Computing and Informatics, Vol. 32, 2013, 441–460

NMIBAS: A NOVEL MULTI-RECEIVER ID-BASED ANONYMOUS SIGNCRYPTION WITH DECRYPTION FAIRNESS

Liaojun Pang

School of Life Sciences and Technology
Xidian University
Xi'an 710071, China
&
Department of Computer Science
Wayne State University
Detroit MI48202, USA
e-mail: liaojun.pang@wayne.edu, ljpang@mail.xidian.edu.cn

Huixian Li

School of Computer Science and Engineering
Northwestern Polytechnical University
Xi'an 710072, China
&
Department of Computer Science
Wayne State University
Detroit MI48202, USA

Yumin Wang

State Key Laboratory of Integrated Service Networks
Xidian University
Xi'an 710071, China

Abstract. Based on the ring signature technology, the multi-receiver ID-based anonymous signcryption (MIBAS) is proposed, and its goal is to protect the privacy of the sender or so-called signer. In an MIBAS scheme, every receiver can verify whether the sender is a member of a trusted group and thus ensure the reliability of the message source, but he could not get the real sender. However, MIBAS paid no attention to privacy of the receivers and has not taken the privacy of the receivers into account during its design. Our analyses show that there widely exist the receiver privacy exposure and decryption unfairness problems in the existing multi-receiver ID-based signcryption schemes. Motivated by these concerns, a new multi-receiver ID-based anonymous signcryption (nMIBAS) is proposed to protect the identity of the receivers. The nMIBAS scheme can not only solve the problem that the existing schemes cannot protect the privacy of receivers, but also meet the fairness of decryption to prevent the possible cheating behavior of the sender effectively. Analysis shows that this scheme is a secure and effective signcryption scheme.

Keywords: Decryption fairness, multi-receiver signcryption, ID-based signcryption, anonymity, signcryption

Mathematics Subject Classification 2010: 94A60

1 INTRODUCTION

In broadcasting or multicasting services, the message sender usually needs to transmit some sensitive information by the broadcasting channel, and hopes that only the authorized users can get the information while the unauthorized one can get nothing. Therefore, the sender has to encrypt the message before broadcasting it. On the other hand, the users also hope to authenticate the source of the received messages to avoid receiving some boring information. Due to the two requirements above, the concept of the multi-receiver signcryption [1] is proposed, which is the fusion result of the multi-receiver encryption technology and the signcryption technology. Since the multi-receiver signcryption scheme can use only one signcryption operation to implement broadcasting the same message securely to many receivers simultaneously, it is more effective and practical than the traditional one-to-one scheme, which makes it especially suitable for network secure broadcast and secure multicast. At present, the multi-receiver signcryption and its applications have become a hot spot in the field of information security.

However, as people paid more and more attention to personal privacy issues, how to protect the identity of the participants from being exposed has been a challenge to multi-receiver signcryption designer. Recently, the multi-receiver anonymous signcryption [2] has been proposed, and it is expected to solve the sender's privacy exposure problem; that is to say, the sender hopes that the authorized users only can verify whether the messages comes from a member of a reliable group but cannot get the sender's true identity. In such an anonymous scheme, the sender of the messages hides his/her identity in a set of identities and uses his/her own private key to signcrypt a piece of information, and then broadcasts the ciphertext.

Upon receiving the ciphertext, each authorized receiver can use his/her private key to verify the validity of the ciphertext and decrypt it to get the plaintext.

In practical applications, participant privacy does not mean only the privacy of the sender; the receivers also want to keep it secret to others that they have received a message. Unfortunately, none of the existing multi-receiver signcryption schemes [2, 3, 4, 5, 6, 9] have taken receiver privacy into account. In fact, these schemes completely reveal receiver identity in the ciphertext, because in these schemes, the list of identities of all authorized users and the correlation order is a part of the ciphertext. In addition to the privacy issues, this kind of disposal in the existing schemes can also lead to the decryption unfairness problem, that is to say, when the ciphertext information is partly damaged, it is possible for part of the authorized users to decrypt the ciphertext correctly while it is impossible for others. This decryption unfairness problem can definitely affect the applications of the multi-receiver signcryption scheme. Moreover, this weakness can probably give a chance to the sender to cheat a receiver whom s/he hates by sending him or her a partly distorted message, without being perceived.

Motivated by these concerns, we shall propose a new scheme to solve the receivers' identity exposure and decryption unfairness problems. In our scheme, the ciphertext does not include the list of the receiver identities directly, which avoids the receiver's privacy exposure. At the same time, the whole ciphertext of our scheme is necessary for each receiver to implement the correct decryption, and any distortion in the ciphertext will lead to impossible decryption to all receivers. Compared with the existing schemes, in addition to secrecy and unforgeability, our scheme also has the following advantages:

1. The receiver is kept anonymous. The identity of the receiver will not be leaked by the ciphertext like the existing schemes, which can protect their privacy.
2. Decryption process is fair for all the receivers, which makes all authorized receivers have the same probability to get the correct plaintext.

The rest of this paper is organized as follows. In Section 2, we introduce related works. In Section 3, we introduce some preliminaries about mathematical backgrounds and security definitions used in this paper. In Section 4, we present our proposed scheme in details. In Section 5, we prove our scheme's security, and then evaluate and compare it with the existing schemes. In Section 6, we summarize our work.

2 RELATED WORK

The concept of signcryption was first proposed by Zheng [7] in 1997, and its main idea is to deal with the public key encryption and digital signature at the same time. Compared with the traditional signature-then-encryption mode, this method needs less computation and communication cost. Since then, researchers paid more and more attention to signcryption [8, 9]. In 2002, the first ID-based signcryption scheme [8] was proposed. However, these schemes are only one-to-one scheme, that is to say the sender could signcrypt a message only for one receiver in each operation. When the sender needs to transmit the same message to multiple receivers, s/he has to repeat the same signcryption process for each receiver.

When transmitting the same message to many receivers, the traditional encryption scheme is low in efficiency and real time because the same encryption process should be repeated multiple times [10]. Therefore, the concept of multi-receiver encryption is put forward. Fusing the concept of multi-receiver encryption and the thought of signcryption, Duan et al. [1] put forward the first multi-receiver ID-based signcryption in 2006. In their scheme, the sender signcrypts the messages once, and each authorized receiver can use his/her own private key to check the validity of the received ciphertext and decrypt it simultaneously. However, in its scheme, the ciphertext includes every receiver's identity information which is necessary for decryption, because without the list of the receivers, the receiver cannot correctly locate and find what s/he needs for the decryption. Although the receiver list is not definitely included in the ciphertext of the scheme [1], we think that missing the receivers' identity list may be caused by inattention of the authors. In 2007, a more efficient multi-receiver ID-based signcryption algorithm was proposed in [3], and it definitely added a receivers' identity list into the ciphertext, which corrects the mistake in [1]. Since then, other similar schemes [4, 5] have been put forward early or late.

The design philosophy of anonymous signature was derived from ring signature, which was proposed by Rivest et al. [11] in 2001 originally. This scheme assures that the receiver could not know the real signer (i.e. the sender) of the messages, but can verify whether the signer is a member of a trusted group, which will not only satisfy the anonymity of the signer, but also ensure the reliability of the message source. By using the ring signature, Huang et al. [12] proposed the first ID-based anonymous signcryption scheme in 2005. With the same idea, Lal et al. extend it to the multi-receiver case and proposed the first sender-anonymous multi-receiver ID-based signcryption in [2]. In this scheme, the identity of the real sender is put in a set of identities to achieve anonymity of the sender, and the receiver only knows the received messages are signed by one person in this set and thus trusts the source of the messages, but s/he cannot know who has signed the messages. In 2010, the literature [15] proposed another multi-receiver signcryption scheme satisfying the anonymity of the sender. In this scheme, there also exists the decryption unfeasibility problem because of lack of the receivers' identity list in the ciphertext. We also can easily find that the existing multi-receiver anonymous signcryption [2, 15] schemes only consider the anonymity of the sender, without taking the receiver's anonymity problem into account.

Through the above analyses, it can be concluded that either the existing multi-receiver signcryption schemes [1, 2, 3, 4, 5, 6, 15] do not consider anonymity, or they just consider the anonymity of the sender, and do not mention the receiver's anonymity. In fact, for all the above schemes, the ciphertext must include the receivers' identity list (maybe there is an omission in the schemes [1, 15]), because the receiver list and the receiver order help each receiver to locate and find what s/he needs for the decryption in the ciphertext. However, including the receiver list into the ciphertext can inevitably lead to some defects as follows. First, it directly exposes the receiver identity, and in fact no one wants to reveal his/her privacy in practical applications. Second, the needed information of each receiver is only a part of the ciphertext, so there may exist the unfairness possibility in decryption. If an error appears in the process of transmission, it will lead to the result that some receivers can verify or decrypt the messages correctly, but others can not. More serious problem is that the scheme is unable to avoid the sender's duplicitous attack, for example, the sender deliberately gives a wrong message to a receiver [16, 17].

Motivated by these concerns, we shall present a new anonymous multi-receiver signcryption scheme which can meet the receiver's and the sender's anonymity simultaneously. Our scheme uses a special set to confuse the real identities of the receivers, and does not contain the receivers' identity list in the ciphertext, so the identity of each authorized receiver is sightless. Thus, not only the attacker cannot get the information of the receivers, but also each authorized receiver cannot get anything about others' identity, so the receivers' privacy issue is well solved. In addition, because the ciphertext is transmitted by the broadcasting channel, anyone can receive the broadcasted information but only the authorized ones can decrypt correctly. So in our scheme we provide a method for the users to determine if they have the decryption permissions to avoid the unnecessary decryption computation of unauthorized users. Because the necessary information of each receiver is the same, once some element is damaged, no receiver can decrypt it correctly, which makes our scheme meet the decryption fairness.

3 PRELIMINARIES

3.1 Security Assumptions

In this section, we shall briefly introduce some security assumptions used in our scheme.

Let G_1 be an additive group and G_2 be a multiplicative group of the same order q and let P be a generator of G_1. Let $e : G_1 \times G_2 \to G_2$ be a bilinear mapping. The CDH and DBDH problems can be described as follows.

1. Computational Diffie-Hellman (CDH) Problem: Given $\langle P, aP, bP\rangle$ for some $a, b \in Z_q^*$, to compute abP.
2. Decisional Bilinear Diffie-Hellman (DBDH) Problem: Given $\langle P, aP, bP, cP, Z\rangle$ for some $a, b, c \in Z_q^*, Z \in G_2$, to decide if $Z = e(P, P)^{abc}$.

Definition 1. CDH Assumption: We define an algorithm B with an output $\beta \in \{0, 1\}$, which has advantage $Adv_B^{CDH} = Pr[B(P, aP, bP) = abP : a, b \in Z_q^*]$ in solving the CDH problem. If for any polynomial-time algorithm the advantage Adv_B^{CDH} is negligible, we say that the CDH assumption holds.

Definition 2. DBDH Assumption: We define an algorithm B with an output $\beta \in \{0,1\}$, which has advantage $Adv_B^{DBDH} = Pr[B(P, aP, bP, cP, e(P,P)^{abc}) = 1] - Pr[B(P, aP, bP, cP, Z) = 1]$ in solving the DBDH problem, where $a, b, c \in Z_q^*$ and $Z \in G_2$. If for any polynomial-time algorithm the advantage Adv_B^{DBDH} is negligible, we say that the DBDH assumption holds.

3.2 Multi-Receiver Identity-Based Anonymous Signcryption (MIBAS)

Formal definition of a MIBAS scheme consists of four algorithms, namely: KeyGen, Extract, Anony-signcrypt and De-signcrypt, described as follows.

KeyGen: The Private Key Generator (PKG) runs this algorithm to generate a master key s_0 and public parameters *params*. Note that the public parameters should be published while the master key should be kept secret.

Extract: This is the private key extraction algorithm run by PKG. Inputting an identity ID_i, PKG's master key s_0 and the public parameter *params*, PKG runs this algorithm to generate the private key d_i associated with ID_i, namely $d_i = \text{Extract}(ID_i, s_0, params)$. Here, the identity ID_i is used as the public key and d_i is the corresponding private key.

Anony-signcrypt: This algorithm is run by the sender or so-called signer. Inputting PKG's public parameter *params*, a plaintext message M, a set of m identities $L = (ID_1, ID_2, K, ID_m)$ selected by the sender, which contains the sender's identity ID_s, that is to say $ID_s \in L$, the receivers' identity set $L' = (ID'_1, ID'_2, K, ID'_n)$, and the sender's private key d_s, the sender runs this algorithm to generate the ciphertext C associated with M, namely $C = \text{Anony-signcrypt}(params, M, L', L, d_s)$. Note: In our MIBAS scheme, we shall let C meet $L' \notin C$, and use a pseudo-identity list to replace the real receiver list L' for the sake of anonymity of the receivers.

De-signcrypt: This algorithm is run by the receivers. Inputting the ciphertext C, PKG's public parameter *params*, the receiver's identity $ID'_i (i \in 1, 2, \ldots, n)$ and his private key d'_i, the receiver runs this algorithm to decrypt the ciphertext. If the ciphertext C is valid and the receiver is an authorized one, this algorithm outputs the corresponding plaintext M, namely $M = \text{De-signcrypt}(C, params, ID'_i, d'_i)$; otherwise it outputs an error message $\perp$.

3.3 Security Model

3.3.1 Message Confidentiality

For message confidentiality, the most widely accepted security model is the ciphertext indistinguishability under the chosen-ciphertext attack (CCA). It was proposed in the scheme [8] first, and then Duan et al. [1] expanded it to the multi-receiver environment, and described it as indistinguishability of ciphertexts under selective multi-ID, chosen ciphertext attack (IND-sMIBSC-CCA). Later, Lal et al. [2] extended it to the anonymous environment, and described it as indistinguishable against chosen ciphertext attacks (IND-sMIBAS-CCA2), which is described as follows.

Definition 3. IND-sMIBAS-CCA2 (indistinguishable against chosen ciphertext attacks (IND-sMIBAS-CCA2): Let A be a polynomial-time attacker. Let Π be a general multi-receiver ID-based anonymous signcryption scheme. Consider that A interacts with a Challenger B in the following game:

Setup: B runs the KeyGen algorithm to generate a master key s_0 and the system public parameter *params*. Then, B gives *params* to A and keeps s_0 secret. Upon receiving *params*, A outputs n target identities denoted as $L'^* = \{ID_1'^*, ID_2'^*, \ldots, ID_n'^*\}$.

Phase 1: A probes B with the following queries adaptively.

Extract queries: Upon receiving the Extract query from A about the identity $ID(ID \neq ID_i'^*, i = 1, 2, \ldots, n)$, B runs the Extract algorithm to compute $d_{ID} = \text{Extract}(ID, s_0, \mathit{params})$, and then sends it to A.

Anony-signcrypt queries: A defines a group of m identities denoted as $L = \{ID_1, ID_2, \ldots, ID_m\}$, a plaintext denoted as M, and a group of n receivers denoted as $L' = \{ID_1', ID_2', \ldots, ID_n'\}$. B randomly chooses an identity $ID_i \in L$, computes its private key d_i and the corresponding ciphertext as $C = \text{Anony-signcrypt}(\mathit{params}, M, L', L, d_i)$. Then, B sends the ciphertext C to A.

De-signcrypt queries: A defines a group of m identities denoted as $L = \{ID_1, ID_2, \ldots, ID_m\}$, a group of n receivers denoted as $L' = \{ID_1', ID_2', \ldots, ID_n'\}$ and a ciphertext denoted as C. B firstly chooses a receiver $ID_j' \in L'$, and computes its private key d_j'. If the ciphertext C is valid, B computes the plaintext as $M = \text{De-signcrypt}(C, \mathit{params}, M, L, d_j')$, and sends M to A; otherwise, outputs an error message $\perp$.

Challenge: A chooses a pair of messages (M_0, M_1) that have the same length, and a group of m identities denoted as $L^* = \{ID_1^*, ID_2^*, \ldots, ID_m^*\}$, where each $ID_i^*(i = 1, 2, \ldots, m)$ has not been used to query the Extract oracle. Upon receiving the messages (M_0, M_1), B randomly chooses a bit $\beta \in \{0, 1\}$ and computes the ciphertext $C^* = \text{Anony-signcrypt}(\mathit{params}, M_\beta, L'^*, L^*, d_i^*)$, where d_i^* is the private key of ID_i^*. Then, B sends C^* to A.

Phase 2: A issues new queries as in Phase 1. Here, A cannot ask the Extract queries on anyone in L^*, nor ask De-signcrypt queries on the ciphertext C^*. Also, A cannot ask De-signcrypt queries on the ciphertext C that is only different from C^* in the receivers' information.

Guess At the end of the game, A outputs a guessed bit $\beta' \in \{0, 1\}$. If $\beta' = \beta$, A wins the game.

The adversary A defined above is called an IND-sMIBSC-CCA2 adversary, and its probability advantage is defined as follows:

$$\text{Adv}_{\Pi}^{\text{IND-sMIBSC-CCA2}}(A) = \left| \Pr[\beta = \beta'] - \frac{1}{2} \right|. \tag{1}$$

If for any IND-sMIBSC-CCA2 adversary A, its guessing advantage is less than ε within running time t, then we call the scheme Π to be (t, ε)-IND-sMIBSC-CCA2 secure.

3.3.2 Unforgeability

Any signcryption scheme should meet unforgeability, which means the sender cannot deny the fact that s/he has signed some message. Duan et al. [1] defined the unforgeability as strong existential unforgeability under selective multi-ID, chosen message attack (SUF-sMIBSC-CMA). Similarly, Lal et al. [2] extended their definition to suit the anonymous case, and called it the existentially unforgeable against adaptive chosen message attack (EUF-MIBAS-CMA), which shall be described as follows:

Definition 4 (EUF-MIBAS-CMA)**.** Suppose F is a Forger, and let Π denote a multi-receiver ID-based anonymous signcryption scheme. Consider that F interacts with a Challenger B in the following game:

Setup: B runs the KeyGen algorithm to generate a master key s_0 and the public parameter *params*. Then, B gives *params* to F and keeps s_0 secret.

Attack: F issues queries as those in Definition 3.

Forgery: F finally outputs a new ciphertext denoted as C^* and a group of n receivers denoted as $L'^* = \{ID_1'^*, ID_2'^*, \dots, ID_n'^*\}$. If it can be checked that C^* is generated by ID_s^* based on the plaintext M and $L^* = \{ID_1^*, ID_2^*, \dots, ID_m^*\}$ and can be correctly decrypted by anyone in L'^*, F wins the game. Here, F cannot ask Extract query on anyone in groups L^* and L'^*, and C^* can not be generated by the Anony-signcrypt algorithm. The advantage of F is defined as its success probability.

4 THE PROPOSED SCHEME (NMIBAS)

Our nMIBAS scheme includes the following four algorithms named KeyGen, Extract, Anony-signcrypt and De-signcrypt respectively, which are described as follows.

4.1 The KeyGen Algorithm

The KeyGen algorithm is carried out by PKG, and includes the following steps:

1. Let G_1 and G_2 be an additive group and a multiplicative group with the order $q \geq 2^k$, where k is a given security parameter, and let P be a generator of G_1. Choose a bilinear mapping $e : G_1 \times G_1 \rightarrow G_2$.
2. Randomly choose an integer $s_0 \in Z_q^*$ as the master key and let $P_{pub} = s_0 P \in G_1$ be the corresponding public key. In succession, randomly choose $P_0 \in G_1^*$ and compute $g = e(P_{pub}, P_0)$.

3. Choose 4 cryptographic one-way hash functions: $H_1 : \{0,1\}^* \rightarrow G_1$; $H_2 : G_2 \rightarrow \{0,1\}^{l_0}$; $H_3 : \{0,1\}^{l_0} \times G_1 \rightarrow Z_q^*$; $H_4 : \{0,1\}^* \rightarrow Z_q^*$, where l_0 denotes the bit length of the plaintext message.
4. Publish the system parameter $params = \langle G_1, G_2, q, e, P, P_{pub}, P_0, g, H_1, H_2, H_3, H_4 \rangle$, and store the master key s_0 in a secure way.

4.2 The Extract Algorithm

The Extract algorithm should also be carried out by PKG. With *params*, s_0 and a participant identity $ID \in \{0,1\}^*$ as input, PKG runs this algorithm process as the following steps:

1. Compute the public key of the identity ID as $Q_{ID} = H_1(ID)$.
2. Compute $d_{ID} = s_0 Q_{ID}$, and let d_{ID} be the private key of the participant ID.

4.3 The Anony-Signcrypt Algorithm

The Anony-signcrypt algorithm is carried out by the message sender, that is to say the sender of the message. Let ID_S be the true message sender, and let $L' = \{ID'_1, ID'_2, \ldots, ID'_n\}$ denote the set of n receivers selected by the sender. With the system public parameters *params* and a plaintext messageas M as input, ID_S does the following steps to signcrypt the message M:

1. Choose a set of participants $L = \{ID_1, ID_2, \ldots, ID_m\}$, such that $ID_S \in L$ and $L \cap L' = \phi$. These participants are used to puzzle the message receivers and the adversary to prevent them from obtaining the true identity of the sender.
2. Choose $(m-1)$ integersrandomly and compute $R_i = u_i P$ where $i \in \{1, 2, \ldots, m\} \setminus \{S\}$.
3. Randomly choose an integer $u_S \in Z_q^*$, and then compute $\alpha = \sum_{i=1}^{m} u_i, U = \alpha P, \sigma = g^{\alpha}$ and $W = H_2(\sigma) \oplus M$.
4. Compute $h_i = H_3(W, R_i)$ for all $i \in \{1, 2, \ldots, m\} \setminus \{S\}$, and let $R_S = u_S Q_S - \sum_{i=1, i \neq S}^{m} (R_i + h_i Q_i)$. Here, Q_S is the public key of ID_S. At last, set $R = \{R_1, R_2, \ldots, R_m\}$.
5. Compute $V = (u_S + h_S) \cdot d_S$, where $h_S = H_3(W, R_S)$ and d_S denotes the private key of ID_S.
6. Let $x_j = H_4(ID'_j)$ and $y_j = \alpha(P_0 + Q'_j)$, where $j = 1, 2, \ldots, n$ and Q'_j denotes the public key of ID'_j, and thus we can get n pairs: $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$.
7. For $j = 1, 2, \ldots, n$, compute $f_j(x) = \prod_{1 \leq j \neq j' \leq n} \frac{x - x_{j'}}{x_j - x_{j'}} = a_{j,1} + a_{j,2}x + \ldots + a_{j,n}x^{n-1}$, where $a_{j,1}, a_{j,2}, \ldots, a_{j,n} \in Z_q$.
8. For $j = 1, 2, \ldots, n$, compute $T_j = \sum_{j'=1}^{n} a_{j',j} y_{j'}$ and let $T = \{T_1, T_2, \ldots, T_n\}$.
9. Define the ciphertext of the plaintext M as $C = \langle U, V, W, T, R, L \rangle$.

4.4 The De-Signcrypt Algorithm

The De-signcrypt algorithm can be carried out by each authorized receiver. With the ciphertext $C = \langle U, V, W, T, R, L \rangle$ and the system public parameters *params* as input, each receiver $ID'_j (j = 1, 2, \ldots, n)$ can use his/her private key d'_j to decrypt C to get the plaintext M, which can be shown as the following three sub-algorithms:

Verify sub-algorithm: This sub-algorithm is used to check the validity of the senders in the set L.

1. Compute $K = \sum_{i=1}^{m}(R_i + h_i Q_i)$, where $h_i = H_3(W, R_i), i = 1, 2, \ldots, m$.
2. Check whether the equation $e(V, P) = e(K, P_{pub})$ holds. If yes, the sender must be in the group L; otherwise, stop the process.

Judge sub-algorithm: This sub-algorithm is used to check the decryption rights of the receiver.

1. Check whether the equation $V \cdot Q'_j = K \cdot d'_j$ holds. If yes, ID'_j can run the following decryption process; otherwise, stop the process.

Decrypt sub-algorithm: This sub-algorithm is used to decrypt the ciphertext.

1. Compute $\delta_j = T_1 + x_j T_2 + \ldots + (x_j^{n-1} mod q)T_n$, where $x_j = H_4(ID'_j)$.
2. Compute $\sigma' = e(P_{pub}, \delta_j) \cdot e(U, d'_j)^{-1}$ and $M = H_2(\sigma') \oplus W$. Here, M is the plaintext message.

5 ANALYSES AND DISCUSSIONS

5.1 Correctness Analyses

Theorem 1 (Correctness of the Verify sub-algorithm)**.** That is to say, the Verify sub-algorithm can be used to verify the validity of the sender.

Proof. According to the process defined in Section 4.3, we have

$$\begin{aligned} e(V, P) &= e((u_S + h_S)d_S, P) = e(u_S Q_S + h_S Q_S, P_{pub}) \\ &= e\left(\sum_{i=1, i\neq S}^{m}(R_i + h_i Q_i) + R_S + h_S Q_S, P_{pub}\right) \\ &= e\left(\sum_{i=1}^{m}(R_i + h_i Q_i), P_{pub}\right) \\ &= e(K, P_{pub}). \end{aligned} \tag{2}$$

From Equation (2), it can be concluded that this theorem holds. □

Theorem 2 (The correctness of the Judge sub-algorithm)**.** That is to say, the Judge sub-algorithm can be used to verify whether a receiver is an authorized one.

Proof. For each $ID'_j (j \in \{1, 2, \ldots, n\})$, we have:

$$\begin{aligned} V \cdot Q'_j &= (u_S + h_S) d_S \cdot Q'_j = (u_S Q_S + h_S Q_S) \cdot d'_j \\ &= \left(\sum_{i=1, i \neq S}^{m} (R_i + h_i Q_i) + R_S + h_S Q_S \right) \cdot d'_j \\ &= \sum_{i=1}^{m} (R_i + h_i Q_i) \cdot d'_j = K \cdot d'_j. \end{aligned} \tag{3}$$

That is to say, the equation $V \cdot Q'_j = K \cdot d'_j$ holds. □

Theorem 3 (Correctness of the Decrypt sub-algorithm)**.** That is to say, the Decrypt sub-algorithm can recover the plaintext correctly.

Proof. For each $ID'_j (j \in \{1, 2, \ldots, n\})$, we can compute δ_j as follows:

$$\begin{aligned} \delta_j &= T_1 + x_j T_2 + \ldots + x_j^{j-i} T_j + \ldots + x_j^{n-1} T_n \\ &= (a_{1,1}\alpha(P_0 + Q'_1) + \ldots + a_{n,1}\alpha(P_0 + Q'_n)) + \\ &\quad (x_j a_{1,2}\alpha(P_0 + Q'_1) + \ldots + x_j a_{n,2}\alpha(P_0 + Q'_n)) + \ldots + \\ &\quad (x_j^{j-1} a_{1,j}\alpha(P_0 + Q'_1) + \ldots + x_j^{j-1} a_{n,j}\alpha(P_0 + Q'_n)) + \ldots + \\ &\quad (x_j^{n-1} a_{1,n}\alpha(P_0 + Q'_1) + \ldots + x_j^{n-1} a_{n,n}\alpha(P_0 + Q'_n)) \\ &= (a_{1,1} + a_{1,2}x_j + \ldots + a_{1,n}x_j^{n-1})\alpha(P_0 + Q'_1) + \\ &\quad (a_{2,1} + a_{2,2}x_j + \ldots + a_{2,n}x_j^{n-1})\alpha(P_0 + Q'_2) + \ldots + \\ &\quad (a_{j,1} + a_{j,2}x_j + \ldots + a_{j,n}x_j^{n-1})\alpha(P_0 + Q'_j) + \ldots + \\ &\quad (a_{n,1} + a_{n,2}x_j + \ldots + a_{n,n}x_j^{n-1})\alpha(P_0 + Q'_n) \\ &= \alpha(P_0 + Q'_n). \end{aligned} \tag{4}$$

Then, we have $\sigma' = e(P_{pub}, \delta_j) \cdot e(U, d'_j)^{-1}$, because:

$$\begin{aligned} \sigma' &= e(P_{pub}, \delta_j) \cdot e(U, d'_j)^{-1} \\ &= e(P_{pub}, \alpha(P_0 + Q'_j)) \cdot e(\alpha P, s_0 Q'_j)^{-1} \\ &= e(P_{pub}, \alpha P_0) \cdot e(P_{pub}, \alpha Q'_j) \cdot e(s_0 P, \alpha Q'_j)^{-1} \\ &= e(P_{pub}, P_0)^{\alpha} \cdot e(P_{pub}, \alpha Q'_j) \cdot e(P_{pub}, \alpha Q'_j)^{-1} \\ &= g^{\alpha} = \alpha. \end{aligned} \tag{5}$$

Through the results above, we have $M = H_2(\sigma') \oplus W$. □

5.2 Security Analyses

Our multi-receiver anonymous signcryption scheme can meet the message confidentiality, the signcryption unforgeability, the sender anonymity and the receiver anonymity. Like the scheme [2], the sender anonymity problem is solved by using the ring signature technology, which makes anyone guarantee the sender is one of a set of valid participants but cannot specify who is the exact sender. The sender anonymity proof is similar to the proof of Theorem 2 in [14], and it will not be repeated here. In addition, the list of the receiver identities is not included in the ciphertext, and this makes the receivers anonymous, which shall be discussed in the next section. Therefore, here we should pay more attention to the message confidentiality proof and to signcryption unforgeability, which can be described by the following theorems.

Theorem 4 (Message confidentiality)**.** Suppose that there is an IND-sMIBA-S-CCA2 adversary A having an advantage ε to win the game defined in Definition 3 within running time t. (Here, assume that adversary A can ask q_e queries to Extract, q_s queries to Anony-signcryption, q_d queries to De-signcryption, and q_{H_i} queries to H_i ($i = 1, 2, 3, 4$) at most). Then, there is an algorithm B that can solve the DBDH problem with an advantage $\varepsilon' \geq \varepsilon - \frac{nq_d}{2^k}$ within running time $t' \leq t + 4q_d O(t_1)$, where t_1 is the time consumed by a bilinear pair computation.

Proof. In the following section, we shall show how an algorithm B uses A to solve the DBDH problem with an advantage ε' within running time t'.

First, suppose B is given an instance of the DBDH problem as $\langle P, aP, bP, cP, Z\rangle$, and its aim is to judge whether the formula $Z = e(P,P)^{abc}$ holds or not. B can simulate the Challenger to execute each phase in Definition 3. During this process, A can ask queries to Anony-signcryption, De-signcryption and H_i, $i = \{1, 2, 3, 4\}$ oracles. The results of querying H_i, $i = \{1, 2, 3, 4\}$ are stored in H_i-list, $i = \{1, 2, 3, 4\}$ respectively.

Setup: B sets $P_0 = bP$ and $P_{pub} = cP$, and let $g = e(P_0, P_{pub}) = e(bP, cP) = e(P,P)^{bc}$. Then, give A the system parameters $params = \langle G_1, G_2, q, e, P, P_{pub}, P_0, g, H_1, H_2, H_3, H_4\rangle$. On receiving the system parameter, A outputs n target identities denoted as $L'^{*} = (ID_1'^{*}, ID_2'^{*}, \ldots, ID_n'^{*})$.

Phase 1: A queries B as follows.

H_1**-query:** Input an identity ID_k to H_1. If there exists the tuple (ID_k, l_k, Q_k) in H_1-list, return Q_k; otherwise, do the following steps:

1. If $ID_k = ID_j'^{*}$, $j \in \{1, 2, \ldots, n\}$, choose an integer $l_j'^{*} \in Z_q^*$ at random, and compute $Q_j'^{*} = l_j'^{*}P - P_0$. Otherwise, randomly choose an integer $l_k \in Z_q^*$ and compute $Q_k = l_kP$.
2. Put (ID_k, l_k, Q_k) into H_1-list, and return Q_k.

H_i-query, $i \in \{2, 3, 4\}$: In order to reply to these queries, B should firstly access the corresponding H_i-query, $i \in \{2, 3, 4\}$. If the corresponding query can be found, return it to A. Otherwise, B should randomly choose an integer within the suitable range as the query result and return it to A. At the same time, add the query result to the corresponding list.

Extract query: When B receives the private key extract query about the identity ID_k(here $ID_k \neq ID_j'^*$), finds (ID_k, l_k, Q_k) out from H_1-list, and computes $d_k = l_k P_{pub} = cl_k P$. At last, return d_k to A.

Anony-signcrypt query: When B receives the anony-signcrypt query (M, L, L') (here $L = \{ID_1, ID_2, \ldots, ID_m\}$ and $L' = \{ID_1', ID_2', \ldots, ID_n'\}$), it randomly chooses $ID_S \in L$ firstly, and then has two choices as follows:

1. If $ID_S \neq ID_j'^*$ for all $j \in \{1, 2, \ldots, n\}$, B can access H_1-list and compute the private key of ID_S as $d_S = l_S P_{pub} = cl_S P$. Then, with (M, d_S, L, L') as the input of the Anony-signcrypt algorithm, B computes the ciphertext C and returns it to A.
2. If there exits some $j \in \{1, 2, \ldots, n\}$ such that $ID_S = ID_j'^*$, set $Q_S = l_S P - P_0$. Then, choose $u_1, u_2, \ldots, u_S, \ldots, u_m \in Z_q^*$ at random, and compute $\alpha = \sum_{i=1}^m u_i, \sigma = g^\alpha$ and $W = H_2(\sigma) \oplus M$. For all $i \in \{1, 2, \ldots, m\} \backslash \{S\}$, compute $R_i = u_i P$ and $h_i = H_3(M, R_i)$, and then save them in H_3-list. In succession, compute $U = \alpha P$, $x_j = H_0(ID_j')$ and $y_j = \alpha(P_0 + Q_j')$ for all $j = 1, 2, \ldots, n$. Then, for all $j = 1, 2, \ldots, n$, compute $f_j(x) = \prod_{1 \leq j \neq j' \leq n} \frac{x - x_{j'}}{x_j - x_{j'}} = a_{j,1} + a_{j,2} x + \ldots + a_{j,n} x^{n-1}$ such that $a_{j,1}, a_{j,2}, \ldots, a_{j,n} \in Z_q$, and let $T_j = \sum_{j'=1}^n a_{j',j} y_{j'}$. For $i = S$, choose $h_S \in Z_q^*$ randomly and let $R_S = u_S P - h_S Q_S'^* - \sum_{i=1, i \neq S}^m (R_i + h_i Q_i'^*)$ and $V = u_S P_{pub}$. Then, save (W, R_S, h_S) in H_3-list. Finally, B outputs the ciphertext C and returns it to A.

De-signcrypt query: A outputs a ciphertext $C = \langle U, V, W, T, R, L \rangle$ and a receiver identity $ID_j', j \in \{1, 2, \ldots, n\}$ to query B to start the De-signcrypt query.

If $ID_j' \in L'^*$, B does not know the private key of ID_j', and thus it has to return that the ciphertext C is invalid. However, if C is valid, the probability that A does not find is not more than $\frac{n}{2^k}$.

If $ID_j' \notin L'^*$ and B can check whether the equation $e(V, P) = e(\sum_{i=1}^m (R_i + h_i Q_i), P_{pub})$ holds, B accesses H_1-list to get the private key d_j' of ID_j', and figures out δ_j. With the computation results above, B can compute $\sigma' = e(P_{pub}, \delta_j) \cdot e(U, d_j')^{-1}$ and then obtain the plaintext message as $M = H_2(\sigma') \oplus W$. At last, B returns M to A. Otherwise, the ciphertext C is invalid and B only needs to output the error message $\perp$.

Challenge: A outputs two messages (M_0, M_1) with the same length and a set of m participants denoted as $L^* = \{ID_1^*, ID_2^*, \ldots, ID_m^*\}$. Here, the set of the receivers $L'^* = \{ID_1'^*, ID_2'^*, \ldots, ID_n'^*\}$ is the aim of the attack. B randomly chooses a bit $\beta \in \{0, 1\}$, and then signcrypts the message M_β. First, B sets $U^* = aP$, $\sigma = Z$, and accesses H_1-list to get the value $l_j'^*$ corresponding to $ID_j'^*, i \in \{1, 2, \ldots, n\}$. Second, work out $y_j^* = l_j'^* U^*, j \in \{1, 2, \ldots, n\}$, and $T_j'^*, j \in \{1, 2, \ldots, n\}$. At last, B generates a goal ciphertext $C^* = \langle U^*, V^*, W^*, T^*, R^*, L^* \rangle$ and sends it to A.

Phase 2: A carries out multiple queries as in Phase 1. Here, it is noticed that A cannot query the identity information in L^* during the Extract queries, and cannot query the ciphertext during the De-signcryption queries. At the same time, A cannot query a ciphertext C which is only different from that in the pseudo-identity information T.

Guess: In the end, A should output its guess $\beta' \in \{0,1\}$. If $\beta' = \beta$, B outputs 1 as the answer to the DBDH problem, because:

$$\begin{aligned} Z &= e(P_{pub}, y_j^*)e(U^*, d_j'^*)^{-1} \\ &= e(cP, l_j'^* U^*)e(U^*, d_j'^*)^{-1} \\ &= e(cP, l_j'^* aP)e(aP, l_j'^* cP - cdP)^{-1} \\ &= e(cP, l_j'^* aP)e(aP, l_j'^* cP)^{-1}e(aP, -cdP)^{-1} \\ &= e(P,P)^{abc}. \end{aligned} \tag{6}$$

Otherwise, B answers 0.

Analyses: Now, we shall determine the probability advantage of B. For q_d de-signcryption queries, the probability that B rejects the valid ciphertext is not more than $\frac{nq_d}{2^k}$. If A wins the IND-sMIBAS-CCA2 game, the advantage of B is: $\varepsilon' = |Pr[B(aP, bP, cP, Z) = 1] - Pr[B(aP, bP, cP, e(P,P)^{abc}) = 1]| \geq |\varepsilon + \frac{1}{2} - \frac{nq_d}{2^k} - \frac{1}{2}| = \varepsilon - \frac{nq_d}{2^k}$, and $t' \leq t + 4q_d O(t_1)$ (t_1 is the time consumed by a bilinear pare computation).

□

Theorem 5 (About the unforgeability)**.** Assume that there is an EUF-MIBAS-CMA adversary F which can win the game defined in Definition 4 with an advantage ε within running time t (here, assume that adversary F can ask q_e queries to Extract, q_s queries to Anony-signcryption, q_d queries to De-signcryption, and q_{H_i} queries to H_i ($i = 1,2,3,4$) at most). Then, there is an algorithm B that can solve the CDH problem with an advantage $\varepsilon' \geq \varepsilon - \frac{q_s}{2^k}$ within running time $t' \leq t$, where t_1 is the time consumed by a bilinear pair computation.

Proof. Here, we shall show how B uses F to solve the CDH problem with the probability ε' within running time t'.

First, let B receive a random instance $\langle P, aP, bP\rangle$ of the CDH problem, and B's goal be to figure out abP. To solve this problem, B acts as the Challenger described in Definition 4 to do the following steps.

Setup: B sets $P_{pub} = bP$ and sends the system parameters $params = \langle G_1, G_2, q, e, P, P_{pub}, P_0, g, H_1, H_2, H_3, H_4\rangle$ to F. Upon receiving the parameters, F outputs the target identity ID_S^*. Here, the H_1, H_2, H_3 and H_4 queries should be carried out like in Theorem 4.

Attack: F probes B with the following queries.

Extract query: F produces and identity $ID(ID \neq ID_S^*)$ and gives it to B. B checks H_1-list; if the tuple (ID, l, Q) exists, computes $d = blP$ and returns it to F.

Anony-signcrypt query: Upon receiving an anony-signcrypt query about (m, L', L', ID_S) (where $ID_S \in L = \{ID_1, ID_2, \ldots, ID_m\}$ and $L' = \{ID'_1, ID'_2, \ldots, ID'_n\}$), B randomly chooses $x_i \in Z_p^*, i \in \{1, 2, \ldots, m\}$, and computes $R_i = x_i P, i \in \{1, 2, \ldots, m\} \backslash \{S\}$, $\alpha = \sum_{i=1}^{m} x_i, \omega = g^{\alpha}$, and $R_S = x_S Q_S - \sum_{i=1, i \neq S}^{m} (R_i + h_i Q_i)$. Then, it computes $U = \alpha P$ and $W = H_2(\omega) \oplus M$. In succession, B checks H_3-list, if (W, R_S) exists, gets h_S; otherwise, randomly chooses $h_S \in Z_q^*$ and stores (W, R_S, h_S) in H_3-list. Then, it computes $V = (x_S + h_S) d_S = (x_S + h_S) l_S bP$. B searches H_4-list to find the corresponding result x_j of ID'_i, and computes $y_j = \alpha(P_0 + Q'_j), j = 1, 2, \ldots, n$. Then, B can obain $T_j, j \in \{1, 2, \ldots, n\}$. At last, B obtains the ciphertext C and returns it to F.

Forgery: F generates a target ciphertext $C^* = \langle U^*, V^*, W^*, T^*, R^*, L^* \rangle$. If the forged ciphertext is valid, we have $e(Z^*, P) = e(P_{pub}, \sum_{i=1}^{m} (R_i^* + h_i^* Q_i^*))$. Let $Q_S^* = l_S^* P = aP$, and then $V^* = (x_S^* + h_S^*) d_S^* = (x_S^* + h_S^*) l_S^* bP = (x_S^* + h_S^*) abP$. Now, it is easy for us to get the solution of the CDH problem $abP = V^*(x_S^* + h_S^*)^{-1}$.

Now, we shall determine the success advantage of B. In Anony-signcryption queries, the probability that B fails is not more than $\frac{q_S}{2^k}$, so we have $\varepsilon' \geq \varepsilon - \frac{q_S}{2^k}$, and $t' \leq t$. □

5.3 Performance Analyses

In this section, we shall analyze our scheme by comparing it with the existing multi-receiver signcryption schemes in performance and efficiency.

5.3.1 Performance Comparisons

Table 1 shows the performance comparisons of our scheme with the existing schemes [1, 2, 3, 4, 5, 6, 15].

We shall explain Table 1 as follows:

1. The receivers' anonymity. Receivers' anonymity means that each receiver is anonymous for attackers and other receivers. On one hand, an attacker can not get the ID information of any authorized receiver; on the other hand, every authorized receiver can not get the ID information of the other authorized ones. As the message is broadcasted by the sender, anyone can easily receive it. In the existing schemes [1, 2, 3, 4, 5, 6, 15], the ciphertext requires a receiver list, which denotes the information how the ciphertext is organized (in schemes [1, 15], the list has been omitted by the authors). Only in this way can a receiver find the information s/he requires to decrypt the ciphertext. The receiver list is just the ID information of the authorized receivers and their ID sequences, thus exposing the ID of receivers directly, so the anonymity is not available. However, during the signcryption process of our scheme, as the ID information of all the authorized receivers is mixed by the Lagrange interpolation functions

Schemes	Encryption Algorithm	Design Method	Merits	Demerits
Scheme [1]	ID-based Signcryption	Using Bilinear Pairing Technology	Proposing Multi-Receiver Signcryption Scheme	Losing Receivers' Identity Label; Sender's Identity Exposed; Decryption Unfairness;
Scheme [2]	ID-based Signcryption	Using Bilinear Pairing Technology	Proposing Sender Anonymity	Receivers' Identity Exposed; Decryption Unfairness;
Scheme [3]	ID-based Signcryption	Using Bilinear Pairing Technology	Correct scheme [1] and adding Receivers' Identity Label	Sender's and Receivers' Identity Exposed; Decryption Unfairness;
Scheme [4]	ID-based Signcryption	Using Interpolating Polynomial	Short Ciphertext	Sender's and Receivers' Identity Exposed; Decryption Unfairness;
Scheme [5]	ID-based Signcryption	Using Bilinear Pairing Technology	Short Parameters	Sender's and Receivers' Identity Exposed; Decryption Unfairness;
Scheme [6]	ID-based Signcryption	Using Bilinear Pairing Technology and Interpolating Polynomial	Proposing Threshold Signcryption Scheme	Sender's and Receivers' Identity Exposed; Decryption Unfairness;
Scheme [15]	ID-based Signcryption	Using Bilinear Pairing Technology	Secure in the Standard Model	Losing Receivers' Identity Label; Receivers' Identity Exposed; Decryption Unfairness;
Ours	ID-based Signcryption	Using Bilinear Pairing Technology and Lagrange Interpolating Polynomial	Sender and Receivers Anonymity; Decryption Fairness; Judgment in Advance	None

Table 1. Performance comparisons between the existing schemes and the proposed scheme

and hidden in the pseudo-identity list denoted by $(T_1, T_2, \ldots, T_n)$, any receiver or attacker can not get any information on other authorized receivers. That means our scheme possesses the receiver anonymity.

2. The decryption fairness. Decryption fairness means that for all authorized receivers, the probabilities of correctly decrypting the ciphertext are the same. Once a part of bits in the message is missing or destroyed during the transmission, no receiver can correctly decrypt it; but, in the existing multi-receiver signcryption schemes [1, 2, 3, 4, 5, 6, 15], as long as every receiver receives the partial ciphertext message corresponding to its own ID, it can decrypt the message unmistakably. Whether other receivers' information goes wrong or is destroyed or not does not affect its correct decryption. In this case, when some receivers' ciphertext information goes wrong while others' is kept right during the transmission, only these receivers can not decrypt normally, thus bringing about decryption unfairness. Decryption unfairness can lead to spoofing attack to some receiver by the sender easily. On the contrary, in the decryption process of our scheme, every element in the ciphertext $C = \langle U, V, W, T, R, L\rangle$ is essential for all receivers, so when any element goes wrong, no receiver can decrypt correctly. That is to say, the decryption process is fair for all the authorized receivers in our scheme.

3. The sender's anonymity. Sender's anonymity means the receiver can verify whether the sender is a member of one trusted group and thus ensure the reliability of the message source, but s/he could not know the real sender of the messages. Schemes [2, 3, 4, 5, 6] have not taken the sender's anonymity into account, and each receiver can know who the sender of the received messages is. That is to say, these schemes are not anonymous ones. Based on the ring signature technology, schemes [2, 15] and our scheme hide the real sender into a group of identities $L = \{ID_1, ID_2, \ldots, ID_m\}$, each of which is trusted by the receivers. Therefore, the receivers can verify the validity of the message source, but they cannot prove who the real sender is.

4. Our scheme also provides a method to judge whether a receiver is an authorized one before his/her decryption. The ciphertext of the existing schemes [1, 2, 3, 4, 5, 6, 15] includes the list of the receivers, so each receiver can easily know whether s/he is an authorized one; but in our scheme, in order to achieve the receivers' anonymity, the ID information of the receiver is not included in the ciphertext, so we must provide a method to let each receiver to judge whether s/he is authorized to avoid unnecessary decryption operations. The formula $V \cdot Q'_j = K \cdot d'_j$ in our scheme is used to deal with this problem. If the equation holds for a receiver, s/he is authorized and can continue the following decryption; otherwise, s/he should stop the algorithm.

5.3.2 Signcryption Efficiency Comparisons

Here, we should make a comparison of our scheme and the existing multi-receiver signcryption schemes in signcryption efficiency, including calculation cost and communication traffic (ciphertext length). Table 2 shows the results.

Schemes	**Pairings**	**Exp.**	**Add.**	**Mult.**	**Hash**	**Ciphertext size**	**Public Parameters**
Scheme [1]	1	$n+4$	0	6	3	$(n+3)\vert G_1\vert +$ $\vert ID\vert + \vert M\vert$	10
Scheme [2]	0	1	$3m+n-2$	$2m+n+1$	$m+1$	$(m+n+2)\vert G_1\vert +$ $M + (m+n)\vert ID\vert$	11
Scheme [3]	1	1	$n+1$	$n+5$	2	$(n+2)\vert G_1\vert +$ $\vert G_2\vert + \vert M\vert + n\vert ID\vert$	10
Scheme [4]	0	1	$n+1$	$n+3$	2	$3\vert G_1\vert + \vert M\vert + n\vert ID\vert$	n+9
Scheme [5]	2	2	$n+1$	$n+4$	2	$(n+2)\vert G_1\vert +$ $\vert M\vert + n\vert ID\vert + \vert Z_q\vert$	8
Scheme [6]	1	1	$2n-1$	$4n+4$	2	$(n+3)\vert G_1\vert +$ $\vert M\vert + (n+1)\vert ID\vert$	9
Scheme [15]	1	$2m+n+3$	0	$m+n+1$	2	$(m+n+2)\vert G_1\vert +$ $\vert M\vert + m\vert ID\vert$	13
Ours	0	1	$3m-2$	$2m+1$	$m+1$	$(m+n+2)\vert G_1\vert +$ $\vert M\vert + m\vert ID\vert$	12

Table 2. Signcryption efficiency comparisons between the existing schemes and the proposed scheme

The following is the explanation of Table 2:

1. The ciphertext size. In our scheme, the ciphertext is denoted by $C = \langle U, V, W, T, R, L\rangle$, and thus its length is $(m+n+2)|G_1| + |M| + m|ID|$. In scheme [15], the true length of the ciphertext is $(m+n+2)|G_1| + |M| + (m+n)|ID|$ after we add the receiver list to the ciphertext (as discussed above, the receiver list should be a part of the ciphertext, but has been omitted by the authors). The ciphertext length of scheme [2] is also larger than ours. Although the ciphertext of schemes [1, 3, 4, 5, 6] is smaller, they are not anonymous ones, that is to say, they cannot meet the sender's anonymity and the receivers' anonymity. Compared with the existing anonymous schemes, our scheme has shorter ciphertext, which determines the low communication traffic in practical applications.

2. Then, we talk about the calculation cost. In our scheme, the goal of computing $f_i(x)$ and T_i is to hide the identities of the receivers to achieve the anonymity of the receiver. However, if the receivers are selected, $f_i(x)$ and T_i can be computed in advance, so we do not consider their effect on the computation cost. Therefore, in order to signcrypt a message M, our scheme needs $(3m-2)$ addition operations, $(2m + 1)$ scalar multiplications in G_1 and 1 exponentiation in G_2. Because the most time-consuming operations are the bilinear pair computation and the exponentiation, our scheme has evident advantages over the existing ones in signcryption computation efficiency.

6 CONCLUSIONS

Most of the existing multi-receiver signcryption schemes cannot guarantee the anonymity of the participants. Some given multi-receiver anonymous signcryption schemes only take the anonymity of the sender into account, but no attention is paid to the anonymity of the receivers. Especially, in the existing multi-receiver signcryption schemes, it is required to include the list of receivers into the ciphertext to determine the authorized receivers, which discloses the identities of receivers directly and leads to the decryption unfairness issue. Aiming at the receiver anonymity problem and the decryption unfairness problem, in this paper we propose a new multi-receiver anonymous signcryption scheme named nMIBAS. In nMIBAS, the receivers' identity ceases to be a part of the ciphertext, so the identity of each authorized receiver is hidden and the anonymity of the receivers is guaranteed. The entire ciphertext of nMIBAS is necessary for each receiver in decryption, and this ensures fairness of decryption. At the same time, our scheme provides an effective method for receivers to judge if they are authorized before encryption. Compared with the existing schemes, our scheme has shorter ciphertext and less computation overheads, which makes our scheme more practical than the existing ones. The possible future work is to apply our scheme in practical network communications to solve the security issue of multicasting or broadcasting.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant Nos. 61103178 and 60803151; the Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20096102120045; Basic Science Research Fund in Xidian University under Grant No. K5051310006.

REFERENCES

[1] Duan, S. et al.: Efficient and Provably Secure Multi Receiver Identity based Signcryption. Information Security and Privacy, 2006, pp. 195–206.

[2] Lal, S. et al.: Anonymous ID Based Signcryption Scheme for Multiple Receivers. Cryptology ePrint Archive, Report 2009/345, 2009.

[3] Yu, Y. et al.: Efficient Identity-Based Signcryption Scheme for Multiple Receivers. Autonomic and Trusted Computing, 2007, pp. 13–21.

[4] Sharmila, S. et al.: An Efficient Identity-Based Signcryption Scheme for Multiple Receivers. Advances in Information and Computer Security, 2009, pp. 71–88.

[5] Elkamochi, H. et al.: MIDSCYK: An Efficient Provably Secure Multirecipient Identity-Based Signcryption Scheme. Networking and Media Convergence, 2009, pp. 70–75.

[6] Qin, H. et al.: Identity-Based Multi-receiver Threshold Signcryption Scheme. Security and Communication Networks, Vol. 4, 2011, No. 11, pp. 1331–1337.

[7] Zheng, Y.: Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature)+Cost (Encryption). Advances in Cryptology, 1997, pp. 165–179.

[8] Malone, J.: Identity-Based Signcryption. Cryptology ePrint Archive. Report 2002/098, 2002.

[9] Miao, S. et al.: Cryptanalysis of a Certificateless Multi-Receiver Signcryption Scheme. International Conference on Multimedia Information Networking and Security 2010, pp. 593–597.

[10] Pang, L. J. et al.: Design and Analysis of a Provable Secure Multi-Recipient Public Key Encryption Scheme. Journal of Software, Vol. 20, 2009, No. 10, pp. 2739–2745 (in Chinese with English abstract).

[11] Rivest, R. et al.: How to Leak a Secret. Advances in Cryptology, 2001, pp. 552–565.

[12] Huang, X. et al.: Identity Based Ring Signcryption Scheme: Cryptographic Primitive for Preserving Privacy and Authenticity in the Ubiquitous World. International Conference on Advanced Information Networking and Applications 2005, pp. 649–654.

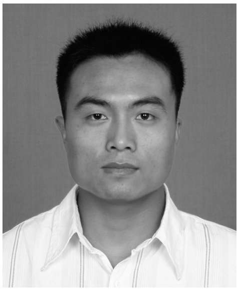
[13] Zhang, J. et al.: A Novel ID-Based Anonymous Signcryption Scheme. Advances in Data and Web Management 2009, pp. 604–610.

[14] Zhang, M. et al.: Analysis and Enhance of Anonymous Signcryption Model. Cryptology ePrint Archive: Report 2009/194, 2009.

[15] Zhang, B. et al.: An ID-Based Anonymous Signcryption Scheme for Multiple Receivers Secure in the Standard Model. Advances in Computer Science and Information Technology 2010, pp. 15–27.

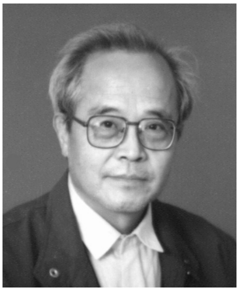
[16] Pang, L. J. et al.: Improved Multicast Key Management of Chinese Wireless Local Area Network Security Standard. IET Communications, Vol. 6, 2012, No. 9, pp. 1126–1130.

[17] Pang, L. J. et al.: A New ID-Based Multi-Recipient Public-key Encryption Scheme. Chinese Journal of Electronics, Vol. 22, 2013, No. 1, pp. 89–92.



Liaojun Pang received his Bachelor and Master degrees in computer science and technology from Xidian University of China, in 2000 and 2003, respectively. In 2006, he received his Ph. D. degree in cryptography from Xidian University of China. Currently he is an Associate Professor in School of Life Sciences and Technology of Xidian University; he is also a visiting scholar at the Department of Computer Science of Wayne State University of USA. His research interests include Internet security, cryptography, secure mobile agent systems and e-commerce security technology. He became a member of IEEE in 2009.

Huixian Li received his Ph. D. degree in cryptography from Dalian University of Technology. Now, she is an Associate professor in the School of Computer Science and Engineering of the Northwestern Polytechnical University, and also a visiting scholar at the Department of Computer Science, Wayne State University of USA. Her research interests include information security, cryptography, and security technologies for mobile health care systems.



Yumin Wang is a Professor at the State Key Lab. of Integrated Service Networks, Xidian University of China. His research interests include cryptography, coding, and information theory. He is a Senior Member of IEEE.