Analysis and Enhance of Anonymous Signcryption Model

Mingwu Zhang[1,2], Yusheng Zhong[1], Pengcheng Li[1], and Bo Yang[1]

[1]Department of Computer Science and Engineering,
College of Informatics,
South China Agricultural University, Guangzhou, 510642, China
[2] National Laboratory for Modern Communications, Chengdu, 610041, China
Email: `csmwzhang@gmail.com, byang@scau.edu.cn`

Abstract. Ring signcryption, a cryptographic primitive to protect security and privacy, is an encryption and authentication scheme in a single logical step which allows a user to anonymously signcrypt a plaintext on behalf of a group of users that decrypter cannot know who is the actual signcrypter. In 2009, Zhang, Gao, Chen and Geng proposed a novel anonymous signcryption scheme(denoted as the ZGCG scheme) which is more efficient in computational cost and ciphertext length than the related schemes. In this paper, however, we show that the ZGCG scheme has not anonymity secure for the receiver, and then we propose an improved anonymous signcryption scheme that remedies the weakness of the ZGCG scheme. Our proposed scheme satisfies the semantic security, unforgeability, signcrypter identity's ambiguity, and public authenticity. We also give the formal security proof in the random oracle model.

Keywords: anonymous signcryption, bilinear pairings, unforgeability, anonymity

1 Introduction

The concept of signcryption was first proposed by Zheng [1] that is a cryptographic primitive to performs signature and encryption simultaneously, at a lower computational costs and communication overheads than the traditional the signature-then-encryption approach. Followed by the first constructions given in [1], a number of new schemes and improvements have been proposed [2–5]. Recently, a formal security proof model for signcryption scheme is formalized in [6]. To achieve simple and safe non-repudiation procedure, Bao and Deng [2] introduced a signcryption scheme that can be verified by a sender's public key. A distinguishing property of ID-based cryptography is that a user's public key can be any binary string that can identify the user's identity, while private keys can be generated by the trusted Private Key Generator(PKG). Several ID-based signcryption schemes have been proposed [7–11].

Ring signcryption [12, 13, 15] is an important method to realize the signcrypter identities' ambiguity that motivated by ring signature [14]. The receiver 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. To obtain that the signcrypter can authenticate the ciphertext was produced by himself, an authenticable anonymous signcryption was proposed in [15] which extend an authentication algorithm to let sender prove that the ciphertext is produced by himslef. In [16], Zhang et. al proposed a novel anonymous signcryption scheme(we called ZGCG scheme) that is more efficient. In this paper, however, we show that the ZGCG scheme is not anonymous for the decrypter nor public authenticable or verifiable for the third party. Furthermore, we propose an improved scheme that remedies the weakness of the ZGCG scheme. The improved scheme has the security notions such as confidentiality, unforgeability, signcrypter identities ambiguity, and public authenticity.

RoadMap. The rest of this paper is organized as follows: Section 2 gives a formal ID-based anonymous signcryption scheme and its security notions. The ZGCG scheme and its security analysis is described in 3. An improved scheme is proposed in section 4 and its security is given in section 5. At last the conclusion is drawn in section 6.

2 Formal Model of ID-based Anonymous Signcryption Scheme

In this section, we will describe the outline and the security requirements of ID-based anonymous signcryption scheme. An ID-based anonymous signcryption scheme consists of four algorithms: Setup, KeyExtract, AnonySigncrypt, and Unsigncrypt.

- Setup: Take an input 1^k, where k is a security parameter, the algorithm generates a master key s and the system's public parameters $params$, which include a description of a finite message space together with a description of a ciphtertext space.
- KeyExtract: Given an identity string $ID \in \{0,1\}^*$, and system master key s, this algorithm outputs the private key associated with the ID, denoted by D_{ID}.
- AnonySigncrypt: If a user A identified by ID_A wishes to send a message m to B identified by ID_B ,this algorithm selects a group of n users' identities by $Ł = \bigcup ID_i (1 \leq i \leq n)$ including the actual signcrypter ID_A , and outputs the ciphertext C.
- Unsigncrypt: When user B receives the cipertext C, this algorithm takes the ciphertext C, Ł, and B's private key D_B as input, and outputs plaintext m when unsigncryption is successful, otherwise it outputs $\perp$.

The algorithms must satisfy the standard consistency constraint of ID-based signcryption scheme as following

$$C = \text{AnonySigncrypt}(m, Ł, D_A, ID_B) \Rightarrow \text{Unsigncrypt}(C, Ł, D_B) = m$$

2.1 Security Notions

The security of ID-based signcryption scheme was first defined by Malone-Lee [4, 10] that satisfies *indistinguishable against adaptive chosen ciphertext attacks* and *unforgeability against adaptive chosen message attacks.* The anonymous signcryption scheme extends the security about *ciphertext anonymity against adaptive chosen ciphertext attacks*, and *public authenticity* and *public verifiability.*

Definition 1. *(*Confidentiality*) An ID-based anonymous signcryption scheme is indistinguishabe against adaptive chosen ciphertext attacks (IND-IDAS-CCA2) if no polynomially bounded adversary has a non-negligible advantage in IDAS game.*

We define the IDAS game played by a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as following:

- Inital: The challenger $\mathcal{B}$ runs Setup algorithm with security parameter k, keeps master key s and gives the *params* to the adversary.
- Phasei-I: The adversary $\mathcal{A}$ performs a series of following queries in an adaptive fashion:
  KeyExtract queries: $\mathcal{A}$ produces an identity ID, $\mathcal{C}$ computes the private key $D_{ID} = \textsc{KeyExtract}(ID)$ to respond to $\mathcal{A}$.
  AnonySigncrypt queries: $\mathcal{A}$ generates a group of n identities $Ł = \{ID_i\}$ (i=1,...,n), a plaintext m and a designated receiver ID_B. $\mathcal{B}$ randomly chooses a user $\mathcal{U}_i \in \{ID_i\}$, computes $D_i = \textsc{KeyExtract}(ID_i)$ and generates ciphertext $C = \textsc{AnonySigncrypt}(m, Ł, D_i, ID_B)$ and sends C to $\mathcal{A}$.
  Unsigncrypt queries: $\mathcal{A}$ chooses a group of identities $Ł = \{ID_i\}$ (i=1,..,n), a receiver identity ID_r and a ciphertext C. $\mathcal{B}$ first generates the privacy key $D_r = \textsc{KeyExtract}(ID_r)$, computes $\textsc{Unsigncrypt}(\{ID_i\}, C, D_r)$, then returns the result to $\mathcal{A}$. This result may be the $\perp$ if C is an invalid ciphertext for ID_r.
- Challenge: $\mathcal{A}$ chooses two plaintexts $m_0, m_1 \in \mathcal{M}$, a group of identities $Ł^* = ID_i^*$ (i=1,...,n), and a designated receiver ID_B^* on which he wishes to be challenged. The challenger $\mathcal{B}$ picks a random $b \in \{0, 1\}$ and computes $C^* = \textsc{AnonySigncrypt}(m_b, Ł^*, ID_B^*)$ and sends C^* to $\mathcal{A}$.
- Phase-II: $\mathcal{A}$ can ask a series number of queries adaptively again as in the first stage with the restriction that he cannot make the KeyExtract query on group $Ł^*$ member nor ID_B^*, and he cannot make the Unsigncrypt query on ciphertext C^*.
- Output: Finally, $\mathcal{A}$ outputs a bit b' and wins the game if $b' = b$.

The adversary $\mathcal{A}$'s advantage is defined as $Adv(\mathcal{A}) = \left|2Pr[b' = b] - 1\right|$.

Definition 2. *(*Anonymity*) An ID-based anonymous signcryption scheme is unconditional anonymous if for any group of n members with identities $L = \bigcup ID_i (1 \leq i \leq n)$, any adversary cannot identify the actual signcrypter with probability better than random guess's.*

That is, $\mathcal{A}$ outputs the identity of actual signcrypter with probability $1/n$ if he is not the member of Ł, and with probability $1/(n-1)$ if he is the member of Ł.

Definition 3. *(*Unforgeability*) An ID-based anonymous signcryption scheme is existentially unforgeable against adaptive chosen-message attacks and adaptive chosen-identity attacks(EUF-IDAS-CMIA) if no polynomially bounded adversary has a non-negligible advantage in the following game:*

- The challenger $\mathcal{C}$ runs the SETUP algorithm with a security parameter k and gives the public parameters to adversary $\mathcal{A}$.
- $\mathcal{A}$ performs a polynomially bounded phase-I queries in IDAS game.
- Finally, $\mathcal{A}$ outputs a cipertext C^* and wins the game if: (1)The C^* is a valid ciphertext under the group users Ł and receiver ID^* such that the result of the UNSIGNCRYPT(C^*, Ł*, ID^*) is not the $\perp$ symbol; (2)C^* was not produced by ANONYSIGNCRYPT oracle; (3)Group Ł identities were not performed KEYEXTRACT queries.

Definition 4. (Public verifiability) *An ID-based anonymous signcryption scheme is publicly verifiable if given a plaintext m and ciphertext C, and possibly 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.*

Definition 5. (Public authenticity) *An ID-based anonymous signcryption scheme is publicly 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 the receiver.*

3 Analysis of the ZGCG scheme

In this section, we review the ZGCG scheme [16], and demonstrate that the ZGCG scheme is neither anonymous in sender identity for the decrypter nor public authenticable or verifiable for a third party.

3.1 Review of the ZGCG scheme

The ZGXCG scheme is described as follow four algorithms.

1. SETUP Given a security k, the PKG chooses bilinear map groups (G_1, G_2) of order $q > 2^k$, bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. Let P be a generator of G_1. It randomly chooses a master key $s \in Z_q^*$ and computes $P_{pub} = sP$ as the corresponding public key. Next, PKG chooses cryptography hash functions: $H_1 : \{0,1\}^* \to \mathbb{G}_1^*$, $H_2 : \mathbb{G}_2 \to \{0,1\}^n$, $H_3 : \{0,1\}^n \times G_2 \to Z_q$, $H_4 : \{0,1\}^* \times G_1 \times \{0,1\}^* \to G_1$. The system public parameters are
   $params = \{G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3, H_4\}$.
2. KEYEXTRACT Given an identity ID, PKG computes user public key $Q_{ID} = H_1(ID)$ and corresponding secret key $D_{ID} = sQ_{ID}$.

3. AnonySigncrypt Let Ł $= \bigcup\{\mathcal{U}_i\}$ (i=1,...,n) be a set of users including the actual signcrypter $ID_S (S \in [1, n])$. To signcrypt a message m on behalf of the group Ł to receiver ID_B, the signcrypter ID_S executes as follows:
   - For $i = 1, ..., n(i \neq s)$, randomly picks $x_i \in_R Z_q^*$ to computes $R_i = x_i P$;
   - Randomly chooses $x_s \in_R Z_q^*$ to compute $\omega = e(P_{pub}, \sum_{i=1}^n x_i Q_B)$, and sets $R_s = x_s P - \sum_{i=1,i\neq s}^n (H_3(R_i, \omega)Q_i + R_i)$;
   - Computes $c = H_2(\omega) \oplus m$, and $U = \sum_{i=1}^n x_i P$;
   - Computes $S = \sum_{i=1}^n x_i H_4(L, U, m) + x_s P_{pub} + H_3(R_s, \omega)D_s$;
   - Finally, outputs the ciphertext of message m as $C = (c, S, U, R_1, ..., R_n)$.
4. Unsigncrypt Upon receiving the cipertext $C = (c, S, U, R_1, ..., R_n)$, ID_B uses his secret key D_B to recover and verify the massage as follows:
   - Computes $\omega = e(U, D_B)$, and $m = c \oplus \omega$;
   - Accepts the message iff the following equation holds:
     $e(S, P) = e(U, H_4(L, U, m))e(P_{pub}, \sum_{i=1}^n (R_i + H_3(R_i, \omega)Q_i))$

3.2 Security and Anonymity Analysis

We now show the ZGCG scheme is neither anonymous for the ciphertext unsigncrypter nor publicly authenticable or verifiable for a third party.

1.Anonymity analysis. Only S and R_s contain signcrypter ID_S and group L users identity information in ciphertext $C = (c, S, U, R_1, ..., R_n)$. We show that $S = \sum_{i=1}^n x_i H_4(L, U, m) + x_s P_{pub} + H_3(R_s, \omega)D_s$ leaks the actual signcrypter identity ID_S. We have

$$\begin{aligned} e(S, P) &= e(\textstyle\sum_{i=1}^n x_i H_4(L, U, m) + x_s P_{pub} + H_3(R_s, \omega)D_s, P) \\ &= e(\textstyle\sum_{i=1}^n x_i H_4(L, U, m), P)e(x_s P_{pub} + H_3(R_s, \omega)D_s, P) \\ &= e(U, H_4(L, U, m))e(x_s P + H_3(R_s, \omega)Q_s, P_{pub}) \end{aligned}$$

The designcrypter ID_B can get the value ω by $e(U, D_B)$, and check whether the user $\mathcal{U}_j (1 \leq j \leq n)$ is the actual signcrypter by checking the following equation:

$$e(x_j P + H_3(R_j, \omega)Q_j, P_{pub}) = e(S, P)e(U, H_4(L, U, m))^{-1}$$

It is only the actual signcrypter ID_S who can pass through the above checking equation because it has the generated equation $R_s = x_s P - \sum_{i=1,i\neq s}^n (H_3(R_i, \omega)Q_i + R_i)$ in AnonySigncrypt algorithm. The other user in Ł cannot pass through the checking equation because his x_i is randomly picked from Z_q^*, and $R_i = x_i P$ is uniformly distributed in G_1.

2. Public verifiability and authenticity analysis. We show that the ZGCG scheme is neither public verifiable nor public authenticable. The verification equation $e(S, P) = e(U, H_4(L, U, m))e(P_{pub}, \sum_{i=1}^n (R_i + H_3(R_i, \omega)Q_i))$ needs receiver's decrypting agreeing key ω. If a third party want to check the equation, he must obtain the ω. It cannot provide public verifiability. If the decrypting receiver sends ω to a third party, it cannot provide the confidentiality in this scheme because the third party can decrypt the plaintext by $m = c \oplus \omega$. So the decrypting receiver cannot leak ω to any third party so that the scheme is not public authenticable.

4 Improved Anonymous Signcryption Scheme

To overcome the weakness of the ZGCG scheme, we improve the anonymous signcryption in this section.

1. Setup Given a security k, the PKG chooses groups G_1 and G_2 of prime order $q > 2^k$ (with G_1 additive and G_2 multiplicative), bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, a generator P of G_1. It randomly picks a master key $s \in Z_q^*$ and computes $P_{pub} = sP$. Next, PKG chooses hash functions: $H_1 : \{0,1\}^* \to \mathbb{G}_1^*$, $H_2 : \mathbb{G}_2 \to \{0,1\}^n$, $H_3 : \{0,1\}^l \times G_1 \to Z_q^*$, where n and l is plaintext and ciphertext length. The PKG keeps the master key s and public system parameters
   $params = \{G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3, H_4\}$.
2. KeyExtract Given an identity ID, PKG computes user public key $Q_{ID} = H_1(ID)$ and corresponding secret key $D_{ID} = sQ_{ID}$.
3. AnonySigncrypt Let $\text{Ł} = \bigcup\{\mathcal{U}_i\}$ (i=1,...,n) be a set of users including the actual signcrypter ID_S. To signcrypt a message m on behalf of the group Ł to receiver ID_B, ID_S executes as follows:
   - For $i = 1, ..., n(i \neq s)$, randomly picks $x_i \in Z_q^*$ to computes $R_i = x_i P$;
   - Randomly picks $x_s \in Z_q^*$ to compute $\omega = e(P_{pub}, \sum_{i=1}^n x_i Q_B)$, and sets $c = H_2(\omega) \oplus m$;
   - Computes $R_s = x_s Q_s - \sum_{i=1, i\neq s}^n (H_3(c, R_i)Q_i + R_i)$, and $U = \sum x_i P$;
   - Computes $S = (x_s + H_3(c, R_s))D_s$;
   - Finally, outputs the ciphertext $C = (c, S, U, R_1, ..., R_n)$.
4. Unsigncrypt Upon receiving the cipertext $C = (c, S, U, R_1, ..., R_n)$, ID_B uses his secret key D_B to recover and verify the massage as follows:
   - Checks whether $e(S, P) = e(P_{pub}, \sum_{i=1}^n (R_i + H_3(c, R_i)Q_i))$. If the equation holds, computes $\omega' = e(U, D_B)$, then recovers plaintext $m = c \oplus H_2(\omega')$; otherwise outputs $\perp$ as failure.

5 Correctness and Security Analyzes

5.1 Correctness

If the ciphertext C is generated in the way described as above algorithm, it has $\omega' = e(U, D_B) = e(\sum_{i=1}^n x_i P, D_B) = e(sP, \sum_{i=1}^n x_i Q_B) = \omega$
Furthermore,

$$\begin{aligned} e(S,P) &= e((x_s + H_3(c,R_i))D_s, P) = e((x_s Q_s + H_3(c,R_i)Q_s, P_{pub}) \\ &= e(\textstyle\sum_{i=1,i\neq s}^n (H_3(c,R_i)Q_i + R_i) + R_s + H_3(c,R_i)Q_s, P_{pub}) \\ &= e(\textstyle\sum_{i=1}^n (H_3(c,R_i)Q_i + R_i), P_{pub}) \end{aligned}$$

5.2 Security

Theorem 1. (Confidentiality) *In the random oracle model, if there is an IND-IDAS-CCA2 adversary $\mathcal{A}$ who can distinguish ciphertexts from the users set $\bigcup\{\mathcal{U}_i\}$ with an advantage ϵ when running in at most q_{H_i} queries to $H_i (1 \leq i \leq 3)$ hashes, at most q_E key extract queries, q_S signcryption queries, q_U unsigncryption queries. Then, there exists another algorithm $\mathcal{B}$ that can solve a random instance of the DBDH problem with an advantage $Adv(\mathcal{B}) \geq (\epsilon - \frac{q_U}{2^k})/q_{H_0}^2$.*

Proof. Let the distinguisher $\mathcal{B}$ receives a random instance (P, aP, bP, cP, h) of the DBDH problem whose goal is to decide whether $h = e(P,P)^{abc}$ or not. In order to solve this problem, $\mathcal{B}$ runs $\mathcal{A}$ as a subroutine and act as $\mathcal{A}$'s challenger in the *IDAS* game. We assume that: (1)$\mathcal{A}$ will ask for $H_1(ID)$ before ID is used in any other queries; (2)$\mathcal{A}$ never makes an UNSIGNCRYPT query on a ciphertext obtained from the ANONYSIGNCRYPT oracle, and he can only make UNSIGNCRYPT queries for or guessed ciphertext.

Setup: At first, $\mathcal{B}$ sets $P_{pub} = cP$ as system public key and sends *params* to $\mathcal{A}$ after running the SETUP algorithm with parameter k. The value c is unknown to $\mathcal{B}$ and is used as the role of the PKG's master key.

Queries-I: For the key extraction and the signcryption/unsigncryption on the message m, $\mathcal{B}$ simulates the hash oracles(H_1, H_2, H_3), KEYEXTRACT oracle, ANONYSIGNCRYPT oracle, and UNSIGNCRYPT oracle. $\mathcal{A}$ can perform its queries adaptively in which every query may depend on the answers according to the previous ones.

H_1 queries. To response these queries, $\mathcal{B}$ maintains the list L_1 of tuples (ID, b). When $\mathcal{A}$ queries the oracle H_1, $\mathcal{B}$ chooses a random number $j \in \{1, ..., q_{H_1}\}$. At the jth H_1 query, $\mathcal{B}$ answers by $H_1(ID_j) = bP$, otherwise for queries $H_1(ID_e)$ with $e \neq j$, $\mathcal{B}$ chooses $b_e \in_R Z_q^*$, answers $H_1(ID_e) = b_eP$ and accords the pair (ID_e, b_e) in list L_1.

H_2, H_3 queries. When $\mathcal{A}$ asks queries on these hash values, $\mathcal{B}$ checks the corresponding lists. If an entry for the query is found, the same answer will be given to $\mathcal{A}$; otherwise, a randomly generated value will be used as an answer to $\mathcal{A}$, the query and the answer will then be recorded in the lists.

KEYEXTRACT queries. When $\mathcal{A}$ asks a query KEYEXTRACT(ID_i), $\mathcal{B}$ first searches the corresponding tuple (ID_i, b_i) in L_1. If $ID_i = ID_j$, $\mathcal{B}$ fails and stops. Otherwise, $\mathcal{B}$ computes the secret key $D_i = b_iP_{pub} = cb_iP$ and returns D_i to $\mathcal{A}$.

ANONYSIGNCRYPT queries. $\mathcal{A}$ can perform a ANONYSIGNCRYPT queriy for a plaintext m, a user group $L = \bigcup\{\mathcal{U}_i\}$ and a designated receiver with identity ID_B.

- $\mathcal{B}$ randomly chooses a user $\mathcal{U}_A \in L$ whose identity is $ID_A (ID_A \neq ID_j)$. $\mathcal{B}$ can compute $\mathcal{U}_A$'s secret key $D_A = b_AP_{pub}$ where b_A is in the corresponding tuple (ID_A, b_A) in L_1;
- $\mathcal{B}$ runs ANONYSIGNCRYPT (m, L, D_A, ID_B) to signcrypt a message m on behalf the group L using $\mathcal{U}_A$'s private key D_A;
- At last, $\mathcal{B}$ returns the result C to $\mathcal{A}$.

UNSIGNCRYPT queries. At any time, $\mathcal{A}$ can perform an UNSIGNCRYPT query for a ciphertext $C = (c, S, U, R_1, ..., R_n)$ between the group L and the receiver ID_B.

- If $ID_B = ID_j$, $\mathcal{B}$ always returns $\mathcal{A}$ that the ciphertext is invalid, because $\mathcal{B}$ does not know ID_j's secret key in KEYEXTRACT oracle. If this ciphertext is a valid one, the probability that $\mathcal{A}$ will find is no more than 2^{-k};
- If $ID_B \neq ID_j$, the equation $e(S, P) = e(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_i))$ holds, $\mathcal{B}$ computes $\omega = e(U, D_B)$, $m' = c \oplus H_2(\omega)$ and returns m'. Otherwise $\mathcal{B}$ notifies $\mathcal{A}$ that the ciphertext is invalid with symbol $\perp$;
  For all q_U UNSIGNCRYPT queries, the probability to reject a valid ciphertext does not exceed $q_U/2^k$.

Challenge: After performing a series number of queries-I, $\mathcal{A}$ chooses two message $m_0^*, m_1^* \in \mathcal{M}$, n users $Ł^* = \{ID_1^*, ..., ID_n^*\}$ and a receiver ID_B^*. If $ID_B^* \neq ID_j$, $\mathcal{B}$ fails and stops. $\mathcal{B}$ chooses $b \in_R \{0, 1\}$ and let $U^* = aP, \omega = h(h$ is $\mathcal{B}$ candidate for the DBDH problem). Then $\mathcal{B}$ signcrypts the message m_b^* as described in the ANONYSIGNCRYPT request and sends the ciphertext $C^* = (c^*, S^*, U^*, R_1^*, ..., R_n^*)$ to $\mathcal{A}$.
$\mathcal{A}$ performs a second series of queries just like in queries-I. In this stage, he can query neither the secret key of any user in the group $Ł^*$ nor ID_B^*, and he cannot make the UNSIGNCRYPT oracle to the ciphertext C^*. At the end of the simulation, he produces a bit b' for which he believes the relation C^*=ANONYSIGNCRYPT $(m_b^*, Ł^*, ID_j)$ holds and sends b' to $\mathcal{B}$. At this moment, if $b' = b$, $\mathcal{B}$ answers 1 as a result of DBDH problem because his selection h satisfying $h = e(U^*, D_j) = e(ap, cbP) = e(P, P)^{abc}$. If $b' \neq b$, $\mathcal{B}$ answers 0.

Success probability: Now we analyze $\mathcal{B}$'s success probability. The probability that $\mathcal{B}$ does not fail during the key extraction queries is greater than $1/q_{H_0}$. Furthermore, with a probability $1/q_{H_0}$, $\mathcal{A}$ chooses to be challenge on the ID_j to solve DBDH problem if $\mathcal{A}$ wins the IND-IDAS-CCA2 game. we have
$p_1 = Pr[b' = b]\text{ANONYSIGNCRYPT}(m_b^*, D_A^*, ID_j)] = \epsilon + \frac{1}{2} - \frac{q_U}{2^k}$
$p_2 = Pr[b' = i | h \in_R G_2] = 1/2$ (i=0,1)
$Adv(\mathcal{B}) = \frac{p_1 - p_2}{q_{H_0}^2} = (\epsilon - \frac{q_U}{2^k})/q_{H_0}^2$

Theorem 2. (Anonymity) *The improved anonymous signcryption scheme is full anonymous.*

Proof. Given a ciphertext $C = (c, S, U, R_1, ..., R_n)$, we know that $c, U, R_i (i \neq s)$ cannot leak any identity information about group identity L. It remains to consider whether R_s and S leaks information about the actual signcrypter. It has

$$\begin{aligned} e(S,P) &= e((x_s + H_3(c,R_i))D_s, P)) = e((x_s + H_3(c,R_i))Q_s, P_{pub}) \\ &= e(x_s Q_s, P_{pub}) e(H_3(c,R_s)Q_s, P_{pub}) \\ &= e(R_s + \textstyle\sum_{i=1,i\neq s}^{n}(R_i + H_3(c,R_i)Q_i), P_{pub}) e(H_3(c,R_s), P_{pub})) \\ &= e(\textstyle\sum_{i=1,i\neq s}^{n}(R_i + H_3(c,R_i)Q_i), P_{pub}) e(H_3(c,R_s) + R_s, P_{pub})) \end{aligned}$$

It seems that it can check whether ID_i is the actual signcrypter by
$e(S,P) = e(\sum_{i=1,i\neq j}^{n}(R_i + H_3(c,R_i)Q_i), P_{pub}) e(H_3(c,R_j) + R_j, P_{pub}))$

However, it is no use in leaking signcrypter information because the above equality not only holds when $i = j$, but also $\forall \in \{1, ..., n\} \backslash \{j\}$.

$e(R_i + \sum_{j=1, j \neq i}^{n} (R_j + H_3(c, R_j)Q_j), P_{pub}) e(H_3(c, R_i)Q_i, P_{pub})$
$= e(R_i + \sum_{j=1, j \neq i}^{n} (R_j + H_3(c, R_j)Q_j) + H_3(c, R_i)Q_i, P_{pub})$
$= e(\sum_{j=1}^{n} (R_j + H_3(c, R_j)Q_j), P_{pub}) = e(\sum_{j=1}^{n} (x_j + H_3(c, R_j)D_j), P)$
$= e(S, P)$

Theorem 3. *(*Unforgeability*) The improved anonymous signcryption scheme is existentially unforgeable against adaptive chosen-message and adaptive chosen-identity attacks (EUF-IDAS-CMIA).*

Proof. The improved scheme is unforgeable against adaptive chosen-message and chosen-identity attacks that can be derived directly from the security of Chow's ID-based ring signature scheme [**?**] under the CDH assumption. If an adversary can forge a valid message of the proposed scheme, then he must be able to forge a valid Chow's ring signature. That is if $\mathcal{A}$ can forge a valid ciphertext on message m, say $C = (c, S, U, R_1, ..., R_n)$ of a user group Ł and a designated receiver ID_B, then $\sigma^* = (S, R_1, ..., R_n)$ can be viewed as the Chow's ID-based ring signature on message $m = c$ of the ring Ł.

Theorem 4. *(*Public authenticity *The improved anonymous signcryption scheme is public authenticable.*

Proof. When obtains the ciphertext $C = (c, S, U, R_1, ..., R_n)$, anyone can check the ciphertext C's origin group without knowing the content of the message and getting any help of the receiver by the following equation:
$e(S, P) = e(P_{pub}, \sum_{i=1}^{n} (R_i + H_3(c, R_i)Q_i))$

6 Conclusion

We have showed that the ZGCG scheme that providing neither anonymous for unsigncrypter nor public verifiable or authenticable for a third party. We also proposed an improved anonymous signcryption scheme that satisfying confidentiality, unforgeability, signcrypter anonymity and public authenticity in the random oracle model.

Acknowledgment

The authors gratefully thank the anonymous reviewers for their valuable suggestion. This work was supported by the National Natural Science Foundation of China under Grants 60773175 and 60673077, the Foundation of National Laboratory for Modern Communications under Grant 9140c1108010606.

References

1. Y. Zheng. Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature)+cost(encryption). *Advances in Crypto'97,LNCS 1294*, pp.165–179, Springer-Verlag, Berlin, 1997.
2. F. Bao and R.H. Deng. A signcryption scheme with signature directly verifiable by public key. *Public Key Cryptography-PKC'98, LNCS 1431*, pp.55–59, Springer-Verlag, Berlin, 1998
3. DH Yun,, PJ Lee. New signcryption schemes based on KCDSA. In ICISC2001, LNCS 2288, pp.533-547, 2002
4. J Malone-Lee, W Mao. Two birds one stone: signcryption schemes using RSA. CTRSA2003, LNCS 2612, pp. 211-226, 2003
5. Chung Ki Li, Guomin Yang, Duncan S. Wong, Xiaotie Deng, and S S M.Chow. An efficient signcryption scheme with key privacy . *EuroPKI 2007, LNCS 4582*, pp. 78-93, 2007
6. Joonsang Baek, Ren Steinfeld, Yuliang Zheng. Formal proofs for the security of signcryption. *Journal of cryptology.* 20(1): 203-235, 2007
7. L. Chen and J. Malone-Lee. Improved identity-based signcryption. *Public Key Cryptography-PKC 2005, LNCS 3386*, pp. 362–379, Springer-Verlag, 2005.
8. Y Yu, B Yang, Y Sun, and S Zhu. Identity based signcryption scheme without random oracles. Computer standard & interfaces, 31(1): 56-62, 2009
9. 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. *Advance in Cryptology-ASIACRYPT 2005, LNCS 3788*, pp. 515–532, 2005
10. 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 ciphertext authenticity. *Information Security and Cryptology-ICISC 2003*, LNCS 2971, pp. 352-369, Springer-Verlag, 2004.
11. Tan, C. H. Analysis of improved signcryption scheme with key privacy. *Information Processing Letters* 99(4), pp.135-138, 2006
12. TH Yuen, and VK Wei.Fast and Proven Secure Blind Identity-Based Signcryption from Pairings. CT-RSA2005, LNCS 3376, pp.305-322, 2005
13. X Y. Huang, Willy Su, Yi M. Identity-based ring signcryption scheme: cryptographic primitives for preserving privacy and authenticity in the ubiquitious world. *19th International conference on Advance Information Networking and Applications*, pp. 649-654, 2003
14. Rivest R L, Shamir A, Tauman Y. How to leak a secret. *Proc of Asiacrypt01, 2001.* Berlin: Springer-Verlag, 552-565, 2001
15. M W Zhang, B Yang, Y Chen, and W Zhang. Efficient secret authenticatable anonymous signcryption scheme with identity privacy. ISI Workshops 2008, LNCS 5075, pp.126-137, 2008
16. Jianhong Zhang, Shengnan Gao, Hua Chen, and Qin Geng. A Novel ID-Based Anonymous Signcryption Scheme. In Q. Li et al. (Eds.): APWeb/WAIM 2009, LNCS5446, pp. 604-610, 2009