Anonymous ID Based Signcryption Scheme for Multiple Receivers

Sunder Lal and Prashant Kushwah
Department of Mathematics
Dr B. R. A. (Agra) University
Agra- 282002 (UP) - INDIA
E-mail: sunder_lal2@rediffmail.com, pra.ibs@gmail.com

Abstract: Anonymous signcryption is synonyms of ring signcryption which provides anonymity of the sender along with the advantages of signcryption. Multi receiver signcryption is suited for situation where a sender wants to send a message to multiple receivers in the confidential and authenticated way. This paper proposes an identity based anonymous signcryption scheme in multi-receiver setting. It also provides proofs of provable security of the proposed scheme under some computationally difficult problems.

Keywords: Signcryption, ring signcryption, multi-receiver signcryption, ID based cryptography

1. Introduction: The main advantages of public key cryptography are encryption and digital signature, used to achieve confidentiality and authenticity of a message respectively. There are scenarios where both primitives are needed (for example secure e-mailing). Earlier signature-then-encryption approach was followed to achieve both primitive. However, this approach has high computational cost and communication overhead. In 1997, Zheng [28] proposed a novel cryptographic primitive "Signcryption" which achieves both confidentiality and authenticity in a single logical step with the cost significantly lower than 'signature-then-encryption' approach. In 2002, Beak et al. [1] first formalized and defined security notions for signcryption via semantic security against adaptive chosen ciphertext attack and existential unforgeability against adaptive chosen message attack.

Shamir introduced the concept of identity based cryptography in 1984 [21] to remove the extra burden of digital certificates and key management from public key cryptography. The idea is that the public key of a user can be publicly computed from his unique public available information such as an e-mail address, an IP address or social security number etc while private key can be generated by a trusted private key generator (PKG). In 2001, Boneh and Franklin [5] gave the first practical identity based encryption scheme. The first identity based signcryption scheme was proposed by Malone-Lee [15] in 2003. He also considered security notions of signcryption in identity based setting. Since then quite a few identity based signcryption schemes have been proposed [3, 6, 7, 9, 14, 16].

The concept of multi-receiver setting was first formalized by Bellare et al. [4] for public key encryption i.e. if there are m receivers numbered 1, …, m and each of them generates for itself a private key and public key pair denoted by (sk_i, pk_i). A sender encrypts a message M using pk_i to obtain C_i for i = 1, …, m and then sends $(C_1, ..., C_m)$ as a ciphertext. Upon receiving the ciphertext, receiver i extracts C_i and decrypt it using sk_i. Beak et al. [2] formalized identity based encryption to the multi-receiver setting. Duan et al. [10] consider the situation where there are not only multiple receivers but also multiple senders. As an example, consider that there are several managers, each of whom wants to securely broadcast an e-mail to the employees of the company independently. Once an employee receives several ciphertexts from different managers, an issue of message authentication will arise. In such cases, confidentiality and authenticity required simultaneously. Motivated by this Duan et al. [10] gave the first multi-receiver identity based signcryption scheme. Later on some more multi-receiver identity based signcryption schemes were proposed in [18, 19, 23].

Ring signcryption or anonymous signcryption is a cryptographic primitive motivated from ring signature, which was first proposed by Rivest el al. [17]. Ring signature provides anonymity along with the authenticity in such a way that verifier does not know who has signed the message but he can verify that one of the person form the ring (group) has signed it. Ring signcryption enables a user to send a message confidentially and authentically to a specific receiver in an anonymous way. The first identity based ring signcryption was proposed by Huang et al. [11]. Some more identity based ring signcryption scheme are reported in [8, 12, 13, 20, 24, 25, 26, 27, 29, 30]. However, most of them are proved to be insecure and then improved in [20, 26, 22, 27].

In this paper we propose a multi receiver identity based anonymous signcryption scheme motivated from the following scenario: Consider the example [17, 20] where a member of cabinet wants to leak very important and juicy information regarding the president of the nation, to the press. He has to leak secrete in an anonymous way, else he will be spotted person in the cabinet. The press will not accept the information unless it is authenticated by one of the members of the cabinet. Here if the information is so sensitive and should not be leaked until the authorities in the press receive it, we should have confidential transmission of information. Thus we require anonymity to safeguard the cabinet member who sends the information, the information should be authenticated for the authorities in the press to consider it and it should be confidential until it reaches the hands of the right person in the press. All three properties are together achieved by ring signcryption. Here we point out the problems that can occurs (i) it will be dangerous to give the sensitive information to a single person (receiver), (ii) single receiver can be from malicious party and (iii) cabinet member wants to transmit the information to the different press authorities. In such cases it is desirable to transmit the information to multiple receivers. In such a scenario ring signcryption in multi-receiver setting is best suited.

2. Multi-receiver ID based Anonymous signcryption

First we give the formal definition of multi receiver ID based anonymous signcryption (MIBAS) scheme which is followed by the security model for MIBAS.

Definition: A multi receiver ID based anonymous signcryption (MIBAS) scheme consists of the following algorithms:

Setup: On input a security parameter k, Private Key Generator (PKG) runs this algorithm to generate master secrete key s and the system wide public parameters params which includes the description of finite message and ciphertext spaces. Further we assume params as input of following algorithm so we do not need to explicitly provide them to each algorithm

Extract: On input an identity ID of a user PKG runs this algorithm to generate users' public keys (Q_{ID}) and private key (D_{ID}).

Anonysigncrypt: A user ID_A runs this algorithm to send a message M to m receivers with identities $\{ID'_1,...,ID'_m\} = L'$ anonymously. This algorithm selects a group of n users' identities $\{ID_1,...,ID_n\} = L$ including the actual signcrypter ID_A, and outputs the ciphertext C.

Unsigncrypt: Upon receiving the ciphertext C, the receiver ID'_j runs this algorithm to recover M if the message was properly encrypted or signed otherwise it returns the error symbol $\perp$.

These algorithms must satisfy the standard consistency constraint

M = Unsigncrypt (C = (Anonysigncrypt $(M, D_A, ID'_j (1 \le j \le m), L, L')$), D'_j, L, L')

As in [10], a multi receiver anonymous signcrypted ciphertext is a combination of text part and receivers information part. Text part is same to the all receivers (including the information of sender group) and the receiver information part can be viewed an m-tuple where the j-th component is specific to receiver ID'_j. To unsigncrypt a ciphertext receiver ID'_j extract the text part and the j-th component from receivers' information part to recover M.

Security notions:

The widely accepted notion for message confidentiality and unforgeability of ID based signcryption are indistinguishable against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen message attacks, which were first considered by Malone-Lee [15]. Duan and Cao [10] extended these security notions to multi receiver setting under selective multi identity attack in which adversary is assumed to output ahead of time multiple identities that it wishes to attack. They refer these security notions as indistinguishability of ciphertexts under selective multi ID, chosen ciphertext attack (IND-sMIBSC-CCA) and strong existential unforgeability under selective multi-ID, chosen message attack (SUF-sMIBSC-CMA). Also anonymous signcryption has additional security notions via ciphertext anonymity against adaptive chosen ciphertext attacks, public authenticity and public verifiability. We adapt these notions in the setting of multi-receiver identity based anonymous signcryption.

Message confidentiality: An MIBAS scheme is indistinguishable against chosen ciphertext attacks (IND-sMIBAS-CCA2) if no probabilistic polynomially bounded adversary has a non-negligible advantage in the following game:

Setup: The challenger $\mathcal{B}$ runs this algorithm to produce a master key s and system wide public parameters "params". $\mathcal{B}$ gives params to the adversary $\mathcal{A}$ and keeps the master key s secrete. After receiving the params $\mathcal{A}$ outputs multiple target identities, denoted by $\{ID_1'^*,...,ID_m'^*\} = L'^*$

Phase1: The adversary $\mathcal{A}$ probes the challenger $\mathcal{B}$ with the following kind of queries adaptively

Extract queries: $\mathcal{A}$ produces an identity ID and gives it to the challenger $\mathcal{B}$. $\mathcal{B}$ runs this algorithm to computes the private key $D_{ID} = \mathrm{Extract}(s, ID)$ corresponding to ID. $\mathcal{B}$ returns D_{ID} to $\mathcal{A}$. A restriction here is that $ID \neq ID_j'^*$ for j = 1, …, m.

Anonysigncrypt queries: $\mathcal{A}$ generates a group of n identities $L = \{ID_1,...,ID_n\}$, a plaintext M and m receivers' identities $L' = \{ID_1',...,ID_m'\}$. $\mathcal{B}$ randomly chooses a user $ID_i \in L$, computes $D_i = \mathrm{Extract}(ID_i)$ and generates the ciphertext C = Anonysigncrypt $(M, D_i, ID_j'\ (1 \le j \le m),$ $L, L')$ and sends C to $\mathcal{A}$.

Unsigncrypt queries: $\mathcal{A}$ generates a group of identities $L = \{ID_1,...,ID_n\}$, a set of receivers' identities $L' = \{ID_1',...,ID_m'\}$ and a ciphertext C. $\mathcal{B}$ first chooses randomly a receiver ID_j' from L', computes the private key $D_j' = \mathrm{Extract}(s, ID_j')$, computes unsigncrypt (C, D_j', L, L') and returns M if C is a valid ciphertext otherwise returns $\perp$.

Challenge: $\mathcal{A}$ chooses two equal length messages $M_0, M_1 \in \mathcal{M}$, a group of identities $L^* = \bigcup_{i=1}^{n} ID_i^*$ on which he has not queried the key extraction oracle. $\mathcal{B}$ flips the coin to choose $b \in_R \{0,1\}$ and computes $C^* =$ $\mathrm{Anonysigncrypt}(M_b, D_i, ID_j'^*\ (\mathrm{for}\ 1 \le j \le m), L^*, L'^*)$, under private key of a sender ID_i chosen randomly from L^* and public key of attacked identities $ID_1'^*,...,ID_m'^*$. Then $\mathcal{B}$ send C^* to $\mathcal{A}$ as a challenge.

Phase 2: $\mathcal{A}$ issues new queries as in Phase 1. It can not ask unsigncrypt query on ciphertext C^* nor query the unsigncrypt oracle on an identity and a ciphertext C' which is only different from C^* in the receivers' information part. Also $\mathcal{A}$ can not ask the key extraction query on group L^*.

Guess: At the end of the game, $\mathcal{A}$ outputs a bit b' and wins if $b' = b$.

The adversary's success probability is defined as $\mathrm{Succ}^{\mathrm{IND-CCA2}}_{\mathrm{sMIBAS}}(\mathcal{A}) = \frac{1}{2} + \varepsilon$ where ε is required to be negligible in k.

Unforgeability: An MIBAS scheme is existentially unforgeable against adaptive chosen message attack (EUF-MIBAS-CMA) if no probabilistic polynomially bounded adversary has a non-negligible advantage in the following game:

Setup: The challenger $\mathcal{B}$ runs this algorithm to produce a master key s and system wide public parameters "param". $\mathcal{B}$ gives params to the forger $\mathcal{F}$ and keeps the master key s secrete.

Attack: $\mathcal{F}$ issues queries of same type as in message confidentiality game.

Forgery: Eventually $\mathcal{F}$ outputs a ciphertext C^* and m arbitrary receivers' identities $L'^* = \{ID'^*_1,...,ID'^*_m\}$. $\mathcal{F}$ wins the game if C^* is a valid ciphertext under some sender group $L^* = \{ID^*_1,...,ID^*_m\}$ and given m receivers' private keys i.e. the result of Unsigncrypt (C^*, D'^*_j, L^*, L'^*) is not the error symbol $\perp$ with the restrictions that $\mathcal{F}$ can not ask key extraction query on any group L^*, L'^* and C^* was not produced by Anonysigncrypt oracle.

Anonymity [27]: An MIBAS scheme is unconditionally anonymous if for any group of n members with identities $L = \{ID_1,...,ID_n\}$, the probability of any adversary to identify the actual signcrypter is not more than random guess's i.e. $\mathcal{A}$ 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.

Public Verifiability [27]: An MIBAS scheme is public verifiable if given a plaintext m and ciphertext C, and possible some additional information provided by the receiver, anyone can verify that C is a valid message of the sender without knowing the receiver's private key.

Public Authenticity [27]: An MIBAS scheme is public authenticable if anyone can verify that the validity and the origin of the ciphertext without knowing the content of the message and getting any help from receiver.

3. Preliminaries

Bilinear Pairing: Let $\mathbb{G}_1$ be an additive group and $\mathbb{G}_2$ be a multiplicative group both of the same prime order q. A function $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is called a **bilinear pairing** if it satisfies the following properties:

1. $\forall P, Q \in \mathbb{G}_1, \forall a, b \in \mathbb{Z}_q^*, e(aP, bQ) = e(P, Q)^{ab}$

2. For any $\mathcal{O} \neq P \in \mathbb{G}_1$, there is $Q \in \mathbb{G}_1$, such that $e(P, Q) \neq 1$.

3. There exists an efficient algorithm to compute $e(P, Q), \forall P, Q \in \mathbb{G}_1$.

CDH Problem: Given a generator P and two elements aP, bP of a group $\mathbb{G}_1$, the Computational Diffie-Hellman problem (CDH problem) in $\mathbb{G}_1$ is to compute abP.

DBDH Problem: Given two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of the same prime order q, a bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, a generator P of $\mathbb{G}_1$, three elements aP, bP, cP of $\mathbb{G}_1$ and an element $H \in \mathbb{G}_2$, the Decisional Bilinear Diffie-Hellman problem (DBDH problem) is to decide whether $H = e(P, P)^{abc}$.

4. The proposed scheme (MIBAS):

Setup: Given a security parameter k, PKG chooses two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of same order q (prime), a bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, a generator P of $\mathbb{G}_1$. PKG chooses his master key $s \in_R \mathbb{Z}_q^*$ (keeps secrete) and compute his public key $P_{pub} = sP \in \mathbb{G}_1$. It also chooses $R \in_R \mathbb{G}_1, R \neq \mathcal{O}$ and computes $g = e(R, P_{pub})$. The hash functions are set as $H_1 : \{0,1\}^* \to \mathbb{G}_1$, $H_2 : \mathbb{G}_2 \to \{0,1\}^t$ and $H_3 : \{0,1\}^t \times \mathbb{G}_1 \to \mathbb{Z}_q^*$ where t is the length of plaintext and ciphertext.

The system public parameters are param = $\{\mathbb{G}_1, \mathbb{G}_2, q, e, P, R, g, P_{pub}, H_1, H_2, H_3\}$

Key Extract: On receiving an identity $ID \in \{0,1\}^*$, PKG computes user's public key Q_{ID} = $H_1(ID)$ and the corresponding private key $D_{ID} = sQ_{ID}$.

Anonysigncrypt: Suppose the sender ID_S wants to send a message M anonymously to m different receivers $L^{'} = \{ID_1^{'}, ..., ID_m^{'}\}$. ID_S does the following

- Chooses a set of users $L = \{ID_1, ..., ID_n\}$ (including ID_S) different from $L^{'}$
- Picks $x_i \in_R \mathbb{Z}_q^*$ and computes $R_i = x_i P$ for i = 1, …, n ($i \neq S$)
- Picks $x_S \in_R \mathbb{Z}_q^*$ and computes $\alpha = \sum_{i=1}^{n} x_i$, $\omega = g^{\alpha}$ and $c = H_2(\omega) \oplus m$
- Computes $U = \alpha P$ and $T_j = \alpha(R + Q_j^{'})$ for j = 1, …, m
- Computes $h_i = H_3(c, R_i)$ and $R_S = x_S Q_S - \sum_{i=1, i \neq S}^{n} (R_i + h_i Q_i)$
- Computes $Z = (x_S + h_S) D_S$ where $h_S = H_3(c, R_S)$

The ciphertext is C = $(c, U, Z, R_1, ..., R_n, T_1, ..., T_m, L, L^{'})$.

Unsigncrypt: Upon receiving the ciphertext C = $(c, U, Z, R_1, ..., R_n, T_1, ..., T_m, L, L^{'})$, each receiver $ID_j^{'}$ uses his private key to decrypt C

- Computes $e(Z, P)$ and $e(P_{pub}, \sum_{i=1}^{n}(R_i + h_i Q_i))$ where $h_i = H_3(c, R_i)$ for i = 1, …, n
- If $e(Z, P) =$ $e(P_{pub}, \sum_{i=1}^{n}(R_i + h_i Q_i))$, computes $\omega' = e(P_{pub}, T_i) e(U, D_j^{'})^{-1}$ and recovers plaintext $M = c \oplus H_2(\omega')$. Otherwise outputs $\perp$ as failure.

Consistency:

$$\begin{aligned} e(Z, P) &= e((x_S + h_S) D_S, P) = e(x_S Q_S + h_S Q_S, P_{pub}) \\ &= e(\textstyle\sum_{i=1, i \neq S}^{n}(R_i + h_i Q_i) + R_S + h_S Q_S, P_{pub}) \\ &= e(\textstyle\sum_{i=1}^{n}(R_i + h_i Q_i), P_{pub}) \end{aligned}$$

and

$$\begin{aligned} \omega' &= e(P_{pub}, T_j) e(U, D_j^{'})^{-1} = e(sP, \alpha(R + Q_j^{'})) e(\alpha P, sQ_j^{'})^{-1} \\ &= e(P, R)^{s\alpha} e(P, Q_j^{'})^{s\alpha} e(P, Q_j^{'})^{-s\alpha} \\ &= e(P_{pub}, R)^{\alpha} = g^{\alpha} = \omega \end{aligned}$$

5. Security Analysis:

Theorem 1: (Message confidentiality) Assume that an IND-sMIBAS-CCA2 adversary $\mathcal{A}$ has an advantage ε against proposed scheme when asking q_{h_i} queries to random oracle H_i (i = 1, 2, 3) and q_s signcryption queries q_u unsigncryption queries. Then there is an algorithm $\mathcal{B}$ to solve the DBDH problem with an advantage $Adv(\mathcal{A}) \geq (\varepsilon - \frac{mq_u}{2^k})$.

Proof: We show how to build an algorithm $\mathcal{B}$ that solve DBDH problem with the help of an adversary $\mathcal{A}$. Let $\mathcal{B}$ receives a random instance (P, aP, bP, cP, h) of the DBDH problem, $\mathcal{B}$'s goal is to decide whether $h = e(P, P)^{abc}$ or not. To solve this problem $\mathcal{B}$ acts as $\mathcal{A}$'s challenger in the message confidentiality game. During the game $\mathcal{A}$ queries, $H_i\ (i = 1, 2, 3)$ oracles, anonysigncrypt oracle and unsigncrypt oracle. To handle $\mathcal{A}$'s queries, $\mathcal{B}$ maintains lists $L_i\ (i = 1, 2, 3)$ to $H_i\ (i = 1, 2, 3)$ queries for consistency purposes. We assume that for any ID, $\mathcal{A}$ will ask $H_1(ID)$ query before ID is used in any other query.

Setup: $\mathcal{B}$ sends system parameter params to $\mathcal{A}$ with $P_{pub} = cP$, $R = bP$, and $g = e(R, P_{pub})$ $= e(bP, cP) = e(P, P)^{bc}$. Then $\mathcal{A}$ outputs multiple target identities, denoted by $\{ID_1^{'*}, ..., ID_m^{'*}\} = L^{'*}$.

Phase 1: Now $\mathcal{A}$ starts probing the following queries

H_1 query for ID_k : $\mathcal{B}$ check the list L_1, if the tuple (ID_k, λ_k, Q_k) exists returns Q_k. Otherwise does the following:

- If $ID_k = ID_j^{'*}$ for some $j \in [1, m]$, chooses randomly $\lambda_j^{'*} \in \mathbb{Z}_q^*$ and computes $Q_j^{'*} = \lambda_j^{'*} P - R$
- Else chooses λ_k randomly from $\mathbb{Z}_q^*$, compute $Q_k = \lambda_k P$
- Store (ID_k, λ_k, Q_k) into L_1 and returns Q_k.

H_i (i = 2, 3) queries: To response these queries, $\mathcal{B}$ checks the corresponding list. If the query already exists, the same answer will be returned to $\mathcal{A}$. Otherwise $\mathcal{B}$ produce a random element from appropriate range and returned s an answer to $\mathcal{A}$, the query and the answer will then be added in the corresponding list.

Extract query for ID_k : $\mathcal{B}$ recovers (ID_k, λ_k, Q_k) from the list L_1, computes $D_k = \lambda_k P_{pub}$ $= c\lambda_k P$ and returns D_k to $\mathcal{A}$. Note that $\mathcal{A}$ can not ask the extract query for $ID_k = ID_j^{'*}$.

Anonysigncrypt query: $\mathcal{A}$ submit an anonysigncrypt query with a message M, a user group $L = \{ID_1, ..., ID_n\}$ and m arbitrary receivers $L' = \{ID'_1, ..., ID'_m\}$. There are two possibilities $L \neq L^{'*}$ or $L = L^{'*}$.

If $L \neq L^{'*}$ then $\mathcal{B}$ randomly chooses a user $ID_A \in L$ such that $ID_A = ID_j^{'*}$ for any j $= 1, ..., m$. Therefore $\mathcal{B}$ knows the secrete key of ID_A i.e. $D_A = \lambda_A P_{pub}$ from the list L_1 and runs anonysigncrypt algorithm with input m, D_A, ID'_j $(1 \leq j \leq m)$, L and L' to produces C. Finally $\mathcal{B}$ returns the ciphertext C to $\mathcal{A}$.

If $L = L^{'*}$ then $\mathcal{B}$ does the following

- Chooses randomly a user $ID_S^{'*} \in L^{'*} =$ L. Note that $Q_S^{'*}$ has been set to $\lambda_j^{'*} P - R$ for some $\lambda_S^{'*} \in \mathbb{Z}_q^*$
- Chooses randomly $x_1, x_2, ..., x_S, ..., x_n \in \mathbb{Z}_q^*$ and computes $\alpha = \sum_{i=1}^{n} x_i$, $\omega = g^{\alpha}$ and c = $H_2(\omega) \oplus M$
- For i = 1 to n, $i \neq S$, computes $R_i = x_i P$. Obtain the value $h_i = H_3(c, R_i)$ and store in the list L_3
- Computes $U = \alpha P$ and $T_j = \alpha(R + Q'_j)$ for $i = 1, ..., m$

- For i = S, chooses randomly $h_S \in \mathbb{Z}_q^*$, sets $R_S = x_S P - h_3 Q_S^{'*} - \sum_{i=1, i\neq S}^{n}(R_i + h_i Q_i^{'*})$ and $Z = x_S P_{pub}$. Adds the tuple (c, R_S, h_S) to L_3
- Finally $\mathcal{B}$ outputs the ciphertext $C = (c, Z, U, R_1, ..., R_n, T_1, ..., T_m, L^{'*}, L^{'})$.

Unsigncrypt query: $\mathcal{A}$ submit an unsigncrypt queries with a ciphertext $C = (c, Z, U, R_1, ..., R_n, T_1, ..., T_m, L^{'*}, L^{'})$.

If $L^{'} = L^{'*}$, $\mathcal{B}$ always return the ciphertext is invalid because $\mathcal{B}$ does not know the secrete key of any $ID_j^{'*} \in L^{'*}$. If this ciphertext is valid one, the probability that $\mathcal{A}$ will find is know more than $m/2^k$.

If for some j, $ID_j^{'} \neq ID_j^{'*} \in L^{'}$ $(1 \leq j \leq m)$, $\mathcal{B}$ find that the check equation $e(Z, P) = e(\sum_{i=1}^{n}(R_i + h_i Q_i),\ P_{pub})$ holds, then $\mathcal{B}$ find the secrete key corresponding to $ID_j^{'}$ from the list L_1, computes $\omega' = e(P_{pub}, T_i)e(U, D_j^{'})^{-1}$, $M^{'} = c \oplus H_2(\omega')$ and returns $M^{'}$. Otherwise $\mathcal{B}$ returns $\perp$ for invalid ciphertext.

Challenge: $\mathcal{A}$ outputs two message $M_0, M_1 \in \mathcal{M}$, n users group $L^* = \{ID_1^*, ..., ID_n^*\}$. Receivers set $L^{'*} = \{ID_1^{'*}, ..., ID_n^{'*}\}$ is attacked identities. $\mathcal{B}$ selects a random bit $b \in_R \{0,1\}$ and sets $U^* = aP$, $\omega = h$ (from DBDH problem tuple), $T_j^* = \lambda_j^{'*} U^*$ for j = 1, …, m (where $\lambda_j^{'*}$ corresponds to $ID_j^{'*}$ in L_1 list). Then $\mathcal{B}$ signcrypt the message M_b and sends the ciphertext $C^* = (c*, Z^*, U^*, R_1^*, ..., R_n^*, T_1^*, ..., T_m^*, L^*, L^{'*})$ to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ probes the new queries as in Phase 1. In the Phase 2, $\mathcal{A}$ cannot query the secrete key of any user in the group L^* and can not make unsigncrypt query to the ciphertext C^*. Also $\mathcal{A}$ can not make the unsigncryption query on a ciphertext C which is only different from C^* in the receiver information part.

At the end of the simulation, $\mathcal{A}$ produces a bit $b^{'}$ as a guess. At this moment if $b^{'} = b$, $\mathcal{B}$ answer 1 as a result of DBDH problem because his selection h satisfying

$$h = e(P_{pub}, T_j)e(U^*, D_j^{'*})^{-1} = e(cP, \lambda_j^{'*} U^*)e(U^*, D_j^{'*})^{-1} = e(cP,\ \lambda_j^{'*} aP)e(aP,\ \lambda_j^{'*} cP - cbP)^{-1}$$

$$= e(cP,\ \lambda_j^{'*} aP)e(aP,\ \lambda_j^{'*} cP)^{-1} e(aP, -cbP)^{-1} = e(P, P)^{abc}$$

otherwise $\mathcal{B}$ answer 0.

Probability of success: Now we determine the advantage of $\mathcal{B}$. The probability that $\mathcal{B}$ rejects the valid ciphertext for all q_U unsigncryption queries does not exceed $\frac{mq_u}{2^k}$. If $\mathcal{A}$ wins IND-sMIBAS-CCA2 game then we have

$$p_1 = \Pr[b^{'} = b \,|\, \text{Anonysigncrypt}(M_b, D_A^*, ID_j^{'*} (1 \leq j \leq m), L^*, L^{'*})] = \varepsilon + \tfrac{1}{2} - \frac{mq_u}{2^k}$$

$$p_2 = \Pr[b^{'} = i \,|\, h \in_R \mathbb{G}_2] = \tfrac{1}{2},\ (i = 0,\ 1)]$$

$$\text{Adv}(\mathcal{B}) = \left| \Pr_{a,\ b,\ c \in_R \mathbb{Z}_q^*,\ h \in_R \mathbb{G}_2}[1 \leftarrow \mathcal{B}(aP, bP, cP, h)] - \Pr_{a,\ b,\ c \in_R \mathbb{Z}_q^*}[1 \leftarrow \mathcal{B}(aP, bP, cP, e(P, P)^{abc})] \right|$$

$$\geq |p_1 - p_2| = (\varepsilon - \tfrac{mq_u}{2^k}).$$

Theorem 2: (Unforgeability) The multi-receiver anonymous signcryption scheme is existentially unforgeable against adaptive chosen-message and identity attacks (EUF-MIBAS-CMIA).

Proof: The proof is similar to the proof of Theorem 3 of [27]. If an adversary can forge a valid ciphertext of the proposed scheme, then he must be able to forge a valid Chow's ring signature [8]. That is if $\mathcal{A}$ can forge a valid ciphertext on message M, say $(c, U, Z, R_1,..., R_n, T_1, ..., T_m)$ for the sender's group L and receivers group $L^{'}$ then $\sigma^* = (Z, R_1,...,R_n)$ can be viewed as the Chow's ID based ring signature on message M = c of the ring L.

Theorem 3: (Anonymity) The multi-receiver anonymous signcryption scheme has full anonymity.
Proof: The proof is similar to the proof of Theorem 2 of [27].

Theorem 4: (Public authenticity) The multi-receiver anonymous signcryption scheme is public authenticable.
Proof: The proof is similar to the proof of Theorem 4 of [27].

6. Conclusion: We have proposed an identity based ring signcryption scheme for multiple receiver. We have shown that the proposed scheme has message confidentiality, unforgeability, anonymity and public authenticity. The proof of message confidentiality depends upon the hardness of DBDH problem while the proof for unforgeability follows directly from the Chow et el ID based ring signature scheme [8].

References:

1. J. Baek, R. Steinfeld, Y. Zheng: Formal proofs of security of signcryption, PKC 02, LNCS # 2274, pp. 81-98, 2002
2. J. Baek, R. Safavi-Naini and W. Susilo: Efficient multi-receiver identity based encryption and its application to broadcast encryption, PKC 05, pp. 380-397, 2005.
3. P. S. L. M. Barreto, B. Libert, N. McCullagh and J. J. Quisquater: Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, Asicrypto'05, LNCS 3788, pp. 515-532, Springler-Verlag, 2005.
4. M. Bellare, A. Boldyreva and S. Micali: Public key encryption in a multi-user setting: Security proofs and improvements, EUROCRYPT' 2000, LNCS # 1807, pp. 259-274, Springler-Verlag, 2000.
5. D. Boneh and M. Franklin: Identity–based encryption scheme from Weil pairing. CRYPTO 2001, LNCS # 2139, Springer-Verlag, 2001, 213-229.
6. X. Boyen: Multipurpose Identity based signcryption: A Swiss army knife for identity based cryptography. CRYPTO 2003, LNCS # 2729, pp. 389-399, Springer-Verlag, 2003.
7. L. Chen and J. Malone-Lee: Improved identity-based signcryption. PKC 2005, LNCS # 3386, pp. 362-379, Springer-Verlag, 2005.
8. S. S. M. Chow, L. C. K. Hui and S. M. Yiu: Efficient identity based ring signature, Proc. of ACNS 2005 Springer-Verlag pp. 499-512, 2005.
9. S. S. M. Chow, S. M. Yiu, L. C. K. Hui and K. P. Chow: Efficient forward and provably secure ID based signcryption scheme with public verifiability and public cipher text authenticity. ICISC'2003, LNCS # 2971, pp. 352-369, Springer-Verlag, 2003.
10. S. Duan and Z. Cao: Efficient and provably secure multi receiver identity based signcryption. ACISP 2006, LNCS # 4058, pp. 195-206, Springer-Heidelberg, 2006.
11. X. Huang, W. Susilo, Y. Mu and Futai Zhang: Identity based ring signcryption scheme: Cryptographic primitive for preserving privacy and authenticity in the ubiquitous world, International Conference on Advance Information Networking and Applications (AINA'05) Vol. 2 (INA, USW, WAMIS and IPv6 papers) pp. 649-654, 2005.
12. F. Li, M. Shirase and T. Takagi: Analysis and improvement of authenticatable ring signcryption scheme, Journal of Shanghai Jiaotong University (Science), Vol. 13, pp 679-683, 2008.
13. F. Li, H. Xiong and Y. Yu: An efficient id-based ring signcryption scheme, International coference on Communications, Circuits and Systems, ICCCAS'08 pp. 483-487, 2008.

14. B. Libert and J. J. Quisquater: New identity based signcryption schemes from pairings, IEEE Information Theory Workshop, Paris, France, http://eprint.iacr.org/2003/023, 2003.
15. J. Malone-Lee: Identity-based signcryption, Cryptology ePrint Archive Report 2002/098.
16. D. Nalla and K. C. Reddy: Signcryption scheme for identity based cryptosystems. Cryptology ePrint Archive, Report 2003/066, http://eprint.iacr.org/2003/066.pdf, 2003.
17. R. L. Rivest, A Shamir and Y. Tauman: How to leak a secret, ASIYACRYPT 2001, LNCS # 2248, pp. 552-565, 2001.
18. S. S. D. Selvi, S. S. Vivek, R. Gopalkrishnan, N. N. Karuturi and C. P. Rangan: Cryptanalysis of id based signcryption scheme for multiple receivers. http://eprint.iacr.org/200/238.pdf, 2008.
19. S. S. D. Selvi, S. S. Vivek, R. Srinivasan, and C. P. Rangan: An Efficient Identity-based signcryption schemes for multiple receivers, Cryptology ePrint Archive, Report 2008/341, http://eprint.iacr.org/2008/341.pdf, 2008.
20. S. S. D. Selvi, S. S. Vivek, and C. P. Rangan: On the security of identity based ring signcryption schemes, Cryptology ePrint Archive, Report 2009 /144, http://eprint.iacr.org/ 2009/144.pdf, 2009.
21. A. Shamir: Identity-based cryptosystems and signature schemes. CRYPTO 84, LNCS # 196, pp 47-53 Springer-Verlag, 1984.
22. S. S. Vivek, S. S. D. Selvi, and C. P. Rangan: Cryptanalysis of ring signature and ring signcryption schemes, Cryptology ePrint Archive, Report 2009 /052, http://eprint.iacr.org/ 2009/052.pdf, 2009.
23. Y. Yu, Y. Bo, H. Xinyi and Z. Mingwu: Efficient identity based signcryption scheme for multiple receiver, ATC 2007, LNCS # 4610, pp. 13-21 Springer-Verlag, 2007.
24. Y. Yu, F. Li, C. Xu and Y. Sun: An efficient identity based anonymous signcryption scheme, Wuhan University Journal of Natural Sciences, Vol. 13, pp. 670-674, 2008.
25. J. Zhang and S. Gao, H. Chen and Q. Geng: A novel ID-based anonymous signcryption scheme, Q. Li et al (Eds.): APWeb/WAIM 2009, LNCS # 5446, pp. 604-610, 2009.
26. M. Zhang, B. Yang, S. Zhu and W. Zhang: Efficient secret authenticatable anonymous signcryption, Computer Standard & Interfaces Journal, 2008.
27. M. Zhang, Y. Zhong, P. Li and B. Yang: Analysis and enhance of anonymous signcryption model, Cryptology ePrint Archive, Report 2009 /194, http://eprint.iacr.org/ 2009/194.pdf, 2009.
28. Y. Zheng: Digital signcryption or how to achieve cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption), CRYPTO'97, LNCS # 1294, pp. 165-179, Springer-Verlag, 1997.
29. Z. Zhu, Y. Zhang and F. Wang: An efficient and provable secure identity based ring signcryption scheme. In Computer Standards & Interfaces, pp. 649-654, http://dx.doi.org/10. 1016/j.csi.2008.09.023, 2008.
30. L. Zhun and F. Zhang. Efficient ID-based ring signature and ring signcryption schemes. In International Conference on Computational Intelligence and Security, 2008. CIS ’08., Vol. 2, pp. 303–307, 2008.