Completely Anonymous Multi-Recipient Signcryption Scheme with Public Verification

Liaojun Pang^{1,2*}, Huixian Li^{2,3}, Lu Gao¹, Yumin Wang¹

1 School of Life Sciences and Technology, Xidian University, Xi'an, China, **2** Department of Computer Science, Wayne State University, Detroit, Michigan, United States of America, **3** School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an, China

Abstract

Most of the existing multi-recipient signcryption schemes do not take the anonymity of recipients into consideration because the list of the identities of all recipients must be included in the ciphertext as a necessary element for decryption. Although the signer's anonymity has been taken into account in several alternative schemes, these schemes often suffer from the *cross-comparison attack* and *joint conspiracy attack*. That is to say, there are few schemes that can achieve complete anonymity for both the signer and the recipient. However, in many practical applications, such as network conference, both the signer's and the recipient's anonymity should be considered carefully. Motivated by these concerns, we propose a novel multi-recipient signcryption scheme with complete anonymity. The new scheme can achieve both the signer's and the recipient's anonymity at the same time. Each recipient can easily judge whether the received ciphertext is from an authorized source, but cannot determine the real identity of the sender, and at the same time, each participant can easily check decryption permission, but cannot determine the identity of any other recipient. The scheme also provides a public verification method which enables anyone to publicly verify the validity of the ciphertext. Analyses show that the proposed scheme is more efficient in terms of computation complexity and ciphertext length and possesses more advantages than existing schemes, which makes it suitable for practical applications. The proposed scheme could be used for network conferences, paid-TV or DVD broadcasting applications to solve the secure communication problem without violating the privacy of each participant. **Key words:** Multi-recipient signcryption; Signcryption; Complete Anonymity; Public verification.

Citation: Pang L, Li H, Gao L, Wang Y (2013) Completely Anonymous Multi-Recipient Signcryption Scheme with Public Verification. PLoS ONE 8(5): e63562. doi:10.1371/journal.pone.0063562

Editor: Francesco Pappalardo, University of Catania, Italy

Received: October 18, 2012; **Accepted:** April 3, 2013; **Published:** May 10, 2013

Copyright: © 2013 Pang et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Funding: National Natural Science Foundation of China under grant numbers 61103178, 61103199 and 60803151; the Research Fund for the Doctoral Program of Higher Education of China under grant number 20096102120045; Basic Science Research Fund in Xidian University under grant number K5051310006. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing Interests: The authors have declared that no competing interests exist.

* E-mail: liaojun.pang@wayne.edu

Introduction

With development of network technology and its applications, a lot of group-oriented network services such as network multicasting or broadcasting have been proposed. Usually, in these services, a message sender is required to securely send the same messages to a group of recipients, such that only a certain number of recipients can read the messages while unauthorized recipients can extract nothing useful from these messages [1]. Therefore, the concept of multi-recipient encryption was put forward [2–6], and it has been considered as one of most promising solutions to solve the security problem of securing multicasting or broadcasting. Later, combining the concept of multi-recipient encryption with the idea of Zheng's signcryption [7], Duan *et al.* [8] proposed the first multi-recipient signcryption scheme. In their scheme, to achieve the goal of sending the same message to all authorized recipients confidentially, the sender only needs to execute one signcryption operation, and at the same time, each recipient can verify the validity of messages. Since then, many excellent multi-recipient signcryption schemes [9–11] were proposed, which take more security properties into consideration than Duan *et al.*'s scheme. In general, multi-recipient signcryption can be used in many important applications, such as paid-TV or DVD broad-

casting systems [10], where only authorized or paying users should be able to access such services.

Nevertheless, today, more and more people are concerned regarding personal privacy, thus participant anonymity should be taken into account when designing multi-recipient signcryption [12]. For example, in paid-TV and DVD broadcasting application systems, service providers do not want others to obtain the real identities from the ciphertext messages. Therefore, multi-recipient signcryption with the sender (or called the signer) anonymity had been introduced. In literature, there have been several multi-recipient signcryption schemes [13–17] which try to assure anonymity of the sender. The concept of anonymous signature was firstly proposed by Rivest *et al.* [18]. In 2005, Huang *et al.* [19] proposed the first anonymous signcryption scheme, which used an ID-based ring signature to assure anonymity of the signer. However, their scheme is only a single-recipient scheme. Later, based on similar thoughts, Lal *et al.* [13] extended this method for multi-recipient environments. Furthermore, a multi-recipient scheme with anonymity of the sender [14–17] was proposed. Although these schemes [13–17] provide solutions for assuring signer anonymity, there are still some unsolved issues. For example, they suffer from two new attacks known as the *cross-comparison attack* [20] and the *joint conspiracy attack* [21]. Based on the

ring signature, schemes [13–17] construct a list which includes the real signer and several valid participants which are chosen randomly by the signer hiding the real signer in this list. Although this perfectly works to some extent, an attacker can obtain a number of different ciphertexts from the same message source by closely monitoring network traffic, thus by comparing the signers' identities from different lists an attacker can narrow down the scope of the target signer. Using this scheme, an attacker can directly obtain the identity of the real signer. Even if the attacker does not directly obtain the real signer's identity, he/she has narrowed down the scope of the attacker's guess. In addition, it is still possible for such an attacker to retrieve a list which includes the real signer. Then, he/she can cooperate with some participants in the list to narrow down the scope and guess the real signer with a larger probability. In addition, the list of chosen participants can increase the length of the ciphertext quite significantly, potentially reducing the transmission efficiency. More important, the identities of all the authorized recipients are usually included in the ciphertext of these anonymous schemes in plaintext [13–19], which is not always wanted.

Generally speaking, anonymity of participants includes both the sender's and the recipient's anonymity. Besides the anonymity of the sender, the anonymity of the recipient is often equally important so that designers of multi-recipient signcryption schemes should pay attention. For example, in paid-TV and DVD broadcasting application systems, no user should accept that his/her subscription of these services is publicly viewable to others especially when the service is quite sensitive. However, unfortunately, almost none of the existing schemes take the anonymity of recipients into consideration because the identity of each recipient must be included in the ciphertext as a necessary element for decryption. The list of the authorized recipients' identities in the ciphertext is used to show who are the authorized recipients and how each authorized recipient gets his/her person-specific data for encryption from the ciphertext during the decryption process. Thus, schemes [9–11] directly expose the recipient's identity and therefore violate their privacy. Also, the fact that different recipients have different person-specific data for decryption can lead to decryption unfairness. This means that if some recipient's person-specific data are damaged due to communication errors, he/she cannot decrypt the ciphertext but the others can still decrypt the ciphertext correctly [12]. Therefore, it is urgent and challenging for researchers to solve the recipient anonymity issue of multi-recipient signcryption.

Following the arguments above, it is known that almost none of the existing multi-recipient signcryption schemes take the full anonymity of recipients and senders into account. Although there are several schemes that provide a solution for anonymity of the signer, they are not perfect, that is, they suffer from the *cross-comparison attack* and the *joint conspiracy attack*. Therefore, existing schemes cannot deal with the anonymity of the sender or the recipient properly. Furthermore, these schemes are not suitable for applications that need complete anonymity for the sender and the recipient. For example, in a network conference application, every conference participant often wants to be kept anonymous when he/she is taking part in the conference discussion. Furthermore, if a participant (i.e. sender) wants to publish criticism or objections, he/she hopes that others (i.e. recipients) do not know his/her identity. At the same time, the recipient cannot want the other recipients to reveal that he/she is an authorized recipient. In fact, today, anonymity is one of the most important prerequisites for people to talk freely and make objective decisions.

Motivated by the above, this paper proposes a completely anonymous multi-recipient signcryption scheme which meets: (1)

The identity of the sender is kept secret; (2) The identities of all the recipients are kept secret; (3) Each recipient can easily judge whether the received message is from an authorized source, but he/she cannot determine the real identity of the sender; (4) Each recipient can easily judge whether he/she is an authorized recipient, but he/she cannot determine the identity of any other authorized recipient; (5) The validity of ciphertext can be verified publicly. Speaking of practical applications, the proposed scheme can be in principle used for network conference, paid-TV or DVD broadcasting application systems to assure secure communication among authorized participants, while at the same time, providing complete anonymity for all participants.

To facilitate the description of our scheme, notations used throughout the document are summarized in Table 1.

Preliminaries

Complexity Assumptions

The security of the proposed scheme is based on the following problems and security assumptions.

Let G_1 and G_2 be two cyclic groups of prime order q and let P be a generator of G_1 . Let $e: G_1 \times G_1 \rightarrow G_2$ be a bilinear mapping. The DBDH, CDH and DBDH-M problems can thus be defined as:

- (1) **Decisional Bilinear Diffie-Hellman (DBDH) Problem:** Given (P, aP, bP, cP, Ψ) , for $\Psi \in G_2$ and unknown $a, b, c \in \mathbb{Z}_q^*$, determine whether $\Psi = e(P, P)^{abc}$ holds.

Definition 1: The advantage of any probabilistic polynomial time (PPT) algorithm B in solving the DBDH Problem is defined as: $\text{Adv}_B^{\text{DBDH}} = |\Pr[B(P, aP, bP, cP, e(P, P)^{abc}) = 1] - \Pr[B(P, aP, bP, \Psi) = 1]|$.

DBDH assumption: For any PPT algorithm B , $\text{Adv}_B^{\text{DBDH}}$ is negligible.

- (2) **Computational Diffie-Hellman (CDH) Problem:** Given $(P, aP, bP) \in G_1$, for some $a, b \in \mathbb{Z}_q^*$, compute abP .

Table 1. Notations.

Name	meaning
q	Large prime integer
G_1	Additive group of order q
G_2	Multiplicative group of order q
$\mathbb{Z}_q^*$	The set of positive integers which are less than q
P	Generator of G_1
e	Bilinear mapping, i.e. $e: G_1 \times G_1 \rightarrow G_2$
H_i	Cryptographic hash function, $i = 1, 2, 3, 4$
ID_i	The identity of the participant i
Q_i	Public key of ID_i
D_i	Private key of ID_i
PKG	Private key generator
s	The master key of PKG
P_{pub}	The system master public key
CDH	Computational Diffie-Hellman Problem
DBDH	Decisional Bilinear Diffie-Hellman Problem
DBDH-M	Modified Decisional Bilinear Diffie-Hellman Problem
PPT	Probabilistic polynomial time
Pr	The probability of an event
Adv	The advantage of one algorithm in solving a problem

doi:10.1371/journal.pone.0063562.t001

Definition 2: The advantage of any PPT algorithm B in solving the CDH Problem is defined as: $\text{Adv}_B^{\text{CDH}} = \Pr[B(P, aP, bP) = abP, a, b \in \mathbb{Z}_q^*]$.

CDH assumption: For any PPT algorithm B , $\text{Adv}_B^{\text{CDH}}$ is negligible.

- (3) **Modified Decisional Bilinear Diffie-Hellman (DBDH-M) Problem:** Given (P, aP, bP, Γ) , for $\Gamma \in G_1$ and unknown $a, b \in \mathbb{Z}_q^*$, determine whether $\Gamma = a^2bP$ holds.

Definition 3: The advantage of any PPT algorithm B in solving the DBDH-M Problem is defined as: $\text{Adv}_B^{\text{DBDH-M}} = |\Pr[B(P, aP, bP, a^2bP) = 1] - \Pr[B(P, aP, bP, \Gamma) = 1]|$.

DBDH-M assumption: For any PPT algorithm B , $\text{Adv}_B^{\text{DBDH-M}}$ is negligible.

Algorithm Model

Our identity(ID)-based multi-recipient signcryption scheme with complete anonymity consists of four algorithms, namely: Setup, Extract, Anony-signcrypt and De-signcrypt, shown as follows:

Setup. Private Key Generator (PKG) runs this algorithm to generate a master key s and public parameters params . Note that the public parameters are publicly known while the master key must be kept secret.

Extract. This algorithm is run by PKG to extract the private key of the user. With a user's identity ID , PKG's master key s and the public parameter params as input, it outputs the private key D associated with ID , namely $D = \text{Extract}(ID, s, \text{params})$. The private key D must be kept secret.

Anony-signcrypt. This algorithm is run by the signer ID_S . With PKG's public parameter params , a plaintext message M , a list of recipients' identity $L = \{ID_1, ID_2, \dots, ID_n\}$ as input, the signer ID_S runs this algorithm to generate a ciphertext C associated with M , namely $C = \text{Anony-signcrypt}(\text{params}, M, L, D_S)$, which satisfies $L \notin C$ and $ID_S \notin C$.

De-signcrypt. With the ciphertext C , PKG's public parameter params , the recipient's identity $ID_i (i \in \{1, 2, \dots, n\})$ and its private key D_i as input, the recipient can run this algorithm to decrypt the ciphertext. The recipient can first judge whether he/she is an authorized recipient. If not, he/she outputs an error message $\perp$ and exits the algorithm. Otherwise, he/she continues to carry out the decryption process and outputs the plaintext M associated with C , namely $M = \text{De-signcrypt}(C, \text{params}, D_i)$.

Message Confidentiality

The security model of ciphertext indistinguishability under chosen ciphertext attack was first proposed by Canetti *et al.* [20]. Later, Duan *et al.* [8] extended this security model for the multi-recipient environments, called as indistinguishability of ciphertexts under selective multi-ID, chosen ciphertext attack (IND-sMIBSC-CCA) shown as Definition 4.

Definition 4. IND-sMIBSC-CCA: Let A be a polynomial-time attacker and Π be an ID-based multi-recipient scheme. Consider that A interacts with a Challenger B in the following game:

Setup. Challenger B runs this algorithm to generate master key s and public parameters params , sends params to A , and keeps the master key s secret. Upon receiving public parameters, A outputs n target identities $L^* = \{ID_1^*, ID_2^*, \dots, ID_n^*\}$.

Phase 1. A performs a number of queries to B :

Extraction query: Upon receiving private key extraction query about an identity ID , $ID \neq ID_i^*, i = 1, 2, \dots, n$, B runs the Extract algorithm to get $D = \text{Extract}(ID, s, \text{params})$.

Anony-signcryption query: A chooses a target plaintext M , a list of recipients' identity information $L = \{ID_1, ID_2, \dots, ID_n\}$ and gives

them to B . B randomly chooses an identity ID_S , computes the private key D_S , and generates the ciphertext $C = \text{Anony-signcrypt}(\text{params}, M, L, D_S)$ and returns it to A .

De-signcryption query: A generates the list of target identities $L^* = \{ID_1^*, ID_2^*, \dots, ID_n^*\}$ and a ciphertext C . B randomly chooses an identity $ID_j \in L$ and computes its private key D_j . If C is a valid ciphertext, B decrypts it to obtain the corresponding plaintext $M = \text{De-signcrypt}(C, \text{params}, D_j)$ and returns it to A ; otherwise, B outputs an error message $\perp$.

Challenge. A outputs a target plaintext pair (M_0, M_1) and an arbitrary identity ID_S with its private key D_S . Upon receiving (M_0, M_1) and D_S , B picks up a random bit $\beta \in \{0, 1\}$ and creates a target ciphertext $C^* = \text{Anony-signcrypt}(\text{params}, M_\beta, L^*, D_S)$, and then returns C^* to A .

Phase 2. A performs a number of queries like Phase 1. Note that A cannot query the identity information in L^* in the Extraction query, and cannot query C^* in the De-signcryption query.

Guess. Finally, A outputs its guess $\beta' \in \{0, 1\}$. If $\beta' = \beta$, he wins this game.

An attacker A mentioned above is referred to as an IND-sMIBSC-CCA attacker. We define A 's guessing advantage as follows:

$$\text{Adv}_\Pi^{\text{IND-sMIBSC-CCA}}(A) = |\Pr[\beta = \beta'] - 1/2| \quad (1)$$

The scheme Π is said to be (t, ϵ) -IND-sMIBSC-CCA secure, if for any IND-sMIBSC-CCA attacker A , its guessing advantage is less than ϵ within polynomial running time t .

Unforgeability

This security model has been proposed by Duan *et al.* [8] and is called strong existential unforgeability under selective multi-ID, chosen message attack (SUF-MIBSC-CMA) shown as Definition 5.

Definition 5. SUF-MIBSC-CMA: Suppose F is a forger, and let Π be an ID-based multi-recipient scheme. Consider that F interacts with a Challenger B in the following game:

Setup. B runs this algorithm to generate a master key s and a public parameter params . B gives the params to F and keeps s secretly. Upon receiving this parameter, F outputs n target identities $L^* = \{ID_1^*, ID_2^*, \dots, ID_n^*\}$.

Attack. F performs a number of queries to B as described in Definition 4.

Forgery. F finally outputs a new ciphertext message C^* , a list of recipient identities $L = \{ID_1, ID_2, \dots, ID_n\}$. If C^* is the ciphertext of the message M generated by $ID_i^* (i \in \{1, 2, \dots, n\})$ and can be decrypted by any of recipients in L , C^* is a valid ciphertext and F wins this game. The restriction here is that F cannot ask for private key extraction on ID_i^* , and C^* cannot be produced by the Anony-signcrypt algorithm.

The scheme Π is said to be (t, ϵ) -SUF-sMIBSC-CMA secure, if for any SUF-sMIBSC-CMA attacker F , its guessing advantage is less than ϵ within polynomial running time t .

Recipient Anonymity

This security model has been proposed by Fan *et al.* [5] and is called anonymous indistinguishability of encryptions under selective ID, chosen ciphertext attack (ANON-sID-CCA) and shown as Definition 6.

Definition 6. ANON-sID-CCA: Let A be a polynomial-time attacker. Let Π be an ID-based multi-recipient scheme. Consider that A interacts with a Challenger B in the following game:

Setup. Challenger B runs the Setup algorithm to generate the master key s and public parameters $params$. Then, B sends $params$ to A and keeps s secret.

Phase 1. A outputs a target identity pair (ID_1^*, ID_2^*) . Upon receiving (ID_1^*, ID_2^*) , the Challenger B randomly chooses $\beta \in \{1, 2\}$.

Phase 2. A issues private key extraction queries. Upon receiving a private key extraction query, denoted by ID_j , Challenger B runs the private key extraction algorithm to get $D_j = \text{Extract}(ID_j, s, params)$. The constraint here is that $ID_j \neq ID_i^*, i = 1, 2$.

Phase 3. A issues de-signcryption queries for the target identities. Upon receiving a de-signcryption query about (C^*, ID_i^*) , $i = 1, 2$, Challenger B returns $M^* = \text{De-signcrypt}(C^*, params, D_i^*)$ to A , where D_i^* is the private key of ID_i^* .

Challenge. A outputs a target plaintext M to B . Then, Challenger B creates a related ciphertext $C = \text{Anony-signcrypt}(params, M, ID_\beta)$ and returns it to A .

Phase 4. A issues private key extraction queries as those in Phase 2 and de-signcryption queries for target identities as those in Phase 3. The restriction here is that $C \neq C^*$.

Guess. Finally, A outputs its guess $\beta' \in \{1, 2\}$. If $\beta = \beta'$, A wins the game.

An attacker A mentioned above is referred to as an ANON-sID-CCA attacker. We define A 's guessing advantage as follows:

$$\text{Adv}_{\Pi}^{\text{ANON-sID-CCA}}(A) = |\Pr[\beta = \beta'] - 1/2| \quad (2)$$

The scheme Π is said to be (t, ϵ) -ANON-sID-CCA secure, if for any ANON-sID-CCA attacker A , its guessing advantage is less than ϵ within polynomial running time t .

Methods

The proposed scheme is composed of the following four algorithms. And at the same time, we shall take the network conference application as an example to show how to use our scheme.

Setup Algorithm

PKG performs the following process:

- (1) Let G_1 be an additive group and G_2 be a multiplicative group with the same prime order q , ($q \geq 2^k$, k is a long integer). Let P be a generator of G_1 . Choose a bilinear mapping $e: G_1 \times G_1 \rightarrow G_2$.
- (2) Define four one-way hash functions: $H_1: \{0, 1\}^* \rightarrow G_1$; $H_2: G_2 \rightarrow \{0, 1\}^{|M|}$; $H_3: \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$; $H_4: \{0, 1\}^{|M|} \times G_1 \times \dots \times G_1 \rightarrow \mathbb{Z}_q^*$, where $|M|$ is the length of the plaintext message.
- (3) Choose a random number $s \in \mathbb{Z}_q^*$ as the master key, and set $P_{pub} = sP \in G_1$ as the system's public key. Publish the system parameter $params = \langle G_1, G_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4 \rangle$ and keep the master key s secret.

Practically speaking, PKG is acted by some authority. For example, in a network conference application, the organizer of a conference should deal with the PKG, which is responsible for developing the system parameters as the steps mentioned above.

Extract Algorithm

With $params$, s , and an identity $ID \in \{0, 1\}^*$ as input, PKG performs this algorithm to generate the private key of the identity ID:

- (1) Compute ID's public key $Q_{ID} = H_1(ID)$.
- (2) Compute ID's private key $D_{ID} = sH_1(ID) = sQ_{ID}$.

Each participant, the sender or the recipient, should register himself/herself at PKG and obtain his/her private key from PKG by this algorithm. For example, in a network conference application, if someone wants to attend a conference and talk with other participants, he/she must firstly send his/her ID information to the organizer PKG to get his/her own private key computed by PKG.

Anony-signcrypt Algorithm

With $params$, a plaintext M and his/her private key D_S as input, the signer ID_S chooses a list of recipients' identity $L = \{ID_1, ID_2, \dots, ID_n\}$ and performs this algorithm to generate the ciphertext C of the plaintext M :

- (1) Randomly choose two secret integers $r, \alpha \in \mathbb{Z}_q^*$ and a secret element $P_1 \in G_1$, and then compute $Y = rQ_S$, $U = \alpha P$, $X = \alpha Y$, $\omega = e(P_{pub}, P_1)^\alpha$ and $\sigma = H_2(\omega) \oplus M$, where Q_S is the public key of ID_S .
- (2) For $i = 1, 2, \dots, n$, compute $x_i = H_3(ID_i)$ and $y_i = \alpha(P_1 + Q_i)$, where Q_i is the public key of ID_i .
- (3) For $i = 1, 2, \dots, n$, compute $f_i(x) = \prod_{1 \leq i \neq j \leq n} \frac{x - x_j}{x_i - x_j} = a_{i,1} + a_{i,2}x + \dots + a_{i,n}x^{n-1}$, where $a_{i,1}, a_{i,2}, \dots, a_{i,n} \in \mathbb{Z}_q$.
- (4) For $i = 1, 2, \dots, n$, compute $T_i = \sum_{j=1}^n a_{j,i}y_j$ and then let $T = \{T_1, T_2, \dots, T_n\}$.
- (5) Compute $h = H_4(\sigma, X, U, T)$, and then compute $W = (\alpha + h) \cdot rD_S$, where D_S is the private key of ID_S .
- (6) Generate the ciphertext: $C = \langle Y, X, U, \sigma, W, T \rangle$.

After obtaining the private key, each participant can securely and anonymously send messages to other participants that he/she selects. For example, in a network conference application, any participant can freely select some participants as expected recipients to receive his/her messages. What he/she needs to do is to encrypt the messages by this algorithm and then broadcast the ciphertext.

De-signcrypt Algorithm

The algorithm is carried out by the recipient. With $C = \langle Y, X, U, \sigma, W, T \rangle$, $params$, the recipient's identity ID_i and his/her private key D_i as input, the recipient ID_i decrypts C as follows:

Public verification. The one, who has not registered himself/herself with PKG to get his/her private key, can use the following steps to check the integrity or validity of the ciphertext. The registered participant can skip this process and directly jump to the following judgement algorithm:

- (1) Compute $h = H_4(\sigma, X, U, T)$.
- (2) Verify whether the equation $e(W, P) = e(X + hY, P_{pub})$ holds. If yes, the ciphertext is valid. Otherwise, the ciphertext is invalid or has been damaged during transmission.

Judgement. The one, who has registered himself/herself with PKG to get his/her private key, can use the following steps to check whether the ciphertext is valid and whether he/she is an authorized recipient before the following encryption process:

- (1) Compute $h = H_4(\sigma, X, U, T)$.
- (2) Check whether the equation $e(W, Q_i) = e(X + hY, D_i)$ holds. If yes, it means that ID_i is one of the recipients designated by the signer and the ciphertext is valid. Otherwise, the recipient quits the decryption process.

De-signcryption. The authorized user can recover the plaintext by the following steps:

- (1) Compute $x_i = H_4(ID_i)$ and then compute $\eta_i = T_1 + x_i T_2 + \dots + (x_i^{n-1} \bmod q) T_n$.
- (2) Compute $\omega' = e(P_{pub}, \eta_i)(U, D_i)^{-1}$ and then get the plaintext as $M' = \sigma \oplus H_2(\omega')$.

The one who receives the broadcasting ciphertext can verify the validity of the message and judge whether he/she is authorized by the public verification or judgement algorithm. If necessary, he/she can use the de-signcryption algorithm to decrypt the ciphertext. In a network conference application, due to the nature of the broadcast communication, anyone, authorized recipients or unauthorized ones, can easily receive the ciphertext and check the validity of the message and the authorization of the decryption. But, only the authorized recipients can decrypt it correctly.

Results and Discussion

Correctness Analyses

Theorem 1. The public verification algorithm in the De-signcryption algorithm is correct.

Proof.

$$\begin{aligned} e(W, P) &= e((\alpha + h) \cdot r D_S, P) \\ &= e((\alpha + h) \cdot r Q_S, sP) \\ &= e(\alpha Y + h Y, sP) \\ &= e(X + h Y, P_{pub}) \end{aligned} \quad (3)$$

In our scheme, although the identity of the real signer is not included in the ciphertext, his/her private key is definitely necessary in the signcryption process, which ensures that only legal participants who have registered himself/herself with PKG can generate a valid ciphertext. That is to say, through this algorithm, anyone can check whether a ciphertext is generated by an authorized participant, but he/she cannot determine the real identity of the signer.

Theorem 2. The judgement algorithm in the De-signcryption algorithm is correct.

Proof. For each authorized ID_i where $i \in \{1, 2, \dots, n\}$, we have

$$\begin{aligned} e(W, Q_i) &= e((\alpha + h) \cdot r D_S, Q_i) \\ &= e((\alpha + h) \cdot r Q_S, sQ_i) \\ &= e(\alpha Y + h Y, D_i) \\ &= e(X + h Y, D_i) \end{aligned} \quad (4)$$

Similarly, because the private key of the real signer is necessary in the signcryption process, this algorithm can also be used to check the validity of ciphertext. At the same time, this algorithm can help a participant, who has registered himself/herself with PKG, to judge whether himself/herself is an authorized recipient, because the private key of the recipient is also necessary in the judgement.

Theorem 3. The decryption algorithm in the De-signcryption algorithm is correct.

Proof. The authorized ID_i , $i \in \{1, 2, \dots, n\}$, can compute η_i as follows:

$$\begin{aligned} \eta_i &= T_1 + x_i T_2 + \dots + x_i^{i-1} T_i + \dots + x_i^{n-1} T_n \\ &= (a_{1,1} \alpha(P_1 + Q_1) + \dots + a_{n,1} \alpha(P_1 + Q_n)) \\ &\quad + (x_i a_{1,2} \alpha(P_1 + Q_1) + \dots + x_i a_{n,2} \alpha(P_1 + Q_n)) + \dots \\ &\quad + (x_i^{i-1} a_{1,i} \alpha(P_1 + Q_1) + \dots + x_i^{i-1} a_{n,i} \alpha(P_1 + Q_n)) + \dots \\ &\quad + (x_i^{n-1} a_{1,n} \alpha(P_1 + Q_1) + \dots + x_i^{n-1} a_{n,n} \alpha(P_1 + Q_n)) \\ &= (a_{1,1} + a_{1,2} x_i + \dots + a_{1,n} x_i^{n-1}) \alpha(P_1 + Q_1) \\ &\quad + (a_{2,1} + a_{2,2} x_i + \dots + a_{2,n} x_i^{n-1}) \alpha(P_1 + Q_2) + \dots \\ &\quad + (a_{i,1} + a_{i,2} x_i + \dots + a_{i,n} x_i^{n-1}) \alpha(P_1 + Q_i) + \dots \\ &\quad + (a_{n,1} + a_{n,2} x_i + \dots + a_{n,n} x_i^{n-1}) \alpha(P_1 + Q_n) \\ &= \alpha(P_1 + Q_i) \end{aligned} \quad (5)$$

Thus, we can get $\omega' = e(P_{pub}, \eta_i)(U, D_i)^{-1} = \omega$, because

$$\begin{aligned} \omega' &= e(P_{pub}, \eta_i) \cdot e(U, D_i)^{-1} \\ &= e(P_{pub}, \alpha(P_1 + Q_i)) \cdot e(\alpha P, sQ_i)^{-1} \\ &= e(P_{pub}, \alpha P_1) \cdot e(P_{pub}, \alpha Q_i) \cdot e(sP, \alpha Q_i)^{-1} \\ &= e(P_{pub}, P_1)^\alpha \cdot e(P_{pub}, \alpha Q_i) \cdot e(P_{pub}, \alpha Q_i)^{-1} \\ &= e(P_{pub}, P_1)^\alpha = \omega \end{aligned} \quad (6)$$

Then, we can get the plaintext through the computations $H_2(\omega') = H_2(\omega)$ and $M = H_2(\omega) \oplus \sigma$.

Security Analyses

We shall give security proof of the proposed scheme on confidentiality, unforgeability and anonymity under the random oracle model.

Theorem 4. In the IND-sMIBSC-CCA security model, if an adversary A has an advantage ϵ against the game defined in Definition 4 within running time t (where A makes at most q_e private key extraction queries, q_s anony-signcryption queries, q_d de-signcryption queries and $q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}$ queries to the Hash functions H_1, H_2, H_3 and H_4 , respectively), then there is a algorithm B in solving the DBDH problem in the time $t' \leq t$ with an advantage $\epsilon' \geq \epsilon - nq_d/2^k$.

Proof. The challenger B is challenged with an instance $(P, \alpha P, bP, cP)$ of the DBDH problem. Assume that there is an adversary A who is capable of breaking the IND-sMIBSC-CCA security with a non-negligible advantage ϵ . B makes use of A to solve the DBDH instance. B simulates the system with various oracles H_1, H_2, H_3 and H_4 and allows A to make polynomially bounded number of queries, adaptive to these oracles. The game between A and B is demonstrated below:

Setup. B sets $P_1 = cP$, $P_{pub} = bP$, and gives $\langle G_1, G_2, q, e, P, P_{G_1}, G_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4 \rangle$ to the attacker A as the public parameters. Upon receiving the system parameters, A outputs n target identities $(ID_1^*, ID_2^*, \dots, ID_n^*)$.

Phase 1. A performs a number of queries to B .

Let H_1, H_2, H_3 and H_4 be random oracles controlled by B as follows. The results of querying H_1, H_2, H_3 and H_4 are stored in H_1 -list, H_2 -list, H_3 -list and H_4 -list, respectively.

H_1 -query. Input an identity $ID_j, j \in \{1, 2, \dots, n\}$, to H_1 . If there exists (ID_j, l_j, Q_j) in H_1 -list, B returns Q_j ; otherwise, does as follows:

- (1) Choose an integer $l_j \in \mathbb{Z}_q^*$ at random;
- (2) If $ID_j \neq ID_i^*, i \in \{1, 2, \dots, n\}$, compute $Q_j = l_j P$; otherwise, compute $Q_j = l_j P - P_1$;
- (3) Put (ID_j, l_j, Q_j) into H_1 -list;
- (4) Return Q_j .

H_2 -query. $i \in \{2, 3, 4\}$: To answer these inquiries, B searches the corresponding list H_i -list ($i = 2, 3, 4$). If the corresponding answer has existed already, B returns the answer to A . Otherwise, B randomly chooses an element in proper scope as the result and returns it to A , and at the same time, B adds the inquiry and the result into the corresponding list.

Extraction query. Upon receiving private key extraction query on identity ID_j ($ID_j \neq ID_i^*, i = 1, 2, \dots, n$), B searches for (ID_j, l_j, Q_j) in H_1 -list. B recovers triple (ID_j, l_j, Q_j) in H_1 -query and computes his private key $D = l_j P_{pub} = l_j bP$, and returns it to A . If $ID_j = ID_i^*$, B aborts and outputs “failure”.

Anony-signcryption query. Upon receiving A 's anony-signcryption query (M, ID_S, L) , B checks if $ID_S \neq ID_i^* (i = 1, 2, \dots, n)$. If $ID_S \neq ID_i^* (i = 1, 2, \dots, n)$, B shall get the private key of ID_S through the Extraction query. After that, B can run the Anony-signcryption query to generate the ciphertext M . An alternative to this is:

- (1) B randomly chooses two secret integers $r, \alpha \in \mathbb{Z}_q^*$, and then computes $Y = rP, X = \alpha Y, U = \alpha P, \omega = e(P_{pub}, P_1)^\alpha$ and $\sigma = H_2(\omega) \oplus M$.
- (2) For $i = 1, 2, \dots, n$, compute $x_i = H_3(ID_i)$ and $y_i = \alpha(P_1 + Q_i)$, where Q_i is the public key of ID_i .
- (3) For $i = 1, 2, \dots, n$, compute: $f_i(x) = \prod_{1 \leq i \neq j \leq n} \frac{x - x_j}{a_{i,1} + a_{i,2}x + \dots + a_{i,n}x^{n-1}}$, where $a_{i,1}, a_{i,2}, \dots, a_{i,n} \in \mathbb{Z}_q$.
- (4) For $i = 1, 2, \dots, n$, compute $T_i = \sum_{j=1}^n a_{j,i} y_j$ and then let $T = \{T_1, T_2, \dots, T_n\}$.
- (5) B randomly chooses an integer $h' \in \mathbb{Z}_q^*$, where h' is set as the output for the random oracle query $H_4(\sigma, X, U, T)$ (This is possible because the random oracles are manipulated by B). Then, B computes $W = (\alpha + h')l_S P_{pub}$.
- (6) B gets the ciphertext $C = \langle Y, X, U, \sigma, W, T \rangle$ and returns it to A .

De-signcryption query. On receiving the De-signcryption query of the ciphertext C together with an identity ID_j , B proceeds as follows:

- (1) If $ID_j = ID_i^*$, B shall return that the ciphertext C is invalid because B does not know the private key of ID .
- (2) If $ID_j \neq ID_i^*$, B computes $h = H_4(\sigma, X, U, T)$, and verifies whether the equation $e(W, P) = e(X + hY, P_{pub})$ holds. If it does not hold, the ciphertext is not valid and then B outputs $\perp$. If it holds, B does the following steps:
 - (a) Find the secret key D corresponding to ID from the H_1 -list.
 - (b) Compute η_j according to T .
 - (c) Compute $\omega' = e(P_{pub}, \eta_j)(U, D)^{-1}$ and then get the plaintext as $M' = \sigma \oplus H_2(\omega')$.

If all the above verifications are true, then B outputs the message M' . Otherwise, the ciphertext is invalid, and B outputs $\perp$.

Challenge. A outputs a target plaintext pair (M_0, M_1) and a private key D_S . Upon receiving (M_0, M_1) and D_S , B picks up a random bit $\beta \in \{0, 1\}$ and signcrypts the message M_β . Firstly, B searches H_1 -list to get l_i^* related to $ID_i^*, i \in \{1, 2, \dots, n\}$, and their public key $Q_i = l_i^* P - P_1$, then computes $y_i^* = a(P_1 + Q_i) = a(P_1 + l_i^* P - P_1) = a l_i^* P$ to get $T_i^*, i \in \{1, 2, \dots, n\}$. B finally creates the target ciphertext $C^* = \langle Y, X, U, \sigma, W, T^* \rangle$ where $X = a l_S P, U = a P, W = (a + h)l_S bP$ and $P_1 = cP$, and then returns C^* to A .

Phase 2. A performs a number of queries as Phase 1. Note that A cannot query the identity information of $(ID_1^*, ID_2^*, \dots, ID_n^*)$ in extraction query, and cannot query C^* in de-signcryption query.

Guess. Finally, A outputs its guess $\beta' \in \{0, 1\}$. If $\beta' = \beta$, B wins this game and outputs 1 as the answer of DBDH problem because $\Psi = e(P_{pub}, P_1)^\alpha = e(bP, cP)^a = e(P, P)^{abc}$. Otherwise, B outputs 0.

From the above discussion, we shall analyze the advantages of B in the following. For q_d de-signcryption queries, the probability to reject a valid ciphertext is not greater than $nq_d/2^k$. If A wins the IND-sMIBSC-CCA game, the advantage of B is

$$\begin{aligned} \epsilon' &= |\Pr[B(bP, cP, rP, \omega) = 1]| \\ &\quad - \Pr[B(bP, cP, rP, e(P, P)^{bcr}) = 1] \\ &\geq |\epsilon + 1/2 - nq_d/2^k - 1/2| \geq |\epsilon \\ &\quad + 1/2 - nq_d/2^k - 1/2| = \epsilon - nq_d/2^k \end{aligned}$$

Theorem 5. In the SUF-sMIBSC-CMA security model, if there is an adversary F who can win the game in the time t with a non-negligible advantage ϵ as described in the definition 5, there will exist an algorithm B which can solve the CDH problem in the time $t' \leq t$ with an advantage $\epsilon' \geq \epsilon - q_s/2^k$, where F can ask at most q_e extraction queries, q_s anony-signcryption queries and $q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}$ queries to H_1, H_2, H_3, H_4 , respectively.

Proof. The challenge B is given (P, aP, bP) as an instance of the CDH problem. Assume that there is an adversary F who has a non-negligible advantage ϵ in breaking the SUF-sMIBSC-CMA security. Then, B uses F to solve the CDH problem. Firstly, B simulates the system with the various oracles H_1, H_2, H_3 and H_4 , and then allows F to adaptively ask polynomially bounded number of queries to these oracles. The game between B and F is demonstrated below:

Setup. B sets $P_{pub} = bP$, and gives $\langle G_1, G_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4 \rangle$ to the attacker F as the public parameters. Upon receiving the system parameters, F outputs n target identities $L^* = \{ID_1^*, ID_2^*, \dots, ID_n^*\}$.

Attack. F adaptively performs polynomially bounded number of queries to the various oracles in this phase, which are similar to those in Theorem 4.

Forgery. F generates a target ciphertext $C^* = \langle Y^*, X^*, U^*, \sigma^*, W^*, T^* \rangle$. If the forgery is successful, the equation $e(W^*, P) = e(X^* + h \cdot r Q_S^*, P_{pub})$ holds. Define $Q_S^* = l_S^* P = aP$, and then we have $W^* = (h + \alpha) \cdot r D_S^* = (h + \alpha) l_S^* bP = (h + \alpha) abP$. Now, it will be very easy to extract the CDH problem's solution $abP = W^*(\alpha + h)^{-1}$.

We consider the advantage of F 's success here. As in the anony-signcryption query, the probability for B to answer a failure signcryption query is not greater than $q_s/2^k$, and then the advantage is $\epsilon' \geq \epsilon - q_s/2^k$.

Theorem 6. In the ANON-sID-CCA security model, if an adversary A has advantage ϵ against the game defined in Definition 6 within running time t (where A makes at most q_e private key extraction queries, q_s anony-signcryption queries, q_d de-signcryption queries and $q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}$ queries to the Hash functions H_1, H_2, H_3 and H_4 , respectively), then there is an algorithm B in solving the DBDH-M problem with an advantage $\epsilon' \geq \epsilon$.

Proof. The challenger B is challenged with an instance (P, aP, bP, Γ) of the DBDH-M problem. Assume that there is an adversary A who is capable of breaking the ANON-sID-CCA security with a non-negligible advantage ϵ . B makes use of A to solve the DBDH-M instance. B simulates the system with hash functions H_1, H_2, H_3 and H_4 , and allows A to make polynomially bounded number of queries. The game between B and A is demonstrated below:

Phase 1. Suppose that A outputs a target identity pair (ID_1^*, ID_2^*) .

Setup. B sets the public key $P_{pub} = \gamma_1 bP$ and lets $P_1 = aP$, where $\gamma_1, \gamma_2 \in \mathbb{Z}_q^*$, and aP and bP are given from the instance of the DBDH-M problem. Here, B does not know a and b . A performs polynomially bounded number of queries to H_1, H_2, H_3 and H_4 , which are similar to those in Theorem 4.

Phase 2. Upon receiving the private key extraction query of an identity ID_j such that $ID_j \neq ID_i^*$, for $i \in \{1, 2\}$, according to $Q_j = l_j P = aP$, B computes $D_j = l_j P_{pub}$.

Phase 3. Upon receiving a decryption query about (C^*, ID_i^*) , $i = 1, 2$ and $C^* = \langle Y^*, X^*, U^*, \sigma^*, W^*, T_1^* \rangle$. Challenger B performs the following steps:

- (1) Compute $\eta = T_1^*$.
- (2) Compute $\omega' = e(P_{pub}, \eta) e(U^*, D_\beta)^{-1}$.
- (3) Judge whether $H_2(\omega') = H_2(\omega)$ holds. If not, return “reject” to A , otherwise return $M^* = H_2(\omega) \oplus \sigma$ to A .

Challenge. A outputs a target plaintext M . Upon receiving M , B does the following steps:

- (1) Compute $U = abP - \gamma_1 P$.
- (2) Compute $\omega = e(P_{pub}, P_1)^{\gamma_2}$.
- (3) Create a target ciphertext $C = \langle Y, X, U, \sigma, W, T_1 \rangle$ and return it to A .

Phase 4. A issues private key extraction queries as those in Phase 2 and decryption queries for target identities as those in Phase 3, where a restriction here is that $C \neq C^*$.

Guess. Finally, A outputs its guess $\beta' \in \{1, 2\}$. If $\beta' = \beta$ holds, B outputs 1. Otherwise, B outputs 0. If $T_1 = a^2 bP$, then

$$\begin{aligned} \omega &= e(P_{pub}, P_1)^{\gamma_2} = e(\gamma_1 bP, \gamma_2 aP) \\ &= e(\gamma_1 bP, \gamma_2 aP + a^2 bP - a^2 bP) \\ &= e(\gamma_1 bP, a^2 bP) e((abP - \gamma_2 P), \gamma_1 abP)^{-1} \\ &= e(P_{pub}, \delta) e(U, D_\beta)^{-1} \end{aligned} \quad (7)$$

Thus, we have $M = H_2(\omega) \oplus \sigma$.

Here, C is the valid ciphertext. We can get $|\Pr[B(P, aP, bP, a^2 bP) = 1] - \Pr[\beta = \beta']| = \Pr[\beta = \beta'] - 1/2| \geq \epsilon$, and $|\Pr[B(P, aP, bP, \Gamma) = 1] - \Pr[\beta = \beta']| = 1/2$ where Γ is randomly chosen from G_1 . Therefore, we have $\epsilon = |\Pr[B(P, aP, bP, a^2 bP) = 1] - \Pr[B(P, aP, bP, \Gamma) = 1]| \geq |1/2 \pm \epsilon| - 1/2 = \epsilon$, that is, $\epsilon' \geq \epsilon$.

Efficiency Analysis

We compare our scheme with existing signcryption schemes [9,10,11,12,13,15,17,19] in terms of calculation costs and communication traffic (ciphertext length). In order to facilitate the description, we define the following symbols shown in Table 2:

First, we talk about the signcryption process. In the proposed scheme, the operation about Lagrange interpolation can also be pre-processed, so these operations can be excluded when considering computational complexity. In order to signcrypt a message M , our scheme needs 1 bilinear operation, 2 addition operations in G_1 , 6 scalar multiplications in G_1 , 1 exponentiation in G_2 and 2 hash operations. The length of the ciphertext is $(n+4)|G_1| + |M|$. The specific comparison results are shown in Table 3, from which one can see that our scheme performs much better than most of the existing schemes in terms of number of parameters, computation complexity and the ciphertext length.

Regarding the de-signcryption in our scheme, some calculations of the de-signcryption algorithm are used to judge the validity of ciphertext and the authorization of the recipient, which is important for broadcast-based communications to avoid receiving unwanted information (e.g. SPAM). Note that although the schemes [9,10,11,13,15] directly provide the recipients' true identities in the ciphertext, in fact the recipient cannot absolutely ensure whether he/she is authorized before checking the validity of the ciphertext. The number of pair operations (T_p , the most time-consuming operation in the existing schemes and our scheme) in our decryption algorithm is smaller than those of the existing schemes, which makes our scheme more attractive in terms of computation performance. Table 4 shows a comparison between the proposed scheme and the existing ones [9,10,11,12,13,15,17,19].

Discussion of Merit and Demerit

Compared to existing schemes, our scheme has some advantages. To achieve the signer's anonymity, the identity of the signer is no longer included in the ciphertext, although the private key of the signer is necessary for signcryption. The recipients can therefore only judge if the ciphertext received is from a trusted signer, but they cannot determine the real identity of the signer. To achieve the recipient's anonymity, the ID information of all authorized recipients is mixed by the Lagrange interpolation polynomial during the signcryption process, which prevents the recipient's ID from being exposed. This method also ensures that only the recipient, who has got the entire ciphertext, can decrypt the ciphertext, thus achieving the decryption fairness. The ID-based cryptography enables one user to confidentially send messages to other users, despite of whether the latter is a registered user, and the public verification property of our scheme enables unregistered users to judge the validity of the received

Table 2. Symbol Definition.

Symbols	Meaning
T_p	Time for bilinear pair operation
T_a	Time for addition operation
T_m	Time for scalar multiplication operation
T_e	Time for exponentiation operation
T_h	Time for Hash operation
T_s	Time for symmetric encryption algorithm

doi:10.1371/journal.pone.0063562.t002

Table 3. Signcryption Efficiency Comparison.

Schemes	Number of parameters	Computation Complexity	Ciphertext length
Yu <i>et al.</i> 's [9]	10	$T_p + (n+1)T_a + (n+5)T_m + T_e + 2T_h$	$(n+2) G_1 + G_2 + M + n ID $
Shamila <i>et al.</i> 's [10]	$n+9$	$(n+1)T_a + (n+3)T_m + T_e + 2T_h$	$3 G_1 + M + n ID $
Elkamchouchi [11]	8	$2T_p + (n+1)T_a + (n+4)T_m + 2T_e + 2T_h + T_s$	$(n+2) G_1 + M + n ID + Z_q $
Pang <i>et al.</i> 's [12]	12	$T_p + (3m-2)T_a + (2m+1)T_m + T_e + (m+1)T_h$	$(m+n+2) G_1 + M + m ID $
Lal <i>et al.</i> 's [13]	11	$(3m+n-2)T_a + (2m+n+2)T_m + T_e + (m+2)T_h$	$(m+n+2) G_1 + M + (m+n) ID $
Zhang B <i>et al.</i> 's [15]	13	$T_p + (m+n+1)T_m + (2m+n+3)T_e + 2T_h$	$(m+n+2) G_1 + M + m ID $
Zhang J <i>et al.</i> 's [17]	10	$T_p + (4m)T_m + (4m-2)T_a + (m+2)T_h$	$(m+2) G_1 + M $
Huang <i>et al.</i> 's [19]	10	$T_p + (2m-3)T_a + (2m+2)T_m + (m+2)T_h$	$2 G_1 + m G_2 + 2 M + m ID + m Z_q $
Ours	10	$T_p + 2T_a + 6T_m + T_e + 2T_h$	$(n+4) G_1 + M $

$|G_1|$: the length of the elements in G_1 ; $|ID|$: the length of ID; $|M|$: the length of the plaintext M ;
 m : the number of signers ($m=1$ in schemes [9–11] and our scheme); n : the number of recipients.
doi:10.1371/journal.pone.0063562.t003

ciphertext before having to register himself/herself with PKG. The merit/demerit comparison between the existing schemes and our scheme is summarized in Table 5.

From Table 5, we can see: (1) The schemes [12,13,15,17,19] have taken anonymity of the sender into account. However, they are all prone to the *cross-comparison attack* and *joint conspiracy attack*. In these schemes, in order to protect the privacy of the sender, the sender randomly chooses some legitimate participants to hide the true identity. But in practice, these schemes are vulnerable to the *cross-comparison attack* and *joint conspiracy attack* mentioned above. (2) The schemes [9,10,11] cannot assure the anonymity of the sender because the identity of the sender is directly given in the ciphertext. (3) The schemes [9,10,11,13,15,17,19] cannot assure the anonymity of the recipient. In these schemes, the ciphertext includes two parts: a recipient identity list and each recipient's specific data. A recipient identity list is required so that an authorized recipient is able to find his/her specific data required for decryption of the ciphertext. Because the recipient identity list is given in plaintext, the ID information of each recipient is exposed, and thus the anonymity of recipients is not assured. This has the advantage that, as long as an authorized recipient receives his/her specific data correctly, he/she can decrypt the ciphertext to retrieve the corresponding message even if other recipients' specific data are invalidated during transmission. While this seems

to represent an advantage on the first sight, it also represents a problem regarding decryption fairness. Decryption unfairness can cause the sender to cheat some recipients actively by just sending incorrect recipient-specific data. (4) In all the existing schemes, public verification is not considered because the identity of the sender or the recipient must be given in the ciphertext in plaintext form, thus there are no requirements for public verification. But in a completely anonymous scheme, public verification is a necessity for recipients so that receiving or operating on unwanted messages is prevented.

To summarize, the ciphertext in our scheme no longer contains the real identity information of all participants, thus our scheme meets anonymity of the sender and recipients at the same time, and efficiently protects the privacy of all involved participants. Even more important, this scheme possesses fair decryption and public verification properties. Furthermore, our scheme is easy to implement in existing applications. Here, we also take a network conference application as an example. In such a case, a message sender needs only to transform the plaintext message to a ciphertext message using our encryption algorithm and then broadcasts it through the broadcast communication channel, while a message recipient simply needs to decrypt the ciphertext using our decryption algorithm. Our scheme requires only extra encryption or decryption operations for each participant and

Table 4. De-signcryption Efficiency Comparison.

Schemes	Ciphertext validity or integrity	Authorized or not	Decryption
Yu <i>et al.</i> 's [9]	$3T_p + 2T_a + 3T_m + 3T_h$	$3T_p + 2T_a + 3T_m + 3T_h$	$3T_p + 2T_a + 3T_m + 3T_h$
Shamila <i>et al.</i> 's [10]	$3T_p + 2T_a + (3n+3)T_m + 2T_e + (n+1)T_h$	$3T_p + 2T_a + (3n+3)T_m + 2T_e + (n+1)T_h$	$3T_p + 2T_a + (3n+3)T_m + 2T_e + (n+1)T_h$
Elkamchouchi <i>et al.</i> 's [11]	$2T_p + T_e + T_m + 2T_h$	$2T_p + T_e + T_m + 2T_h$	$4T_p + 2T_a + T_e + 3T_h + T_s$
Pang <i>et al.</i> 's [12]	$2T_p + (2m-1)T_a + mT_m + mT_h$	$(2m-1)T_a + (m+2)T_m + mT_h$	$4T_p + (2m+n-2)T_a + (m+n+1)T_m + (m+2)T_h$
Lal <i>et al.</i> 's [13]	$2T_p + (2m-1)T_a + mT_m + mT_h$	$4T_p + 2mT_a + (m+1)T_m + (m+1)T_h$	$4T_p + 2mT_a + (m+1)T_m + (m+1)T_h$
Zhang B <i>et al.</i> 's [15]	$(m+5)T_p + T_a + (m+ M +2)T_m + 2T_h$	$(m+5)T_p + T_a + (m+ M +2)T_m + 2T_h$	$(m+5)T_p + T_a + (m+ M +2)T_m + 2T_h$
Zhang J <i>et al.</i> 's [17]	$4T_p + 2mT_a + mT_m + (m+2)T_h$	N/A	$4T_p + 2mT_a + mT_m + (m+2)T_h$
Huang <i>et al.</i> 's [19]	$3T_p + (m+1)T_a + 2mT_m + (m+2)T_h$	N/A	$3T_p + (m+1)T_a + 2mT_m + (m+2)T_h$
Ours	$2T_p + T_a + T_m + T_h$	$2T_p + T_a + T_m + T_h$	$2T_p + nT_a + (n-1)T_m + 2T_h$

$|M|$: the length of the plaintext M ; m : the number of signers ($m=1$ in schemes [9–11] and our scheme); n : the number of recipients.

Note: N/A refers to a single-recipient scheme where the message is transmitted using a unicast communication channel, thus it is unnecessary for the recipient to judge whether he/she is authorized.

doi:10.1371/journal.pone.0063562.t004

Table 5. Comparison of merits and demerits.

Scheme	Signer anonymity	Recipient anonymity	Decryption fairness	Public Verification
Yu <i>et al.</i> 's [9]	No	No	No	No
Shamila <i>et al.</i> 's [10]	No	No	No	No
Elkamchouchi <i>et al.</i> 's [11]	No	No	No	No
Pang <i>et al.</i> 's [12]	Yes (*)	Yes	Yes	No
Lal <i>et al.</i> 's [13]	Yes (*)	No	No	No
Zhang B <i>et al.</i> 's [15]	Yes (*)	No	No	No
Zhang J <i>et al.</i> 's [17]	Yes (*)	No	No	No
Huang <i>et al.</i> 's [19]	Yes (*)	No	No	No
Ours	Yes	Yes	Yes	Yes

Note: (*) refers to schemes prone to the *cross-comparison attack* and *joint conspiracy attack*.
doi:10.1371/journal.pone.0063562.t005

leaves the original implementation untouched, which in fact should represent an easy implementation of our scheme. While our scheme has the advantages mentioned above, it also has some disadvantages, namely its application, which increases the costs for the implementation. For example, it probably takes a great deal to establish PKG and maintain it, which may affect routine application of our scheme to some extent.

Conclusions

Due to the nature of broadcasting communications, the anonymity of both the sender and the recipient is of utmost importance in multi-recipient signcryption. However, almost none of the existing multi-recipient signcryption schemes take the anonymity of recipients into account. Although there are several schemes that provide a solution to the anonymity of the signer, they have known limitations. Owing to practical application requirements, a completely anonymous multi-recipient signcryption becomes more and more important. Aiming at the participants' anonymity, a completely anonymous multi-recipient signcryption is proposed in this paper. The new scheme ensures anonymity of all participants, the sender and all recipients. Furthermore, each recipient can easily judge whether the received message is from an authorized source, but he/she cannot determine the true identity of the sender. Each recipient can easily judge whether he/she is an authorized recipient, but he/she

cannot determine the identity of any other authorized recipient. At the same time, the validity of the ciphertext can be verified publicly. The confidentiality, unforgeability and anonymity of our scheme are formally proven using the random oracles model. Compared to existing schemes, our scheme is more efficient in computation and ciphertext length, and possesses more merits, which makes our scheme suitable for practical applications. Our scheme is important in group-oriented network applications, such as the network conference, paid-TV or DVD broadcasting. The proposed scheme solves the secure communication problem among authorized participants, while at the same time, it provides complete anonymity for all involved participants.

Acknowledgments

The authors would like to thank the anonymous reviewers of this paper for his/her objective comments and helpful suggestions while at the same time helping us to improve the English spelling and grammar throughout the manuscript.

Author Contributions

Proved the security of the scheme: LP HL LG. Conceived and designed the experiments: LP HL. Analyzed the data: LP HL LG YW. Wrote the paper: LP HL LG YW.

References

- Pang LJ, Li HX, Pei QQ (2012) Improved multicast key management of Chinese wireless local area network security standard. IET Communications 6: 1126–1130. doi:10.1049/iet-com.2010.0954.
- Pang L, Li H, Jiao L, Wang Y (2009) Design and analysis of a provable secure multi-recipient public key encryption scheme. Journal of Software 20: 2739–2745. doi:10.3724/SP.J.1001.2009.03552.
- Malone-Lee J (2002) Identity based signcryption. Cryptology ePrint Archive. Report 2002/098. Available: <http://eprint.iacr.org/2002/098.pdf>.
- Back J, Safavi-Naini R, Susilo W (2005) Efficient multi-receiver identity-based encryption and its application to broadcast encryption. Proc. the 8th International Workshop on Theory and Practice in Public Key Cryptography. Les Diablerets, Switzerland: 380–397. doi:10.1007/978-3-540-30580-4_26.
- Fan C, Huang L, Ho P (2010) Anonymous multireceiver identity-based encryption. IEEE Transactions on Computers 59: 1239–1249. doi:10.1109/TC.2010.23.
- Wang X, Wang A, Wang L (2009) Efficient ID-based secure encryption scheme for anonymous receivers. Academy Publisher 4: 1239–1249. doi:10.4304/jnw.4.7.641–648.
- Zhang B, Xu Q (2010) An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model. Proc. the Advances in Computer Science and Information Technology Japan: 15–27. doi:10.1007/978-3-642-13577-4_2.
- Duan S, Cao Z (2006) Efficient and provably secure multi receiver identity based signcryption. Proc. the Information Security and Privacy 11th Australasian Conference. Melbourne, Australia: 195–206. doi:10.1007/11780656_17.
- Yu Y, Yang B, Huang X, Zhang M (2007) Efficient identity-based signcryption scheme for multiple receivers. Proc. the Autonomic and Trusted Computing 4th International Conference. Hong Kong, China: 13–21. doi:10.1007/978-3-540-73547-2_4.
- Shamila S, Sree S, Srinivasan R, Pandu C (2009) An efficient identity-based signcryption scheme for multiple receivers. Proc. the Advances in Information and Computer Security 4th International Workshop on Security. Toyama, Japan: 71–88. doi:10.1007/978-3-642-04846-3_6.
- Elkamchouchi H, Abouelseoud Y (2009) MIDSCYK: An efficient provably secure multirecipient identity-based signcryption scheme. Proc. the International Conference on Networking and Media Convergence. Cairo, Egypt: 70–75. doi:10.1109/ICNM.2009.4907192.
- Pang L, Cui J, Li H, Pei Q, Jiang Z, et al (2011) A new multi-receiver ID-based anonymous signcryption. Chinese journal of computer 34: 2104–2113. doi:10.3724/SP.J.1016.2011.02104.
- Lal S, Kushwah P (2009) Anonymous ID based signcryption scheme for multiple receivers. Cryptology ePrint Archive. Available: <http://eprint.iacr.org/2009/345.pdf>.

14. Qin H, Dai Y, Wang Z (2011) Identity-based multi-receiver threshold signcryption scheme. *Security and Communication Networks* 4: 1331–1337. doi:10.1002/sec.259.
15. Zhang B, Xu Q (2010) An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model. *Proc. of the AST/UCMA/ISA/CAN conferences*. Miyazaki, Japan: 15–27. doi:10.1007/978-3-642-13577-4_2.
16. Zheng Y (1997) Digital signcryption or how to achieve cost (signature & encryption) < cost (signature) + cost (encryption) Proc. the 17th Annual International Cryptology Conference on Advances in Cryptology. London, UK: 165–179. doi:10.1007/BFb0052234.
17. Zhang J, Gao S, Chen H, Geng Q (2009) A novel ID-based anonymous signcryption scheme. *Proc. the Advances in Data and Web Management Joint International Conferences*. Suzhou, China: 604–610. doi:10.1007/978-3-642-00672-2_58.
18. Rivest R, Shamir A, Tauman Y (2001) How to leak a secret: Theory and applications of ring signatures. *Proc. the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*. London, UK: 552–565. doi:10.1007/11685654_7.
19. Huang X, Susilo W, Mu Y, Zhang F (2005) Identity based ring signcryption scheme: Cryptographic primitive for preserving privacy and authenticity in the ubiquitous world. *Proc. the 19th International Conference on Advanced Information Networking and Applications*. Taipei, Taiwan: 649–654. doi:10.1109/AINA.2005.205.
20. Gafurov D, Sneekenes E, Buvarp T (2006) Robustness of biometric gait authentication against impersonation attack. *Proc. The OTM Workshops*. Montpellier, France: 479–488. doi:10.1007/11915034_71.
21. Xie Q, Yu X (2005) A new (t, n) threshold signature scheme withstanding the conspiracy attack. *Wuhan University Journal of Natural Sciences* 10: 107–110. doi:10.1007/BF02828628.