Analysis and Improvement of Authenticatable Ring Signcryption Scheme*

Fagen Li, Masaaki Shirase, and Tsuyoshi Takagi

School of Systems Information Science
Future University-Hakodate
Hakodate 041-8655, Japan
fagenli@uestc.edu.cn

Abstract. Ring signcryption is an anonymous signcryption which allows a user to anonymously signcrypt a message on behalf of a set of users including himself. In an ordinary ring signcryption scheme, even if a user of the ring generates a signcryption, he also cannot prove that the signcryption was produced by himself. In 2008, Zhang, Yang, Zhu, and Zhang solve the problem by introducing an identity-based authenticatable ring signcryption scheme (denoted as the ZYZZ scheme). In the ZYZZ scheme, the actual signcrypter can prove that the ciphertext is generated by himself, and the others cannot authenticate it. However, in this paper, we show that the ZYZZ scheme is not secure against chosen plaintext attacks. Furthermore, we propose an improved scheme that remedies the weakness of the ZYZZ scheme. The improved scheme has shorter ciphertext size than the ZYZZ scheme. We then prove that the improved scheme satisfies confidentiality, unforgeability, anonymity and authenticatability.

Keywords: Identity-based cryptography, bilinear pairings, ring signcryption, ring signature.

1 Introduction

Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. A traditional approach to achieve these requirements is to sign-then-encrypt the message. Signcryption, first proposed by Zheng in 1997 [31], is a cryptographic primitive that performs digital signature and public key encryption simultaneously, at lower computational costs and communication overheads than the signature-then-encryption approach. Several efficient signcryption schemes have been proposed since 1997 [3,11,20,23,25,28]. The original scheme in [31] is based on the discrete logarithm problem but no security proof is given. Zheng's original construction was only proven secure in 2002 by Baek, Steinfeld, and Zheng [2] who described a formal security model in a multi-user setting.

Identity-based (ID-based) cryptography was introduced by Shamir in 1984 [24]. The distinguishing property of ID-based cryptography is that a user's public key can be any binary string, such as an email address that can identify the user. This removes the need for senders to look up the recipient's public key before sending out an encrypted message. ID-based cryptography is supposed to provide a more convenient alternative to conventional public key infrastructure. Several practical ID-based signature schemes have been devised since 1984, but a satisfying ID-based encryption scheme only appeared in 2001 [5]. It was devised by Boneh and Franklin and cleverly uses bilinear maps (the Weil or Tate pairing) over supersingular elliptic curves. A recent direction is to merge the concepts of ID-based cryptography and signcryption to design efficient ID-based signcryption schemes. Several ID-based signcryption schemes have been proposed so far, e.g. [4,6,7,8,16,19]. In addition, many variations of ID-based signcryption were proposed, for examples, ID-based proxy signcryption [13,15,26], ID-based threshold signcryption [10,17,18,21] and unsigncryption [14], and ID-based blind signcryption [27].

* Full version of a paper published in Journal of Shanghai Jiaotong University (Science), Vol. 13, No. 6, pp. 679–683, 2008.

The concept of ring signature was introduced by Rivest, Shamir, and Tauman in 2001 [22]. A ring signature is considered to be a simplified group signature which consists of only users without managers. It protects the anonymity of a signer since the verifier knows that the signature comes from a member of a ring, but doesn't know exactly who the signer is. The first ID-based ring signature scheme was proposed by Zhang and Kim in [29].

In 2005, Huang, Susilo, Mu, and Zhang proposed an ID-based ring signcryption scheme (denoted as the HSMZ scheme) by combining the concepts of ID-based ring signature and signcryption together [12]. In such a scheme, a user can anonymously signcrypt a message on behalf of a set of users including himself. ID-based ring signcryption is very useful to protect privacy and authenticity of a collection of users who are connected through an ad hoc network. However, in [12], even if a user of the ring generates a signcryption, he also cannot prove that the signcryption was produced by himself. Such ring signcryption is not suitable for the following scenario [30]. If Alice want to expose a grafter to a policeman using ring signcryption manner to signcrypt the evidence in order to avoid being retaliated. The policeman will give Alice prize in order to advocate such behavior. However, the policeman can not distinguish who is the actual signcrypter from the group members, and Alice also cannot prove that the signcryption was produced by herself because of the anonymity of ring signcryption.

To solve the above problem, Zhang, Yang, Zhu, and Zhang proposed an identity-based authenticatable ring signcryption scheme (denoted as the ZYZZ scheme) in 2008 [30]. In their scheme, the actual signcrypter can prove that the ciphertext is generated by himself, and the others cannot authenticate it. However, in this paper, we show that the ZYZZ scheme is not secure against chosen plaintext attacks. Furthermore, we propose an improved scheme that remedies the weakness of the ZYZZ scheme. The improved scheme has shorter ciphertext size than the ZYZZ scheme. We then prove that the improved scheme satisfy confidentiality, unforgeability, anonymity and authenticatability.

The rest of this paper is organized as follows. Some preliminary works are given in Section 2. The formal model of ID-based authenticatable ring signcryption is described in Section 3. We analyze the ZYZZ scheme in Section 4. The improved scheme is given in Section 5. We analyze the improved scheme in Section 6. Finally, the conclusions are given in Section 7.

2 Preliminaries

In this section, we briefly describe the basic definition and properties of the bilinear pairings.

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1. Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$, $a, b \in Z_q$.
2. Non-degeneracy: There exists P and $Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$.
3. Computability: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all P,$Q \in G_1$.

The modified Weil pairing and the Tate pairing [5] are admissible maps of this kind. The security of our scheme described here relies on the hardness of the following problems.

Definition 1. *Given two groups G_1 and G_2 of the same prime order q, a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1, the Decisional Bilinear Diffie-Hellman problem (DBDHP) in $(G_1, G_2, \hat{e})$ is to decide whether $h = \hat{e}(P, P)^{abc}$ given (P, aP, bP, cP) and an element $h \in G_2$. We define the advantage of a distinguisher against the DBDHP like this*

$$\begin{aligned} Adv(D) = |&P_{a,b,c,\in_R Z_q, h \in_R G_2}[1 \leftarrow D(aP, bP, cP, h)] \\ &- P_{a,b,c,\in_R Z_q}[1 \leftarrow D(aP, bP, cP, \hat{e}(P, P)^{abc})]|. \end{aligned}$$

Definition 2. *Given two groups G_1 and G_2 of the same prime order q, a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1, the Computational Bilinear Diffie-Hellman problem (CBDHP) in $(G_1, G_2, \hat{e})$ is to compute $h = \hat{e}(P, P)^{abc}$ given (P, aP, bP, cP).*

The decisional problem is of course not harder than the computational one. However, no algorithm is known to be able to solve any of them so far.

3 Formal Model of ID-Based Authenticatable Ring Signcryption

3.1 Generic Scheme

A generic ID-based authenticatable ring signcryption scheme consists of the following five algorithms.

- `Setup:` Given a security parameter k, the private key generator (PKG) generates the system's public parameters *params*. Among the parameters produced by `Setup` is a key P_{pub} that is made public. There is also corresponding master key s that is kept secret.
- `Extract:` Given an identity ID, the PKG computes the corresponding private key D_{ID} and transmits it to its owner in a secure way.
- `Signcrypt:` To send a message m to the receiver Bob whose identity is ID_B, Alice chooses a group $\mathcal{U} = \{u_1, \ldots, u_n\}$ with identities $\{ID_1, \ldots, ID_n\}$ including herself and computes `Signcrypt`$(m, D_{ID_A}, \mathcal{U}, ID_B)$ on behalf of the group to obtain the ciphertext C.
- `Unsigncrypt:` When Bob receives the ciphertext C from Alice, he computes `Unsigncrypt`$(C, \mathcal{U}, D_{ID_B})$ and obtains the plaintext m or the symbol $\perp$ if C is an invalid ciphertext between the group $\mathcal{U}$ and Bob.
- `Authenticate:` Given the ciphertext C and Alice's private key D_{ID_A}, this algorithm outputs $\top$ for "true" or $\perp$ for "false", depending on whether Alice is the actual signcrypter of ciphertext C or not.

We make the consistency constraint that if

$$C = \texttt{Signcrypt}(m, D_{ID_A}, \mathcal{U}, ID_B),$$

then

$$m = \texttt{Unsigncrypt}(C, \mathcal{U}, D_{ID_B}) \quad \text{and} \quad \texttt{Authenticate}(C, D_{ID_A}) = \top.$$

3.2 Security Notions

The HSMZ scheme [12] defines the security notions for ID-based ring signcryption schemes. These notions are indistinguishability against adaptive chosen ciphertext attacks and unforgeability against adaptive chosen messages attacks. The ZYZZ scheme [30] extended the notions to ID-based authenticatable ring signcryption scheme. However, both [12] and [30] do not consider insider security [1]. Insider security can resist attacks from his partner. It means that (a) if the sender's private key is exposed, an adversary is still not able to recover the message from the ciphertext and (b) if the receiver's private key is exposed, an adversary is still not able to forge a signcryption. Here, we modify their definitions slightly by adding the insider security for signcryption. An ID-based authenticatable ring signcryption scheme should satisfy *confidentiality*, *unforgeability*, *anonymity* and *authenticatability*.

For the confidentiality, we consider the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- `Initial:` The challenger $\mathcal{C}$ takes a security parameter k and runs `Setup` to generate system parameters *params* and the master secret key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$.
- `Phase 1:` The adversary $\mathcal{A}$ can perform a polynomially bounded number of queries in an adaptive manner (that is, each query may depend on the responses to the previous queries).

- Key extraction queries: $\mathcal{A}$ chooses an identity ID and receives the extracted private key $D_{ID} = \texttt{Extract}(ID)$.
- Signcryption queries: $\mathcal{A}$ produces a group $\mathcal{U} = \{u_1, \ldots, u_n\}$ with identities $\{ID_1, \ldots, ID_n\}$, an identity ID_j and a plaintext m. $\mathcal{C}$ randomly chooses a user $u_i \in \mathcal{U}$ whose identity is ID_i and computes $D_{ID_i} = \texttt{Extract}(ID_i)$. Then $\mathcal{C}$ acts as u_i on behalf of the group $\mathcal{U}$ and sends the result of $\texttt{Signcrypt}(m, D_{ID_i}, \mathcal{U}, ID_j)$ to $\mathcal{A}$.
- Unsigncryption queries: $\mathcal{A}$ produces a group $\mathcal{U} = \{u_1, \ldots, u_n\}$ with identities $\{ID_1, \ldots, ID_n\}$, an identity ID_j, and a ciphertext C. $\mathcal{C}$ generates the private key $D_{ID_j} = \texttt{Extract}(ID_j)$ and sends the result of $\texttt{Unsigncrypt}(C, \mathcal{U}, D_{ID_j})$ to $\mathcal{A}$ (this result can be the $\perp$ symbol if C is an invalid ciphertext)

– `Challenge:` The adversary $\mathcal{A}$ decides when Phase 1 ends. $\mathcal{A}$ generates two equal length plaintexts m_0, m_1, a user set $\mathcal{U}_A$ and an identity ID_B on which he wants to be challenged. He cannot have asked the private key corresponding to ID_B in Phase 1. $\mathcal{C}$ picks a random bit b from $\{0, 1\}$, chooses $u_s \in \mathcal{U}$, and computes $C = \texttt{Signcrypt}(m_b, D_{ID_s}, \mathcal{U}_A, ID_B)$ which is sent to $\mathcal{A}$.

– `Phase 2:` The adversary $\mathcal{A}$ can ask a polynomially bounded number of queries adaptively again as in Phase 1 with the restriction that it cannot make a key extraction query on ID_B and cannot make an unsigncryption query on $(C, \mathcal{U}_A, D_{ID_B})$ to obtain the corresponding plaintext.

– `Guess:` The adversary $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$.

The advantage of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) = |2P[b' = b] - 1|$, where $P[b' = b]$ denotes the probability that $b' = b$.

Definition 3 (Confidentiality). *An ID-based authenticatable ring signcryption scheme (IDARSC) is said to have the indistinguishability against adaptive chosen ciphertext attacks property (IND-IDARSC-CCA2) if no polynomially bounded adversary has a non-negligible advantage in the confidentiality game.*

Notice that the adversary is allowed to make a key extraction query on any user in the group $\mathcal{U}_A$ in the above definition. This condition corresponds to the stringent requirement of insider security for confidentiality of signcryption [1]. On the other hand, it ensures the forward security of the scheme, i.e. confidentiality is preserved in case the sender's private key becomes compromised.

For the unforgeability, we consider the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{F}$.

– `Initial:` The challenger $\mathcal{C}$ takes a security parameter k and runs `Setup` to generate system parameters *params* and the master secret key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$.

– `Attack:` The adversary $\mathcal{A}$ performs a polynomially bounded number of queries just like in the confidentiality game.

– `Forgery:` $\mathcal{A}$ produces a new triple $(\mathcal{U}_A, ID_B, C)$(i.e. a triple that was not produced by the signcryption oracle), where the private keys of the users in the group $\mathcal{U}_A$ were not asked in the second stage and wins the game if the result of the $\texttt{Unsigncrypt}(C, \mathcal{U}_A, D_{ID_B})$ is not the $\perp$ symbol.

The advantage of $\mathcal{A}$ is defined as the probability that it wins.

Definition 4 (Unforgeability). *An ID-based authenticatable ring signcryption scheme (IDARSC) is said to have the existential unforgeability against adaptive chosen messages attacks (EUF-IDARSC-CMA) if no polynomially bounded adversary has a non-negligible advantage in the unforgeability game.*

Note that the adversary is allowed to make a key extraction query on the identity ID_B in the above definition. Again, this condition corresponds to the stringent requirement of insider security for signcryption [1].

For anonymity, we require that it is impossible for an adversary to guess the identity of the real signcrypter with a probability larger than $1/n$, where n is the size of the ring.

Definition 5 (Anonymity). *An ID-based authenticatable ring signcryption scheme is unconditional anonymous if for any group of n members, any message m and ciphertext C, any adversary cannot identify the actual signcrypter with probability better than random guess. That is, the adversary can only output the identity of the actual signcrypter with probability $1/n$.*

Definition 6 (Authenticatability). *An ID-based authenticatable ring signcryption scheme is authenticatable if and only if the actual signcrypter can authenticate that a ciphertext C was indeed produced by himself. However, the other members of the group cannot authenticate the ciphertext C to be produced by themselves with non-negligible probability.*

4 Analysis of the ZYZZ Scheme

In this section, we show that the ZYZZ scheme [30] is not secure against chosen plaintext attacks.

4.1 Review of the ZYZZ Scheme

The ZYZZ scheme consists of the following five algorithms.

- `Setup`: Given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order q (with G_1 additive and G_2 multiplicative), a generator P of G_1, a bilinear map $\hat{e} : G_1 \times G_1 \to G_2$, and hash functions $H_0 : \{0,1\}^* \to G_1$, $H_1 : G_2 \to \{0,1\}^l$, and $H_2 : \{0,1\}^* \to Z_q^*$. The PKG chooses a master key $s \in Z_q^*$ randomly and computes $P_{pub} = sP$. The PKG publishes system parameters $\{G_1, G_2, l, \hat{e}, P, P_{pub}, H_0, H_1, H_2\}$ and keeps the master key s secret.
- `Extract`: Given an identity ID, the PKG computes $Q_{ID} = H_0(ID)$ and the private key $D_{ID} = sQ_{ID}$. Then PKG sends the private key to its owner in a secure way.
- `Signcrypt`: Consider a set of users $\mathcal{U} = \{u_1, \dots, u_n\}$ including the actual signcrypter Alice. Let ID_i be u_i's identity. To send a message m to Bob with identity ID_B on behalf of the group $\mathcal{U}$, the actual signcrypter Alice, indexed by s (i.e. her public key is $Q_{ID_s} = H_0(ID_s)$ and private key is $D_{ID_s} = sQ_{ID_s}$) performs the following steps.
  1. Choose $r \in Z_q^*$ randomly.
  2. Compute $R = rP$, $R' = \hat{e}(P_{pub}, Q_{ID_B})^r$ and $t = H_1(R')$.
  3. Compute $c = m \oplus t$.
  4. For all $i \in \{1, \dots, n\}, i \neq s$, choose $a_i \in Z_q^*$ randomly, compute $U_i = a_iP$ and $h_i = H_2(m,\mathcal{U}, t, U_i)$.
  5. Choose $a_s \in Z_q^*$ randomly and compute $U_s = a_sQ_{ID_s} - \sum_{i=1, i\neq s}^{n}(U_i + h_iQ_{ID_i})$.
  6. Compute $h_s = H_2(m,\mathcal{U}, t, U_s)$ and $\sigma = (h_s + a_s)D_{ID_s}$.

  The ciphertext is $C = (\mathcal{U}, c, R, h_1, \dots, h_n, U_1, \dots, U_n, \sigma)$.
- `Unsigncrypt`: When receiving C, Bob follows the steps below.
  1. Compute $t = H_1(\hat{e}(R, D_{ID_B}))$.
  2. Recover $m = c \oplus t$.
  3. Accept C if and only if both $h_i = H_2(m,\mathcal{U}, t, U_i)(i = 1, \dots, n)$ and $\hat{e}(P, \sigma) = \hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i + h_iQ_{ID_i}))$ hold, return $\perp$ otherwise.
- `Authenticate`: If the actual signcrypter Alice wants to prove that the ciphertext C was produced by herself, she follows the steps below.
  1. Alice chooses $x \in Z_q^*$ randomly, computes $\mu = \hat{e}(P, \sigma)^x$, and sends μ to the verifier.
  2. The verifier chooses $y \in Z_q^*$ randomly and sends it to Alice.
  3. Alice computes $\nu = (x + y)(h_s + a_s)$ and sends ν to the verifier.
  4. The verifier checks that if $\hat{e}(P_{pub}, Q_{ID_s})^\nu = \mu\hat{e}(P, \sigma)^y$ holds. If the equation holds, the verifier believes that Alice is actual signcrypter and returns $\top$, otherwise returns $\perp$.

4.2 Analysis

We show that the ZYZZ scheme is not secure against chosen plaintext attacks. When $\mathcal{A}$ receives the challenge ciphertext $C^* = (\mathcal{U}^*, c^*, R^*, h_1^*, \ldots, h_n^*, U_1^*, \ldots, U_n^*, \sigma^*)$. $\mathcal{A}$ first makes a "wild guess" of b to be 0. Then, $\mathcal{A}$ follows the steps as follows.

1. Compute $t^* = m_0 \oplus c^*$.
2. Check if $h_i^* = H_2(m_0, \mathcal{U}^*, t^*, U_i^*)$ for $i = 1, \ldots, n$.
3. Check if $\hat{e}(P, \sigma^*) = \hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i^* + h_i^* Q_{ID_i^*}))$.

If the above equations hold, then $\mathcal{A}$ knows that m_0 is the plaintext for the challenge ciphertext. If the above equations do not hold, then $\mathcal{A}$ knows that m_1 is the plaintext for the challenge ciphertext. In fact, it is enough for $\mathcal{A}$ to check one equation, for example $h_1^* = H_2(m_0, \mathcal{U}^*, t^*, U_1^*)$. Therefore, we conclude that the ZYZZ scheme is not secure against chosen plaintext attacks.

5 An Improved Scheme

To overcome the weakness of the ZYZZ scheme [30], we propose an improved scheme in this section. The details of the improved scheme is described as below.

- `Setup:` Given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order q (with G_1 additive and G_2 multiplicative), a generator P of G_1, a bilinear map $\hat{e} : G_1 \times G_1 \to G_2$, a secure symmetric cipher (E, D) and hash functions $H_0 : \{0,1\}^* \to G_1$, $H_1 : G_2 \to \{0,1\}^l$, and $H_2 : \{0,1\}^* \to Z_q^*$. The PKG chooses a master key $s \in Z_q^*$ randomly and computes $P_{pub} = sP$. The PKG publishes system parameters $\{G_1, G_2, l, \hat{e}, P, P_{pub}, E, D, H_0, H_1, H_2\}$ and keeps the master key s secret.
- `Extract:` Given an identity ID, the PKG computes $Q_{ID} = H_0(ID)$ and the private key $D_{ID} = sQ_{ID}$. Then PKG sends the private key to its owner in a secure way.
- `Signcrypt:`Consider a set of users $\mathcal{U} = \{u_1, \ldots, u_n\}$ including the actual signcrypter Alice. Let ID_i be u_i's identity. To send a message m to Bob with identity ID_B on behalf of the group $\mathcal{U}$, the actual signcrypter Alice, indexed by s (i.e. her public key is $Q_{ID_s} = H_0(ID_s)$ and private key is $D_{ID_s} = sQ_{ID_s}$) performs the following steps.
  1. Choose $r \in Z_q^*$ randomly.
  2. Compute $R = rP$ and $k = H_1(\hat{e}(P_{pub}, Q_{ID_B})^r)$.
  3. Compute $c = E_k(m)$.
  4. For all $i \in \{1, \ldots, n\}, i \neq s$, choose $a_i \in Z_q^*$ randomly, compute $U_i = a_i P$ and $h_i = H_2(c, \mathcal{U}, U_i)$.
  5. Choose $a_s \in Z_q^*$ randomly and compute $U_s = a_s Q_{ID_s} - \sum_{i=1, i\neq s}^{n}(U_i + h_i Q_{ID_i})$.
  6. Compute $h_s = H_2(c, \mathcal{U}, U_s)$ and $\sigma = (h_s + a_s) D_{ID_s}$.

  The ciphertext is $C = (\mathcal{U}, c, R, U_1, \ldots, U_n, \sigma)$.
- `Unsigncrypt:` When receiving C, Bob follows the steps below.
  1. Compute $k = H_1(\hat{e}(R, D_{ID_B}))$.
  2. Recover $m = D_k(c)$.
  3. For all $i \in \{1, \ldots, n\}$, compute $h_i = H_2(c, \mathcal{U}, U_i)$.
  4. Accept C if and only if $\hat{e}(P, \sigma) = \hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{ID_i}))$, return $\perp$ otherwise.
- `Authenticate:` If the actual signcrypter Alice wants to prove that the ciphertext C was produced by herself, she follows the steps below.
  1. Alice chooses $x \in Z_q^*$ randomly, computes $\mu = \hat{e}(P, \sigma)^x$, and sends μ to the verifier.
  2. The verifier chooses $y \in Z_q^*$ randomly and sends it to Alice.
  3. Alice computes $\nu = (x + y)(h_s + a_s)$ and sends ν to the verifier.
  4. The verifier checks that if $\hat{e}(P_{pub}, Q_{ID_s})^\nu = \mu \hat{e}(P, \sigma)^y$ holds. If the equation holds, the verifier believes that Alice is actual signcrypter and returns $\top$, otherwise returns $\perp$.

Notice that we compute $h_i = H_2(c, \mathcal{U}, U_i)$ instead of $h_i = H_2(m, \mathcal{U}, t, U_i)$, which can resist the above attack. In addition, our scheme has shorter ciphertext since the ciphertext does not contain $h_1, \ldots, h_n$. In the validity verification phase, the ZYZZ scheme [30] needs to check $n+1$ equations. Our scheme only needs to check 1 equation. Moreover, our scheme provides the ciphertext authenticity [8]. Anyone can verify the validity of the ciphertext without knowing the content of the message. When Bob receives the ciphertext C, he can first compute $h_i = H_2(c, \mathcal{U}, U_i)(i = 1, \ldots, n)$ and verify the validity of the ciphertext by the following equation:

$$\hat{e}(P, \sigma) = \hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{ID_i}))$$

If he finds the ciphertext is valid, he then computes k and recovers m. Otherwise, he need not compute k and recover m. So the computational cost is saved.

6 Analysis of the Improved Scheme

6.1 Correctness

The correctness can be easily verified by the following equations.

$$\hat{e}(R, D_{ID_B}) = \hat{e}(rP, D_{ID_B}) = \hat{e}(rP_{pub}, Q_{ID_B}) = \hat{e}(P_{pub}, Q_{ID_B})^r$$

and

$$\begin{aligned}\hat{e}(P, \sigma) = \hat{e}(P, (h_s + a_s)D_{ID_s}) &= \hat{e}(P_{pub}, h_s Q_{ID_s} + a_s Q_{ID_s}) \\ &= \hat{e}(P_{pub}, h_s Q_{ID_s} + U_s + \sum_{i=1, i \neq s}^{n}(U_i + h_i Q_{ID_i})) \\ &= \hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{ID_i}))\end{aligned}$$

6.2 Security

The following several theorems show that the improved scheme satisfies confidentiality, unforgeability, anonymity and authenticatability.

Theorem 1 (Confidentiality). *In the random oracle model, we assume we have an IND-IDARSC-CCA2 adversary called $\mathcal{A}$ that is able to distinguish ciphertext during the confidentiality game with an advantage ϵ when running in a time t and asking at most q_{H_0} identity hashing queries, at most q_{H_1} H_1 queries, at most q_{H_2} H_2 queries, at most q_K key extraction queries, q_S signcryption queries and q_U unsigncryption queries. Then, there exists a distinguisher $\mathcal{C}$ that can solve the Decisional Bilinear Diffie-Hellman problem in a time $O(t + (q_S + 3q_U)T_{\hat{e}})$ with an advantage*

$$Adv(\mathcal{C})^{DBDH(G_1,P)} > \frac{\epsilon - q_U/2^{k-1}}{2q_{H_0}^2},$$

where $T_{\hat{e}}$ denotes the computation time of the bilinear map.

Proof. See the appendix A. □

Theorem 2 (Unforgeability). *The improved scheme has the existential unforgeability against adaptive chosen messages attacks.*

Proof. See the appendix B. □

Theorem 3 (Anonymity). *The improved scheme has the unconditional signcrypter ambiguity property.*

Proof. See the appendix C. □

Theorem 4 (Authenticatability). *The improved scheme has the authenticatability property.*

Proof. See the appendix D. □

6.3 Performance and Security Comparison

We compare the performance and security of the improved scheme with those of existing schemes [12,30] in Table 1. We consider the costly operations which include point scalar multiplications in G_1 (G_1 Mul), exponentiations in G_2 (G_2 Exp), and pairing operations (Pairing). The D3, D4, D5 and D6 in the "Security" column refer to security under Definitions 3, 4, 5 and 6 respectively. A "Y" means that the scheme meets the definition and a "N" means that the scheme is not secure under the definition.

Table 1. Performance and security comparison

Scheme	Efficiency			Security				Ciphertext size
	G_1 Mul	G_2 Exp	Pairing	D3	D4	D5	D6	
[12]	$3n+2$	0	$n+5$	Y	Y	Y	N	$\lvert\mathcal{U}\rvert + 2l + 2\lvert G_1\rvert + n\lvert G_2\rvert + nq$
[30]	$3n+1$	4	4(+3)	N	Y	Y	Y	$\lvert\mathcal{U}\rvert + \lvert c\rvert + (n+2)\lvert G_1\rvert + nq$
Ours	$3n+1$	4	4(+3)	Y	Y	Y	Y	$\lvert\mathcal{U}\rvert + \lvert c\rvert + (n+2)\lvert G_1\rvert$

From Table 1, we can see that our scheme has same efficiency as the ZYZZ scheme [30]. Both the two schemes need 4 pairing operations in `Signcrypt` and `Unsigncrypt` phases and 3 pairing operations in `Authenticate` phase. However, our scheme has shorter ciphertext than the ZYZZ scheme. The ciphertext size of our scheme is $|\mathcal{U}|+|c|+(n+2)|G_1|$. The ciphertext size of the ZYZZ scheme is $|\mathcal{U}|+|c|+(n+2)|G_1|+nq$. Moreover, Our scheme meets security Definitions 3, 4, 5 and 6. The ZYZZ scheme [30] does not meet the confidentiality definition (D3). The HSMZ scheme [12] does not meet the authenticatability definition (D6). Therefore, our scheme is more efficient and secure than existing schemes [12,30].

7 Conclusions

We have showed that the ZYZZ scheme is not secure against chosen plaintext attacks. Then, we proposed an improved scheme with shorter ciphertext. We proved that the improved scheme satisfies confidentiality, unforgeability, anonymity and authenticatability. Compared with the existing two schemes, our scheme is more efficient and secure.

Acknowledgements

Fagen Li is supported by the JSPS postdoctoral fellowship for research in Japan.

References

1. J.H. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In *Advances in Cryptology-EUROCRYPT 2002*, LNCS 2332, pp. 83–107, Springer-Verlag, 2002.
2. J. Baek, R. Steinfeld, and Y. Zheng. Formal proofs for the security of signcryption. In *Public Key Cryptography-PKC 2002*, LNCS 2274, pp. 80–98, Springer-Verlag, 2002.
3. F. Bao and R.H. Deng. A signcryption scheme with signature directly verifiable by public key. In *Public Key Cryptography-PKC'98*, LNCS 1431, pp. 55–59, Springer-Verlag, 1998.
4. 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. In *Advances in Cryptology-ASIACRYPT 2005*, LNCS 3788, pp. 515–532, Springer-Verlag, 2005.
5. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology-CRYPTO 2001*, LNCS 2139, pp. 213–229, Springer-Verlag, 2001.
6. X. Boyen. Multipurpose identity-based signcryption: a swiss army knife for identity-based cryptography. In *Advances in Cryptology-CRYPTO 2003*, LNCS 2729, pp. 383–399, Springer-Verlag, 2003.
7. L. Chen and J. Malone-Lee. Improved identity-based signcryption. In *Public Key Cryptography-PKC 2005*, LNCS 3386, pp. 362–379, Springer-Verlag, 2005.
8. 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. In *Information Security and Cryptology-ICISC 2003*, LNCS 2971, pp. 352–369, Springer-Verlag, 2004.
9. S.S.M. Chow, S.M. Yiu, and L.C.K. Hui. Efficient identity based ring signature. In *Applied Cryptography and Network Security-ACNS 2005*, LNCS 3531, pp. 499–512, Springer-Verlag, 2005.
10. S. Duan, Z. Cao, and R. Lu. Robust ID-based threshold signcryption scheme from pairings. In *2004 International Conference on Information security*, pp. 33–37, Shanghai, China, 2004.
11. C. Gamage, J. Leiwo, and Y. Zheng. Encrypted message authentication by firewalls. In *Public Key Cryptography-PKC'99*, LNCS 1560, pp. 69–81, Springer-Verlag, 1999.
12. X. Huang, W. Susilo, Y. Mu, and F. Zhang. Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world. In *Advanced Information Networking and Applications-AINA 2005*, pp. 649–654, Taipei, Taiwan, 2005.
13. X. Li and K. Chen. Identity based proxy-signcryption scheme from pairings. In *2004 IEEE International Conference on Services Computing*, pp. 494–497, Shanghai, China, 2004.
14. F. Li, J. Gao, and Y. Hu. ID-based threshold unsigncryption scheme from pairings. In *Information Security and Cryptology-CISC 2005*, LNCS 3822, pp. 242–253, Springer-Verlag, 2005.
15. F. Li, Y. Hu, and S. Liu. ID-based (t, n) threshold proxy signcryption for multi-agent systems. In *Computational Intelligence and Security-CIS 2006*, LNAI 4456, pp. 406–416, Springer-Verlag, 2007.
16. F. Li, Y. Hu, and C. Zhang. An identity-based signcryption scheme for multi-domain ad hoc networks. In *Applied Cryptography and Network Security-ACNS 2007*, LNCS 4521, pp. 373–384, Springer-Verlag, 2007.
17. F. Li and Y. Yu. An efficient and provably secure ID-based threshold signcryption scheme. In *International Conference on Communications, Circuits and Systems (ICCCAS 2008)*, pp. 547–551, IEEE Press, Xiamen, China, 2008.
18. F. Li, C. Xu, and S. Zhou. Improvement of a proactive threshold signcryption scheme. *International Journal of Computers and Applications*, Vol. 30, No. 4, pp. 345–347, 2008.
19. B. Libert and J.J. Quisquater. A new identity based signcryption schemes from pairings. In *2003 IEEE Information Theory Workshop*, pp. 155–158, Paris, France, 2003.
20. J. Malone-Lee and W. Mao. Two birds one stone: signcryption using RSA. In *Topics in Cryptology-CT-RSA 2003*, LNCS 2612, pp. 211–226, Springer-Verlag, 2003.
21. C. Peng and X. Li. An identity-based threshold signcryption scheme with semantic security. In *Computational Intelligence and Security-CIS 2005*, LNAI 3802, pp. 173–179, Springer-Verlag, 2005.
22. R.L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *Advances in Cryptology-ASIACRYPT 2001*, LNCS 2248, pp. 552–565, Springer-Verlag, 2001.
23. M. Seo and K. Kim. Electronic funds transfer protocol using domain-verifiable signcryption scheme. In *Information Security and Cryptology-ICISC'99*, LNCS 1787, pp. 269–277, Springer-Verlag, 2000.
24. A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology-CRYPTO'84*, LNCS 196, pp. 47–53, Springer-Verlag, 1984.

25. R. Steinfeld and Y. Zheng. A signcryption scheme based on integer factorization. In *Information Security Workshop-ISW 2000*, LNCS 1975, pp. 308–322, Springer-Verlag, 2000.
26. Q. Wang and Z. Cao. Two proxy signcryption schemes from bilinear pairings. In *Cryptology and Network Security-CANS 2005*, LNCS 3810, pp. 161–171, Springer-Verlag, 2005.
27. T.H. Yuen and V.K. Wei. Fast and proven secure blind identity-based signcryption from pairings. In *Topics in Cryptology-CT-RSA 2005*, LNCS 3376, pp. 305–322, Springer-Verlag, 2005.
28. D.H. Yum and P.J. Lee. New signcryption schemes based on KCDSA. In *Information Security and Cryptology-ICISC 2001*, LNCS 2288, pp. 305–317, Springer-Verlag, 2002.
29. F. Zhang and K. Kim. ID-based blind signature and ring signature from pairings. In *Advances in Cryptology-ASIACRYPT 2002*, LNCS 2501, pp. 533–547, Springer-Verlag, 2002.
30. M. Zhang, B. Yang, S. Zhu, and W. Zhang. Efficient secret authenticatable anonymous signcryption scheme with identity privacy. In *Intelligence and Security Informatics-ISI 2008*, LNCS 5075, pp. 126–137, Springer-Verlag, 2008.
31. Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost(encryption). In *Advances in Cryptology-CRYPTO'97*, LNCS 1294, pp. 165–179, Springer-Verlag, 1997.

Appendix

A Proof of Theorem 1

Proof. We assume the distinguisher $\mathcal{C}$ receives a random instance (P, aP, bP, cP, h) of the Decisional Bilinear Diffie-Hellman problem. His goal is to decide whether $h = \hat{e}(P,P)^{abc}$ or not. $\mathcal{C}$ will run $\mathcal{A}$ as a subroutine and act as $\mathcal{A}$'s challenger in the IND-IDARSC-CCA2 game. During the game, $\mathcal{A}$ will consult $\mathcal{C}$ for answers to the random oracles H_0, H_1, and H_2. Roughly speaking, these answers are randomly generated, but to maintain the consistency and to avoid collision, $\mathcal{C}$ keeps three lists L_0, L_1, L_2, respectively to store the answers. The following assumptions are made.

1. $\mathcal{A}$ will ask for $H_0(ID)$ before ID is used in any key extraction query, signcryption query and unsigncryption query.
2. Ciphertext returned from a signcryption query will not be used by $\mathcal{A}$ in an unsigncryption query.

At the beginning of the game, $\mathcal{C}$ gives $\mathcal{A}$ the system parameters with $P_{pub} = cP$. Note that c is unknown to $\mathcal{C}$. This value simulates the master key value for the PKG in the game. Then, $\mathcal{C}$ chooses a random number $j \in \{1, 2, \ldots, q_{H_0}\}$. $\mathcal{A}$ asks a polynomially bounded number of H_0 queries on identities of his choice. At the j-th H_0 query, $\mathcal{C}$ answers by $H_0(ID_j) = bP$. For queries $H_0(ID_e)$ with $e \neq j$, $\mathcal{C}$ chooses $b_e \in Z_q^*$ randomly, puts the pair (ID_e, b_e) in list L_0 and answers $H_0(ID_e) = b_eP$.

We now explain how the other kinds of queries are treated by $\mathcal{C}$.

- H_1, H_2 queries: When $\mathcal{A}$ asks queries on these hash values, $\mathcal{C}$ checks the corresponding list. 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 stored in the list.
- Key extraction queries: When $\mathcal{A}$ asks a question $\texttt{Extract}(ID_e)$, if $ID_e = ID_j$, then $\mathcal{C}$ fails and stops. If $ID_e \neq ID_j$, then the list L_0 must contain a pair (ID_e, b_e) for some b_e (this indicates $\mathcal{C}$ previously answered $H_0(ID_e) = b_eP$ on a H_0 query on ID_e). The private key corresponding to ID_e is then $b_eP_{pub} = cb_eP$. It is computed by $\mathcal{C}$ and returned to $\mathcal{A}$.
- Signcryption queries: At any time, $\mathcal{A}$ can perform a signcryption query for a plaintext m, a user group $\mathcal{U}$ and a receiver with identity ID_B. $\mathcal{C}$ randomly chooses a user u_A in the group $\mathcal{U}$ whose identity is ID_A and $ID_A \neq ID_j$ (in this case, the list L_0 must contain a pair (ID_A, b_A), then $\mathcal{C}$ can computes u_A's private key $D_{ID_A} = b_AP_{pub}$). $\mathcal{C}$ uses u_A's private key and runs $\texttt{Signcrypt}(m, D_{ID_A}, \mathcal{U}, ID_B)$ to signcrypt the message on the behalf of the group $\mathcal{U}$. Finally, $\mathcal{C}$ returns the result ciphertext C to $\mathcal{A}$.

- Unsigncryption queries: For a unsigncryption query on a ciphertext $C = (\mathcal{U}, c, R, U_1, \ldots, U_n, \sigma)$ between a user group $\mathcal{U}$ and a receiver with identity ID_B. If $ID_B = ID_j$, $\mathcal{C}$ always notifies $\mathcal{A}$ that the ciphertext is invalid. If $ID_B \neq ID_j$, $\mathcal{C}$ computes $\tau = \hat{e}(R, D_{ID_B})$ ($\mathcal{C}$ could obtain D_{ID_B} from the key extraction algorithm because $ID_B \neq ID_j$), runs the H_1 simulation algorithm to obtain $k = H_1(\tau)$, and runs the H_2 simulation algorithm to obtain $h_i = H_2(c,\mathcal{U}, U_i)$ for $i = 1, \ldots, n$. Then $\mathcal{C}$ checks if $\hat{e}(P, \sigma) = \hat{e}(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{ID_i}))$ holds. If the above equation does not hold, $\mathcal{C}$ rejects the ciphertext. Otherwise $\mathcal{C}$ computes $m = D_k(c)$ and returns m. It is easy to see that, for all queries, the probability to reject a valid ciphertext does not exceed $q_U/2^k$.

After the first stage, $\mathcal{A}$ outputs a set of users $\mathcal{U}_A = \{u_1, \ldots, u_n\}$ with identities $\{ID_1, \ldots, ID_n\}$ and a receiver's identity ID_B he wishes to be challenged. Note that $\mathcal{C}$ fails if $\mathcal{A}$ has asked a key extraction query on ID_B during the first stage. If $ID_B \neq ID_j$, $\mathcal{C}$ fails too.

Then $\mathcal{A}$ outputs two plaintexts m_0 and m_1. $\mathcal{C}$ chooses $b \in \{0, 1\}$ randomly and signcrypts m_b. To do so, he sets $R^* = aP$, obtains $k' = H_1(h)$(where h is $\mathcal{C}$ candidate for the DBDH problem) from the H_2 simulation algorithm, and computes $c_b = E_{k'}(m_b)$. Then $\mathcal{C}$ randomly chooses a user u_s in the group $\mathcal{U}_A$ whose identity is ID_s. For all $i \in \{1, \ldots, n\}, i \neq s$, $\mathcal{C}$ chooses $a'_i \in Z_q^*$ randomly, computes $U_i^* = a'_i P$ and obtains $h'_i = H_2(c_b,\mathcal{U}_A, U_i^*)$ from the H_2 simulation algorithm. Finally, $\mathcal{C}$ chooses $h'_s \in Z_q^*$ and $z' \in Z_q^*$ randomly, computes $U_s^* = z'P - h'_s Q_{ID_s} - \sum_{i=1, i \neq s}^{n}(U_i^* + h'_i Q_{ID_i})$, stores the relationship $h'_s = H_2(c_b, \mathcal{U}_A, U_s^*)$ to the list L_2, and computes $\sigma^* = z'cP$. The ciphertext $C^* = (\mathcal{U}_A, c_b, R^*, U_1^*, \ldots, U_n^*, \sigma^*)$ is returned to $\mathcal{A}$.

$\mathcal{A}$ then performs a second series of queries which is treated in the same way as the first one. At the end of the simulation, he produces a bit b' for which he believes the relation $C^* = \mathtt{Signcrypt}(m_{b'}, D_{ID_s}, \mathcal{U}_A, ID_j)$ holds. At this moment, if $b = b'$, $\mathcal{C}$ outputs $h = \hat{e}(R^*, D_{ID_j}) = \hat{e}(aP, cbP) = \hat{e}(P, P)^{abc}$ as a solution of the DBDH problem, otherwise $\mathcal{C}$ stops and outputs "failure".

We can now assess $\mathcal{C}$'s probability of success. We saw that $\mathcal{C}$ fails if $\mathcal{A}$ asks the private key associated to ID_j during the first stage. We know that there are q_{H_0} ways to choose the ID_j. Among those q_{H_0} identities, at least one of them will never be the subject of a key extraction query from $\mathcal{A}$. Then, with a probability greater than $1/q_{H_0}$, $\mathcal{A}$ will not ask the questions $\mathtt{Extract}(ID_j)$. Further, with a probability exactly $1/q_{H_0}$, $\mathcal{A}$ chooses to be challenged on the ID_j and this must allow $\mathcal{C}$ to solve his DBDH problem if $\mathcal{A}$ wins the IND-IDARSC-CCA2 game.

Since

$$p_1 = \Pr[b' = b | \sigma = \text{Signcrypt}(m_b, D_{ID_i}, ID_j)] = \frac{\epsilon + 1}{2} - \frac{q_U}{2^k},$$

and

$$p_0 = \Pr[b' = i | h \in_R G_2] = \frac{1}{2} \quad \text{for} \quad i = 0, 1,$$

We have

$$\begin{aligned} Adv(\mathcal{C}) &= \frac{|p_1 - p_0|}{q_{H_0}^2} = (\frac{\epsilon + 1}{2} - \frac{q_U}{2^k} - \frac{1}{2})(\frac{1}{q_{H_0}})^2 \\ &= \frac{\epsilon - q_U/2^{k-1}}{2q_{H_0}^2} \end{aligned}$$

The bound on $\mathcal{C}$'s computation time derives from the fact that every signcryption query requires 1 pairing evaluation and every unsigncryption query requires 3 pairing evaluations. □

B Proof of Theorem 2

Proof. The unforgeability of the improved scheme against adaptive chosen messages attacks can be derived directly from the security of the Chow-Yiu-Hui ID-based ring signature scheme [9] under the Computational Diffie-Hellman problem assumption. If an adversary can forge a valid signcryption of the improved scheme, the he must be able to forge a valid signature for the Chow-Yiu-Hui ID-based ring signature scheme. That is, if $\mathcal{A}$ can forge a valid signcryption on message m, say $C = (\mathcal{U}, c, R, U_1, \ldots, U_n, \sigma)$ of a user group $\mathcal{U}$ and a receiver with identity ID_B, then $(\mathcal{U}, U_1, \ldots, U_n, \sigma)$ be viewed as a valid signature for the Chow-Yiu-Hui ID-based ring signature scheme, where the message $m = c$. Since the Chow-Yiu-Hui ID-based ring signature scheme has unforgeability against adaptive chosen messages attacks, the improved scheme also has unforgeability against adaptive chosen messages attacks. □

C Proof of Theorem 3

Proof. Since a_s and $a_i (i = 1, \ldots, n, i \neq s)$ are randomly generated, hence $U_1, \ldots, U_n$ are also uniformly distributed. c does not contain any information about the actual signcrypter. We consider whether $\sigma = (h_s + a_s)D_{ID_s}$ leaks information about the actual signcrypter. We know

$$\begin{aligned}\hat{e}(P, \sigma) &= \hat{e}(P, (h_s + a_s)D_{ID_s}) \\ &= \hat{e}(P_{pub}, (h_s + a_s)Q_{ID_s}) \\ &= \hat{e}(P_{pub}, h_s Q_{ID_s})\hat{e}(P_{pub}, a_s Q_{ID_s}) \\ &= \hat{e}(P_{pub}, h_s Q_{ID_s})\hat{e}(P_{pub}, U_s + \sum_{i=1, i\neq s}^{n} (U_i + h_i Q_{ID_i}))\end{aligned}$$

It seems that the adversary can check if the u_j with identity ID_j is the actual signcrypter by checking whether the following equation holds:

$$\hat{e}(P_{pub}, U_j + \sum_{i=1, i\neq j}^{n} (U_i + h_i Q_{ID_i})) = \frac{\hat{e}(P, \sigma)}{\hat{e}(P_{pub}, h_j Q_{ID_j})}.$$

However, this method is of no use, as the above equation not only holds when $j = s$, but also $\forall \in \{1, 2, \ldots, n\} \backslash \{s\}$, i.e. the signature is symmetric. Indeed, the above equation is just the same as the equation to be checked in the verification procedure.

$$\begin{aligned}&\hat{e}(P_{pub}, U_j + \sum_{i=1, i\neq j}^{n} (U_i + h_i Q_{ID_i})) \\ &= \hat{e}(P_{pub}, \sum_{i=1, i\neq s}^{n} U_i + U_s + \sum_{i=1, i\neq j}^{n} h_i Q_{ID_i}) \\ &= \hat{e}(P_{pub}, \sum_{i=1, i\neq s}^{n} U_i + a_s Q_{ID_s} - \sum_{i=1, i\neq s}^{n} (U_i + h_i Q_{ID_i}) + \sum_{i=1, i\neq j}^{n} h_i Q_{ID_i}) \\ &= \hat{e}(P_{pub}, a_s Q_{ID_s} - \sum_{i=1, i\neq s}^{n} h_i Q_{ID_i} + \sum_{i=1, i\neq j}^{n} h_i Q_{ID_i}) \\ &= \hat{e}(P_{pub}, a_s Q_{ID_s} - h_j Q_{ID_j} + h_s Q_{ID_s}) \\ &= \hat{e}(P, a_s D_{ID_s} - h_j D_{ID_j} + h_s D_{ID_s}) \\ &= \hat{e}(P, \sigma - h_j D_{ID_j}) \\ &= \frac{\hat{e}(P, \sigma)}{\hat{e}(P, h_j D_{ID_j})} \\ &= \frac{\hat{e}(P, \sigma)}{\hat{e}(P_{pub}, h_j Q_{ID_j})}\end{aligned}$$

Therefore, the distribution of $(\mathcal{U}, c, R, U_1, \ldots, U_n, \sigma)$ are independent and uniformly distributed no matter who is the actual signcrypter. Any adversary cannot identify the actual signcrypter with probability better than random guess. That is, the adversary can only output the identity of the actual signcrypter with probability $1/n$. So the improved scheme has the unconditional signcrypter ambiguity property. □

D Proof of Theorem 4

Proof. If u_s with identity ID_s produces a ciphertext $C = (\mathcal{U}, c, R, U_1, \ldots, U_n, \sigma)$, obviously, he can authenticate the ownership of her signcryption by the above scheme. The other members of the group cannot authenticate the ciphertext C to be produced by themselves. If a member u_a with identity ID_a can find some values μ', y', ν', where $\mu' = \hat{e}(P, \sigma)^{x'}$, which can pass the authentication algorithm, i.e. the following equation holds:

$$\hat{e}(P_{pub}, Q_{ID_a})^{\nu'} = \mu' \hat{e}(P, \sigma)^{y'}$$

we can obtain

$$\hat{e}(P_{pub}, Q_{ID_a})^{\frac{\nu'}{x'+y'}} = \hat{e}(P, \sigma) = \hat{e}(P_{pub}, Q_{ID_s})^{h_s + a_s}$$

That is, $\frac{\nu'}{x'+y'} Q_{ID_a} = (h_s + a_s) Q_{ID_s}$ holds. Since the adversary does not know the random number a_s, it is impossible for he to find such μ', y', ν' because of the discrete logarithm problem. Therefore, The improved scheme has the authenticatability property. □