achieving this goal is that the sender encrypts the message for each person respectively. Obviously, the cost of using the approach in large group is very high. Consider a scenario like this, suppose Bob is a cabinet member who wants to leak very important information to the public. The fastest and most convenient way is to leak the information to several different journalists at the same time (avoiding that some of them have been corrupted). Bob wants to remain anonymous, but needs to convince these journalists that the information actually came from a cabinet member. At the same time, the information should not be leaked until most the journalists receive it. Thus, we need anonymity and authentication of Bob, confidentiality of the information before it reaches the honest journalists. All of the properties are together achieved by a primitive called “Anonymous

Signcryption for Multiple Receivers".

Anonymous signcryption or ring signcryption is a novel cryptographic primitive motivated from ring signature [9]. It is an important method to 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 actual signcrypter's identity. Huang et al. [10] proposed the first ID-based ring signcryption scheme along with a security model. Some more ID-based ring signcryption schemes are reported in [11,12,13]. In 2006, Duan et al. [14] gave the first multi-receiver ID-based signcryption scheme which only needs one pairing computation to signcrypt a message for n receivers and in 2009, Sunder Lal et al. [15] proposed the first anonymous ID-based signcryption scheme for multiple receivers. The security of the scheme was proven secure in the random oracle model [16]. Although the model is efficient and useful, it has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure [17]. Therefore, it is an important research problem to construct an ID-based anonymous signcryption scheme secure in the standard model.

Our contribution In this paper, we give the first ID-based anonymous signcryption scheme for multiple receivers in the standard model. The proposed scheme satisfies the semantic security, unforgeability and signcrypter identity's ambiguity. We also give the formal security proof on its semantic security under the hardness of Decisional Bilinear Diffie-Hellman problem and its unforgeability under the Computational Diffie-Hellman assumption.

2. Preliminaries

Let G and G_T be two cyclic multiplicative groups of prime order p and g be a generator of G.

2.1. Bilinear Pairings

The map $e: G \times G \to G_T$ is said to be an admissible bilinear pairing if the following conditions hold true.

(1) e is bilinear, i.e. $e(g^a, g^b) = e(g,g)^{ab}$ for all $a, b \in Z_p$.

(2) e is non-degenerate, i.e. $e(g,g) \neq 1_{G_T}$.

(3) e is efficiently computable.

We refer the reader to [18] for more details on the construction of such pairings.

2.2. Complexity assumptions

2.2.1. Decisional Bilinear Diffie-Hellman (DBDH) Assumption

The challenger chooses $a,b,c,z \in Z_p$ at random and then flips a fair binary coin β. If $\beta = 1$ it output the tuple $(g, A = g^a, B = g^b, C = g^c, Z = e(g,g)^{abc})$. Otherwise, if $\beta = 0$, the challenger outputs the tuple $(g, A = g^a, B = g^b, C = g^c, Z = e(g,g)^z)$. The adversary must then output a guess β' of β.

An adversary, λ, has at least an ε advantage in solving the decisional BDH problem if

$$|\Pr[\lambda(g, g^a, g^b, g^c, e(g,g)^{abc}) = 1] - \Pr[\lambda(g, g^a, g^b, g^c, e(g,g)^z) = 1]| \geq \varepsilon$$

where the probability is over the randomly chosen a,b,c,z and the random bits consumed by λ.

Definition 1. The decisional DBDH assumption holds if no adversary has at least ε advantage in solving the above game.

2.2.2. Computational Diffie-Hellman (CDH) Assumption

The challenger chooses $a,b \in Z_p$ at random and outputs $(g, A = g^a, B = g^b)$. The adversary then attempts to output $g^{ab} \in G$. An adversary, λ, has at least an ε advantage if $\Pr[\lambda(g, g^a, g^b) = g^{ab}] \geq \varepsilon$ where the probability is over the randomly chosen *a*, *b* and the random bits consumed by λ.

Definition 2. The computational CDH assumption holds if no adversary has at least ε advantage in solving the above game.

3. ID-based Anonymous Signcryption scheme for Multiple Receivers (IASCfMR Scheme)

3.1. Generic scheme

An IASCfMR scheme consists of the following algorithms.

• Setup: Given a security parameter *k*, PKG generates a master key *S* and common parameters *P*. *P* is made public while *S* is kept secret.

• Extract: Given an identity ID_u, the PKG runs this algorithm to generate the private key d_u associated with ID_u and transmits it to the user via a secure channel.

• Signcrypt: To send a message m to n' receivers with identity $L' = \{ID'_1, ..., ID'_{n'}\}$ anonymously, The actual signcrypter with identity ID_s selects a group of n users' identities $L = \{ID_1, ..., ID_n\}$ including himself obtain a ciphertext σ by running Signcrypt (m, d_s, L, L').

• Unsigncrypt: Upon receiving the ciphertext σ, the receiver with identity ID'_j in the receiver list $L' = \{ID'_1, ..., ID'_{n'}\}$ runs Unsigncrypt (σ, d'_j, L, L') and obtains the message m or the symbol □ indicating that the ciphertext is invalid.

3.2. Security notions

Now we present security notions for our IASCfMR scheme.

Definition 3. (Signcrypter identity's ambiguity**)** An IASCfMR scheme is unconditional anonymous if for any group of n members with identities in the signer list L, the probability of any adversary to identify the actual signcrypter in not more than random guess's i.e. the adversary output the identity of actual signcrypter with probability 1/n if he is not a member of L, and with probability 1/(n-1) if he is the member of L.

Definition 4. (Semantic security**)** An IASCfMR scheme is said to have the indistinguishability against adaptive chosen ciphertext attacks property (IND-IASCfMR -CCA2) if no polynomially bounded adversary has a non-negligible advantage in the following game.

Setup: The challenger ϑ runs the Setup algorithm with a security parameter k and obtains common parameters P and a master key S. He sends P to the adversary and keeps S secret.

First stage: The adversary 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.

• Extraction queries: The adversary requests the private key of an identity ID_u and receives the extracted private key d_u =Extract (ID_u).

• Signcryption queries: The adversary produces a signer list $L = \{ID_1, ..., ID_n\}$, a receiver list $L' = \{ID'_1, ..., ID'_{n'}\}$ and a plaintext m (Note that the adversary should not have asked the private key corresponding the identities in the receiver list). ϑ computes d_i =Extract (ID_i) $(i \in \{1, ..., n\})$ randomly and σ= Signcrypt (m, d_i, L, L'), then he sends σ to the adversary.

• Unsigncryption queries: The adversary produces a signer list $L = \{ID_1,...,ID_n\}$, a receiver list $L' = \{ID'_1,...,ID'_{n'}\}$ and a ciphertext σ. $\mathcal{G}$ computes d'_i =Extract (ID'_i) $(i \in \{1,...,n'\})$ randomly and sends the result of Unsigncrypt (σ, d'_i, L, L') to the adversary. This result may be the symbol □ if σ is an invalid ciphertext.

Challenge: The adversary chooses two plaintexts, m_0 and m_1, a signer list $L = \{ID_1,...,ID_n\}$, and a receiver list $L' = \{ID'_1,...,ID'_{n'}\}$ on which he wishes to be challenged. He cannot have asked the private key corresponding the identities in the receiver list in the first stage. $\mathcal{G}$ chooses randomly a bit γ, $\mathcal{G}$ computes d_i =Extract (ID_i) $(i \in \{1,...,n\})$ randomly and σ = Signcrypt (m_γ, d_i, L, L') and sends σ to the adversary.

Second stage: The adversary asks a polynomial number of queries adaptively again as in the first stage. It is not allowed to extract the private key corresponding the identities in the receiver list and it is not allowed to make an unsigncryption query for σ under the receiver list.

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

Definition 5. (Unforgeability) An IASCfMR scheme is said to be secure against an existential forgery for adaptive chosen message attacks (EUF-IASCfMR-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.

Setup: The challenger $\mathcal{G}$ runs the Setup algorithm with a security parameter *k* and obtains common parameters *P* and a master key *S*. He sends *P* to the adversary and keeps *S* secret.

Queries: The adversary performs a polynomially bounded number of queries adaptively just like in the previous definition.

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.

4. The concrete scheme

In the section, we describe our IASCfMR scheme. Our concrete scheme is motivated from Waters' ID-based encryption scheme [19] and the signature schemes in [20,21].

• Setup: Choose groups G and G_T of prime order p such that an admissible pairing

$e: G \times G \to G_T$ can be constructed and pick a generator *g* of *G*.

Now, pick a random secret $\alpha \in Z_p$, compute $g_1 = g^\alpha$ and pick $g_2 \leftarrow_R G$. Furthermore, pick elements $u', m' \leftarrow_R G$ and vectors $\Lambda_U = (u_i)$, $\Lambda_M = (m_i)$ of length n_u and n_m, respectively, whose entries are random elements from *G*. Let *H, H_u, H_m* are cryptography hash functions where $H: G_T \to \{0,1\}^{l_t}$, $H_u: \{0,1\}^* \to \{0,1\}^{n_u}$, $H_m: \{0,1\}^{l'} \times \{0,1\}^* \times G_T \to \{0,1\}^{n_m}$ where l_t is the length of plaintext.

The public parameters are $P = (G, G_T, e, g, g_1, g_2, u', \Lambda_U, m', \Lambda_M, H_u, H_m)$ and the master secret *S* is g_2^α.

• Extract: Let *u* be a bit string of length n_u representing an identity and let $u[i]$ be the *i*-th bit of *u*. Define $U' \subset \{1,...,n_u\}$ to be the set of indicies *i* such that $u[i] = 1$.

To construct the private key d_u of the identity *u*, pick $r_u \leftarrow Z_p$ and compute:

$$d_u = (g_2^\alpha (u' \prod_{i \in U'} u_i)^{r_u}, g^{r_u})$$

• Signcrypt: Let *L*= $\{ID_1,\ldots,ID_n\}$ be the list of *n* identities including the one of the actual signer, $L' = \{ID'_1,...,ID'_{n'}\}$ be the receiver list and *m* be a bit string representing a message.

Let the actual signer be indexed *s*, where $s \in \{1,...,n\}$, with private key $d_s = (d_{s1}, d_{s2}) = (g_2^\alpha (u' \prod_{j \in U'_s} u_j)^{r_s}, g^{r_s})$

He selects a group of *n* users' identities $L = \{ID_1,...,ID_n\}$ including himself, picks $r_1,...,r_n, r_m \in Z_p$ randomly, computes $U_j = u' \prod_{i \in U'_j} u_i$ (for *j*=1,...,*n*), $U'_j = u' \prod_{i \in U''_j} u_i$ (for *j*=1,..., n') and follows the steps below:

（1） Compute $\omega = e(g_1, g_2)^{r_m}$

（2） Compute $c = m \oplus H(\omega)$

（3） Compute $\sigma_1 = \{R_1 = g^{r_1}, ..., R_{s-1} = g^{r_{s-1}}, R_s = g^{r_s} \cdot d_{s2}, R_{s+1} = g^{r_{s+1}}, ..., R_n = g^{r_n}\}$

（4） Compute $\sigma_2 = \{R'_j = U'^{r_m}_j \mid j = 1,...,n'\}$

（5） Compute $\sigma_3 = g^{r_m}$

（6） Compute $M = H_m(m, L, \omega)$, $\sigma_4 = d_{s1} \cdot (\prod_{j=1}^{n} (U_j)^{r_j})(m' \prod_{j \in M'} m_j)^{r_m}$ ($M' \subset \{1,...,n_m\}$ be the set of indicies j such that $m[j] = 1$, where $m[j]$ is the jth bit of M).

The resultant ciphertext is $\sigma = (c, \sigma_1, \sigma_2, \sigma_3, \sigma_4, L)$.

• Unsigncrypt: Received a ciphertext $\sigma = (c, \sigma_1, \sigma_2, \sigma_3, \sigma_4, L)$, the receiver with index j in L' decrypts the ciphertext as follows:

（1） Compute $\omega = e(d'_{j1}, \sigma_3) / e(d'_{j2}, R'_j)$

（2） Compute $m = c \oplus H(\omega)$

（3） Compute $M = H_m(m, L, \omega)$

The receiver accepts the message if and only if the following equality holds:

$$e(\sigma_4, g) = e(g_1, g_2)(\prod_{j=1}^{n} e(U_j, R_j))e(m' \prod_{j \in M'} m_j, \sigma_3)$$

5. Analysis of the scheme

5.1. Correctness

The correctness of the scheme can be directly verified by the following equations.

$$\begin{aligned}
&e(\sigma_4, g) = e(d_{s1} \cdot (\prod_{j=1}^{n} (U_j)^{r_j})(m' \prod_{j \in M'} m_j)^{r_m}, g) \\
&= e(g_2^{\alpha} U_s^r, g) \cdot e(\prod_{j=1}^{n} (U_j)^{r_j}, g) e((m' \prod_{j \in M'} m_j)^{r_m}, g) \\
&= e(g_2^{\alpha}, g) \cdot e(\prod_{j=1}^{n} (U_j)^{r_j} \cdot U_s^r, g) e((m' \prod_{j \in M'} m_j)^{r_m}, g) \\
&= e(g_1, g_2)(\prod_{j=1, j \neq s}^{n} e(U_j, R_j)) \cdot e(U_s^{r+r_s}, g) e(m' \prod_{j \in M'} m_j, \sigma_3) \\
&= e(g_1, g_2)(\prod_{j=1, j \neq s}^{n} e(U_j, R_j)) \cdot e(U_s, R_s) e(m' \prod_{j \in M'} m_j, \sigma_3) \\
&= e(g_1, g_2)(\prod_{j=1}^{n} e(U_j, R_j)) e(m' \prod_{j \in M'} m_j, \sigma_3)
\end{aligned}$$

5.2. Security

Theorem 1. *The proposed IASCfMR scheme is unconditional anonymous.*

Proof. We have to show that given a signcryption ciphertext on the message *m* produced by a member in the signcrypter list $L = \{ID_1, ..., ID_n\}$, anyone is not able to identify the actual signcrypter except the real signcrypter himself. To show our scheme satisfies unconditional anonymous, we only prove that anyone in the signcrypter list can produce the same ciphertext on the message *m*. We assume there are two signers A and B with identities ID_i and ID_j ($i, j \in \{1, ..., n\}$) whose private keys are $d_A = (d_{A1}, d_{A2}) = (g_2^{\alpha}(u' \prod_{j \in U'_A} u_j)^{r_A}, g^{r_A})$ and $d_B = (d_{B1}, d_{B2}) = (g_2^{\alpha}(u' \prod_{j \in U'_B} u_j)^{r_B}, g^{r_B})$ respectively.

We know that，to produce signcryption ciphertext on the message *m*, A should picks $r_1, ..., r_i, ..., r_j, ..., r_n, r_m \in Z_p$ randomly and compute as follows:

（1） Compute $\omega = e(g_1, g_2)^{r_m}$

（2） Compute $c = m \oplus H(\omega)$

（3） Compute $\sigma_1 = \{R_1 = g^{r_1}, ..., R_{i-1} = g^{r_{i-1}}, R_i = g^{r_i} \cdot d_{A2}, R_{i+1} = g^{r_{i+1}}, ..., R_n = g^{r_n}\}$

（4） Compute $\sigma_2 = \{R'_s = U'^{r_m}_s \mid s = 1, ..., n'\}$

（5） Compute $\sigma_3 = g^{r_m}$

（6） Compute $\sigma_4 = d_{A1} \cdot (\prod_{j=1}^{n} (U_j)^{r_j})(m' \prod_{j \in M'} m_j)^{r_m}$

In the following, it is shown that there exists random numbers $r'_1, ..., r'_n, r'_m \in Z_p$, by which B can produce the same signcryption ciphertext. The random numbers choose by B are

$$r'_1 = r_1, ..., r'_i = r_i + r_A, ..., r'_j = r_j - r_B, ..., r'_n = r_n, r'_m = r_m$$

Then B could produce the signcryption ciphertext as

（1） Compute $\omega = e(g_1, g_2)^{r'_m}$

（2） Compute $c = m \oplus H(\omega)$

（3） Compute $\sigma_1 = \{R_1 = g^{r_1'}, ..., R_{j-1} = g^{r_{j-1}'}, R_j = g^{r_j'} \cdot d_{B2}, R_{i+1} = g^{r_{i+1}'}, ..., R_n = g^{r_n'}\}$

（4） Compute $\sigma_2 = \{R_s' = U_s''^{r_m'} \mid s = 1, ..., n'\}$

（5） Compute $\sigma_3 = g^{r_m'}$

（6） Compute $\sigma_4 = d_{B1} \cdot (\prod_{j=1}^{n} (U_j)^{r_j'})(m' \prod_{j \in M'} m_j)^{r_m'} = d_{A1} \cdot (\prod_{j=1}^{n} (U_j)^{r_j})(m' \prod_{j \in M'} m_j)^{r_m}$

Obviously, the signcryption ciphertext generated by B is the same as ciphertext generated by A. In other words, given L' on the message *m*, all of the signers in *L* can produce it. So, our IASCfMR scheme is unconditional anonymous. The probability of any adversary to identify the actual signcrypter in not more than random guess's i.e. the adversary output the identity of actual signcrypter with probability 1/n if he is not a member of *L*, and with probability 1/(n-1) if he is the member of *L*.

Theorem 2. *Assume there is an IND-IASCfMR-CCA2 adversary that is able to distinguish two valid ciphertexts during the game defined in Definition 4 with an advantage* ε *and asking at most* q_E *extraction queries,* q_S *signcryption queries and* q_U *unsigncryption queries, then there exists a distinguisher* ϑ *that can solve an instance of the Decisional Bilinear Diffie-Hellman problem with an* $\frac{\varepsilon}{2^{n'+2}((q_E + q_S + q_U)(n_u + 1))^{n'} q_S (n_m + 1)}$ *advantage .*

Proof. Assume that the distinguisher ϑ receives a random DBDH problem instance $(g, A = g^a, B = g^b, C = g^c, Z \in G_T)$, his goal is to decide whether ϑ or not. ϑ will run the adversary as a subroutine and act as the adversary's challenger in the IND-IASCfMR-CCA2 game. Our proof is based on Waters' idea such as in [19,20,21].

Setup: Let $l_u = 2(q_E + q_S + q_U)$ and $l_m = 2q_S$, ϑ choose randomly

(1) Two integers k_u and $F(u_j) = 0 \bmod l_u$ $(0 \le k_u \le n_u, j \in [1, n'])$

(2) An integer $x' \in Z_{l_u}$, an n_u-dimensional vector $L' = \{ID_1', ..., ID_{n'}'\}$ $(x_i \in Z_{n_u})$

(3) An integer $z' \in Z_{l_m}$, an $L = \{ID_1, ..., ID_n\}$-dimensional vector $Z = (z_j)$ $(z_j \in Z_{n_m})$

(4) Two integers $y', \omega' \in Z_p$, an n_u-length vector $Y = y_i$ $(y_i \in Z_p)$ and an n_m-length vector $W = \omega_j$ $(\omega_j \in Z_p)$

For ease of analysis, we define the functions for an identity *u* and a message *m* respectively.

$F(u) = -l_u k_u + x' + \sum_{i \in U'} x_i$ and $J(u) = y' + \sum_{i \in U'} y_i$

$K(m) = -l_m k_m + z' + \sum_{j \in M'} z_j$ and $L(m) = \omega' + \sum_{j \in M'} \omega_j$

Then the challenger assigns a set of public parameters as follows.

$g_1 = g^a$, $g_2 = g^b$, $u' = g_2^{-l_u k_u + x'} g^{y'}$, $u_i = g_2^{x_i} g^{y_i} (1 \le i \le n_u)$, $m' = g_2^{-l_m k_m + z'} g^{\omega'}$,

$m_j = g_2^{z_j} g^{\omega_j} (1 \le j \le n_m)$

Note that these public parameters have the same distribution as in the game between the distinguisher $\mathcal{G}$ and the adversary. For any identity u and any message m, we have

$U = u' \prod_{i \in U'} u_i = g_2^{F(u)} g^{J(u)}$, $m' \prod_{j \in M'} m_j = g_2^{K(m)} g^{L(m)}$.

First stage: $\mathcal{G}$ answers the queries as follows:

Extraction queries

When the adversary asks for the private key corresponding to an identity u, the distinguisher $\mathcal{G}$ first checks if $F(u) = 0$ and aborts in this situation. Otherwise, it chooses a random $r_u \in Z_p$ and gives the adversary the pair $d_u = (d_{u1}, d_{u2}) = (g_1^{\frac{-J(u)}{F(u)}} (u' \prod_{i \in U'} u_i)^{r_u}, g_1^{\frac{-1}{F(u)}} g^{r_u})$

Let $\hat{r}_u = r_u - \frac{a}{F(u)}$, as in Waters' proof [19] and Paterson's proof [20] and we will show in the following, d_u is a valid private key for identity u. The distinguisher $\mathcal{G}$ can generate such a d_u if and only if $F(u) \neq 0 \bmod l_u$. The simulation is perfect since

$$d_{u1} = g_1^{\frac{-J(u)}{F(u)}} (g_2^{F(u)} g^{J(u)})^{r_u} = g_2^a (g_2^{F(u)} g^{J(u)})^{\frac{-a}{F(u)}} (g_2^{F(u)} g^{J(u)})^{r_u} = g_2^a (g_2^{F(u)} g^{J(u)})^{r_u - \frac{a}{F(u)}}$$

$$= g_2^a (g_2^{F(u)} g^{J(u)})^{\hat{r}_u} \text{ and } d_{u2} = g_1^{\frac{-1}{F(u)}} g^{r_u} = g^{r_u - \frac{a}{F(u)}} = g^{\hat{r}_u}.$$

Signcryption queries

At any time, the adversary can perform a signcryption query for a signer list $L = \{ID_1, ..., ID_n\}$, a receiver list $L' = \{ID'_1, ..., ID'_{n'}\}$ and a plaintext m. If for all $j \in [1, n]$, $F(u_j) = 0 \bmod l_u$, $\mathcal{G}$ will simply abort. Otherwise, $\mathcal{G}$ first choose an identity u_i,

where $F(u_i) \neq 0 \bmod l_u$, generates a private key d_i for u_i just calling the extract query algorithm described above, and then runs Signcrypt (m, d_i, L, L') to answer the adversary's query.

Unsigncryption queries

At any time, the adversary can perform an unsigncryption query on a ciphertext σ for a signer list $L = \{ID_1, ..., ID_n\}$ and a receiver list $L' = \{ID'_1, ..., ID'_{n'}\}$. If for all $j \in [1, n']$, $F(u_j) = 0 \bmod l_u$, ϑ will simply abort. Otherwise, ϑ first choose an identity u'_i, where $F(u'_i) \neq 0 \bmod l_u$, generates a private key d'_i for u'_i just calling the extract query algorithm described above, and then runs Unsigncrypt (σ, d'_i, L, L') to answer the adversary's query.

After a polynomially bounded number of queries, the adversary chooses a signer list $L^* = \{ID_1^*, ..., ID_n^*\}$, a receiver list $L'^* = \{ID_1'^*, ..., ID_{n'}'^*\}$ on which he wishes to be challenged. Note that the adversary has not asked a key extraction query on any identity in L'^* during the first stage. Then the adversary submits two messages m_0, m_1 to ϑ. ϑ checks whether the following conditions are fulfilled:

（1） $F(u_j'^*) = 0 \bmod l_u$ for all $j \in [1, n']$, where $u_j'^* = H_u(ID_j'^*)$

（2） $K(m^*) = 0 \bmod l_m$ where $m^* = H_m(m_\gamma, L^*, Z)$

Challenge: If not all the above conditions are fulfilled, ϑ will abort. Otherwise, ϑ flips a fair binary coin γ and constructs a signcryption ciphertext of M_γ as follows. $m_\gamma[i]$ denotes the *i*th bit of m^* and let $M' \subset \{1, ..., n_m\}$ be the set of indicies *j* such that $m_\gamma[i] = 1$. ϑ choose an identity u_s^*, where $F(u_s^*) \neq 0 \bmod l_u$ and $r_1, ..., r_n \in_R Z_p$. ϑ sets the ciphertext as

$$(m_\gamma \oplus H(Z), \{g^{r_1}, ...g^{r_{s-1}}, g^{r_s} \cdot g_1^{\frac{-1}{F(u_s^*)}} g^{r_s^*}, g^{r_{s+1}}, ..., g^{r_n}\},$$
$$\{C^{J(u_i'^*)} \mid i = 1, ...n'\}, C, g_1^{\frac{-J(u_s^*)}{F(u_s^*)}} \cdot \prod_{i=1}^{n} (g_2^{F(u_i^*)} g^{J(u_i^*)})^{r_i} \cdot C^{L(m_\gamma)})$$

Let $Z = e(g,g)^{abc}$, $c = r_m$, $C = g^c$, the simulation is perfect since

$$Z = e(g,g)^{abc} = e(g_1, g_2)^{r_m}, C^{J(u_i'^*)} = (U_i'^*)^{r_m}$$

$$g_1^{\frac{-J(u_s^*)}{F(u_s^*)}} \cdot \prod_{i=1}^{n} (g_2^{F(u_i^*)} g^{J(u_i^*)})^{r_i} \cdot C^{L(m_\gamma)} = d_{s1}^* \cdot (\prod_{j=1}^{n} (U_j)^{r_j})(m' \prod_{j \in M'} m_j)^{r_m}$$

Second stage: The adversary then performs a second series of queries which are treated in the same way as the first stage.

Guess: At the end of the simulation, the adversary outputs a guess γ' of γ.

If $\gamma' = \gamma$, $\mathcal{G}$ answers 1 indicating that $Z = e(g,g)^{abc}$; Otherwise, $\mathcal{G}$ answers 0 to the DBDH problem.

Probability of success: Now we have to assess $\mathcal{G}$'s probability of success. For the simulation to complete without aborting, we require the following conditions fulfilled:

（1） Extraction queries on an identity *ID* have $F(u) \neq 0 \bmod l_u$, where $u = H_u(ID)$.

（2） Signcryption queries on a message *m*, a signer list *L* and a receiver list L' have $F(u_i) \neq 0 \bmod l_u$, for some $i \in [1,n]$ where $ID_i \in L$.

（3） Unsigncryption queries on a ciphertext σ, a signer list *L* and a receiver list L' have $F(u_i') \neq 0 \bmod l_u$ for some $i \in [1,n']$ where $ID_i' \in L'$

（4） $F(u_j'^*) = 0 \bmod p$ for all $j \in [1,n']$, where $u_j'^* = H_u(ID_j'^*)$ and $K(m^*) = 0 \bmod p$ where $m^* = H_m(m_\gamma, L^*)$

Let $u_1, ..., u_{q_I}$ be the output of the hash function H_u appearing in queries not involving the challenge identity list L^*. Clearly, we will have $q_I \leq q_E + q_S + q_U$. Define the events

$A_i : F(u_i) \neq 0 \bmod l_u$ where $i = 1, ..., q_I$

A': $F(u_j'^*) = 0 \bmod p$ for all $j \in [1, n']$, where $u_j'^* = H_u(ID_j'^*)$

B^*: $K(m^*) = 0 \bmod p$ where $m^* = H_m(m_\gamma, L^*)$

Then the probability of ϑ not aborting is $\Pr[\overline{abort}] \geq \Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A' \wedge B^*]$

Since the function F and K are selected independently, therefore, the event $(\bigwedge_{i=1}^{q_I} A_i \wedge A')$ and B^* are independent. Assume $l_u(n_u + 1) < p$ which implies $0 \leq l_u n_u < p$. It is easy to see that $F(u) = 0 \bmod p \Rightarrow F(u) = 0 \bmod l_u$. Furthermore, this assumption implies that if $F(u) = 0 \bmod l_u$, there will be a unique k_u with $0 \leq k_u \leq n_u$ such that $F(u) = 0 \bmod p$. For the randomness of k_u, x' and X, we have

$$\begin{aligned}
&\Pr[A'] = \prod_{j=1}^{n'} \Pr[F(u_j'^*) = 0 \bmod p] \\
&= \prod_{j=1}^{n'} \Pr[F(u_j'^*) = 0 \bmod l_u] \Pr[F(u_j'^*) = 0 \bmod p \mid F(u_j'^*) = 0 \bmod l_u] \\
&= (\frac{1}{l_u} \frac{1}{n_u + 1})^{n'}
\end{aligned}$$

On the other hand, for any *i*, the event A_i and A' are independent, so we have

$$\begin{aligned}
&\Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A'] = \Pr[A'] \Pr[\bigwedge_{i=1}^{q_I} A_i \mid A'] = \Pr[A'](1 - \Pr[\bigvee_{i=1}^{q_I} \overline{A_i} \mid A']) \\
&\geq \Pr[A'](1 - \sum_{i=1}^{q_I} \Pr[\overline{A_i} \mid A']) = (\frac{1}{l_u} \frac{1}{n_u + 1})^{n'} (1 - \frac{q_I}{l_u}) \\
&\geq (\frac{1}{2(q_E + q_S + q_U)(n_u + 1)})^{n'} (1 - \frac{q_E + q_S + q_U}{2(q_E + q_S + q_U)}) \\
&= \frac{1}{2^{n'+1}((q_E + q_S + q_U)(n_u + 1))^{n'}}
\end{aligned}$$

Similarly, we have $\Pr[B^*] = \frac{1}{l_m} \frac{1}{n_m + 1}$

By combining the above result, we have

$$\Pr[\overline{abort}]$$
$$\geq \Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A' \wedge B^*]$$
$$\geq \frac{1}{2^{n'+2}((q_E+q_S+q_U)(n_u+1))^{n'} q_S(n_m+1)}$$

If the simulation does not abort, the adversary will win the game in definition 4 with probability at least ε. Thus B can solve for the DBDH problem instance with probability

$$\frac{\varepsilon}{2^{n'+2}((q_E+q_S+q_U)(n_u+1))^{n'} q_S(n_m+1)}$$

Theorem 3. *Under the CDH assumption, the proposed IASCfMR scheme is existentially unforgeable against adaptive chosen message attack.*

Proof. Assume that a EUF-IASCfMR-CMA forger for our scheme exists, we will construct a challenger ϑ, who runs the forger as a subroutine to solve an instance of CDH problem. ϑ is given a group *G*, a generator *g* and elements g^a and g^b. His goal is to compute g^{ab}.

Setup: ϑ first sets the public parameters using the Setup algorithm described in the previous proof. Note that in Setup phase, ϑ assigns $g_1 = g^a$ and $g_2 = g^b$. After ϑ defines functions $F(u), J(u), K(m), L(m)$ and public parameters u', m', u_i, m_j, we have $u'\prod_{i\in U'} u_i = g_2^{F(u)} g^{J(u)}$, $m'\prod_{j\in M'} m_j = g_2^{K(m)} g^{L(m)}$.

Queries: The forger can perform a polynomially bounded number of queries including private key extraction queries, signcryption queries, and unsigncryption queries. The challenger ϑ answers the forger in the same way as that of Theorem 2.

Forgery: Finally, if ϑ does not abort, the forger will return a new ciphertext $\sigma^* = (c^*, \sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, L^*)$ on message m^*, where m^* has never been queried.

Now, ϑ can unsigncrypt σ^* and obtain m^*. ϑ checks whether the following conditions are fulfilled:

（1） $F(u_j^*) = 0 \bmod l_u$ for all $j \in [1,n]$, where $u_j^* = H_u(ID_j^*)$

（2） $K(m^*) = 0 \bmod l_m$ where $m^* = H_m(m_\gamma, L^*)$

If not all the above conditions are fulfilled, ϑ will abort. Otherwise ϑ computes and outputs

$$\frac{\sigma_4^*}{R_1^{J(u_1^*)}....R_n^{J(u_n^*)}R_m^{L(m^*)}}=\frac{g_2^a\prod_{i=1}^{n}(U_i)^{r_i}\cdot(m'\prod_{j\in M^*}m_j)^{r_m}}{\prod_{i=1}^{n}g^{J(u_i^*)r_i}\cdot g^{L(m^*)r_m}}$$

$$=\frac{g_2^a\prod_{i=1}^{n}(g_2^{F(u_i^*)}g^{J(u_i^*)})^{r_i}\cdot(m'\prod_{j\in M^*}m_j)^{r_m}}{\prod_{i=1}^{n}g^{J(u_i^*)r_i}\cdot g^{L(m^*)r_m}}=g_2^a=g^{ab}$$

as the solution to the given CDH problem.

6. Conclusions

We have proposed an ID-bsed anonymous signcryption scheme for multiple receivers that satisfy the semantic security, unforgeability and signcrypter identity's ambiguity. To our best knowledge, this is the first IASCfMR that can be proven secure in the standard model. As we can see from the concrete scheme, the cost is linear with the size of group. It remains an open problem to construct a much more efficient scheme that is secure in the standard model with constant size signcryption ciphertext while removing all limitations on the size of group.

References

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+cost (encryption), in: Proc. Crypto 1997, LNCS 1294, Springer-Verlag, 1997: 165-179

[2] Shamir A. Identity-based cryptosystem and signature scheme, in: Proc. Crypto 1984, LNCS 196 Springer-Verlag, 1985: 120-126

[3] Malone-Lee J. Identity based signcryption, Cryptology ePrint Archive. Report 2002/098

[4] Libert B, Quisquator J. A new identity based signcryption scheme from pairings, in: Proc. IW 2003: 155-158

[5] Boyen X. Multipurpose identity based signcryption: a Swiss army knife for identity based cryptography, in: Proc. Crypto 2003, LNCS 2792, Springer-Verlag, 2003: 383-399

[6] Chen L, Malone-Lee J. Improved identity-based signcryption, in: Proc. PKC 2005, LNCS 3386, Springer-Verlag, 2005: 362-379

[7] Barreto P, Libert B, McCullagh N, et al. Efficient and provably-secure identity based signatures and signcryption from bilinear maps, in: Proc. Asiacrypt 2005, LNCS 3788, Springer- Verlag, 2005: 515-532

[8] Yu Y, Yang B, Sun Y, et al.Identity based signcryption scheme without random oracles, Computer Standards & Interfaces, 2009, 31(1), 56-62

[9] Rivest R, Shamir A, Tauman Y. How to leak a secret, in: Proc. Asiacrypt 2001. Berlin: Springer- Verlag, 2001: 552-565

[10] Huang X, Su W, Mu Y. Identity-based ring signcryption scheme: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world. In: Safavi-Naini, R., Seberry, J. (eds.) ACISP 2003. LNCS 2727, Springer-Verlag, 2003: 649-654

[11] Li F, Xiong H , Yu Y. An efficient id-based ring signcryption scheme, International conference on Communications, Circuits and Systems, ICCCAS 2008, 2008: 483-487

[12] Zhu Z, Zhang Y, Wang F. An efficient and provable secure identity based ring signcryption scheme, Computer Standards & Interfaces, 2008: 649-654

[13] Zhang J , Gao S, Chen H, et al. A novel ID-based anonymous signcryption scheme, in: Proc. APWeb/WAIM 2009, LNCS 5446, Springer-Verlag, 2009: 604-610

[14] Duan S, Cao Z Efficient and Provably Secure Multi-receiver Identity-based Signcryption, in: Proc. ACISP 2006, LNCS 4058, Springer-Verlag, 2006: 195-206

[15] Lal S, Kushwah P. Anonymous ID Based Signcryption Scheme for Multiple Receivers, Cryptology ePrint Archive: Report 2009/345, 2009. Available from: <http://eprint.iacr.org/2009/ 345>

[16] Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols, in: Proc. CCS 1993, 1993: 62-73

[17] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited (preliminary version), in: Proc. STOC 1998, 1998: 209-218

[18] Boneh D, Franklin M. Identity-based encryption from the Weil pairings, in: Proc. Cryptology- Crypto 2001, LNCS 2139 Springer-Verlag, 2001: 213-229

[19] Waters R. Efficient identity based encryption without random oracles, in: Proc. Eurocrypt 2005, LNCS 3494, Springer-Verlag, 2005: 114-127

[20] Paterson K G, Schuldt J C N. Efficient identity based signatures secure in the standard model, in: Proc. Information Security and Privacy-ACISP 2006, LNCS 4058, Springer-Verlag, 2006: 207-222

[21] Au M, Liu J, Yuen T, et al. ID-Based ring signature scheme secure in the standard model, in: Proc. IWSEC 2006. LNCS 4266, Springer-Verlag, 2006: 1-16