PLOS ONE

RESEARCH ARTICLE

A Novel Multi-Receiver Signcryption Scheme with Complete Anonymity

Liaojun Pang[1,2]*, Xuxia Yan[1], Huiyang Zhao[1], Yufei Hu[1], Huixian Li[3]*

1 State Key Lab. of Integrated Services Networks, School of Life Science and Technology, Xidian Univ., Xi'an, 710071, Shaanxi, China, **2** Dept. of Comput. Sci., Wayne State University, Detroit, MI 48202, United States of America, **3** School of Computer Science and Engineering, Northwestern Polytechnical Univ., Xi'an, 710072, Shaanxi, China

* ljpang@mail.xidian.edu.cn (LP); lihuixian@nwpu.edu.cn (HL)

Citation: Pang L, Yan X, Zhao H, Hu Y, Li H (2016) A Novel Multi-Receiver Signcryption Scheme with Complete Anonymity. PLoS ONE 11(11): e0166173. doi:10.1371/journal.pone.0166173

Editor: Muhammad Khurram Khan, King Saud University, SAUDI ARABIA

Received: June 21, 2016

Accepted: October 23, 2016

Published: November 10, 2016

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Funding: This work was supported by Natural Science Foundation of China (61103178), Natural Science Basic Research Plan in Shaanxi Province of China (2016JM6002 & 2015JM6294), and Fundamental Research Funds for the Central Universities (3102015JSJ0003).

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

Abstract

Anonymity, which is more and more important to multi-receiver schemes, has been taken into consideration by many researchers recently. To protect the receiver anonymity, in 2010, the first multi-receiver scheme based on the Lagrange interpolating polynomial was proposed. To ensure the sender's anonymity, the concept of the ring signature was proposed in 2005, but afterwards, this scheme was proven to has some weakness and at the same time, a completely anonymous multi-receiver signcryption scheme is proposed. In this completely anonymous scheme, the sender anonymity is achieved by improving the ring signature, and the receiver anonymity is achieved by also using the Lagrange interpolating polynomial. Unfortunately, the Lagrange interpolation method was proven a failure to protect the anonymity of receivers, because each authorized receiver could judge whether anyone else is authorized or not. Therefore, the completely anonymous multi-receiver signcryption mentioned above can only protect the sender anonymity. In this paper, we propose a new completely anonymous multi-receiver signcryption scheme with a new polynomial technology used to replace the Lagrange interpolating polynomial, which can mix the identity information of receivers to save it as a ciphertext element and prevent the authorized receivers from verifying others. With the receiver anonymity, the proposed scheme also owns the anonymity of the sender at the same time. Meanwhile, the decryption fairness and public verification are also provided.

Introduction

Research backgroud

In 2000, Bellare *et al.* [1] firstly proposed the concept of multi-receiver public key encryption. In their scheme, to acquire the ciphertext which each authorized receiver can decrypt with his private key, the sender needed to repeatedly use the public key of each receiver to perform the public key encryption for the same plaintext. Although this scheme meets the requirement of the multi-receiver encryption, it is inadaptable to large-scale broadcast encryption, because its encryption computation complexity and ciphertext length are directly related to the number

of the receivers. To overcome this weakness, Kurosawa [2] adopted a "randomness reuse" technique to propose a multi-receiver encryption scheme, in which the computational efficiency was improved. Later, Bellare *et al.* [3] further improved its performance. But these two schemes only concern how to improve the efficiency of multiple encryptions rather than how to reduce the number of encryptions.

Even so, these early multi-receiver schemes pointed out a new direction in the field of the information security: multi-receiver encryption, in which the sender only needs one encryption operation to send the same message for n receivers, and every authorized receiver can independently use his private key to decrypt the ciphertext, which significantly increases the efficiency comparing the early schemes [1–3]. In 2005, by introducing the idea of identity based encryption into the multi-receiver encryption, Baek *et al.* [4] proposed an efficient multi-receiver ID-based scheme, in which the sender only needed to encrypt the same message once and sent it to n selected receivers. This scheme required a linear ciphertext size in proportion to the number of the selected receivers. In 2006, Chatterjee and Sarkar [5] proposed an efficient multi-receiver ID-based scheme with sublinear ciphertext size. Later on, there appeared many great schemes [6–8] contributing to the ID-based multi-receiver encryption.

With the development of encryption, more and more researchers find that receivers need to verify the source of the message in practical applications. There are some signcryption schemes [9–12] have been proposed to advance the signcryption research. For the multi-receiver cryptography, multi-receiver signcryption gradually becomes the research focus. In 2006, the first ID-based multi-receiver signcryption scheme was presented by Duan *et al.* [13], which introduced the concept of Zheng's signcryption [14] into multi-receiver encryption. In Duan *et al.*'s scheme, the sender can sign and encrypt the plaintext in only one operation as well as each authorized receiver can independently decrypt the ciphertext and verify the message source. Later on, many excellent multi-receiver signcryption schemes [15–21] have been proposed by researchers. However, all these early schemes did not care the privacy of participants, because the sender and receiver list, a part of the ciphertext, are required to participate in the de-signcryption process.

Recently, with the maturity of the ID-based multi-receiver signcryption, researchers have paid more attention to the anonymity of participants. Generally speaking, the anonymity includes two parts, the receiver anonymity and the sender anonymity. In 2010, Fan *et al.* [22] pointed out the importance of the receiver anonymity in ID-based multi-receiver setting and proposed a multi-receiver anonymous encryption scheme to protect anonymity of receivers with the Lagrange interpolation polynomial. In their scheme, the Lagrange interpolation polynomial is used to mix and hide the identities of the receivers to avoid exposing their information, and that seems perfect to protect the receiver anonymity. Then, several multi-receiver signcryption schemes [23–25] based on the Lagrange interpolation polynomial were proposed.

For the sender anonymity, in 2009, Lal *et al.* [26] adopted Huang *et al.*'s [27] concept of ring signature to present a multi-receiver signcryption scheme with sender anonymity. Later, based on the ring signature, several multi-receiver signcryption schemes [28–30] were proposed to protect the anonymity of the sender. However, in 2013, Pang *et al.* [31] pointed that these schemes whose sender anonymity is based on the ring signature shall suffer from the cross-comparison attack and the joint conspiracy attack. That is to say, the scope of the real sender could be narrowed down gradually with the increase of communication. Even, the identity of real sender could be uniquely determined. In order to solve this problem, Pang et al. improved the ring signature with a randomized method, which uses the public key of the sender multiplied by a random value to hide the identity of the sender. By this means, any receiver can only judge whether the ciphertext is from a reliable sender or not, rather than actually getting the real identity of the sender. Besides, the receiver anonymity with the

Lagrange interpolation polynomial was provided in Pang *et al.*'s scheme [31]. So, it is a completely anonymous multi-receiver signcryption scheme.

Unfortunately, in 2012, Wang *et al.* [32] and Zhang *et al.* [33] respectively found that Fan *et al.*'s scheme fails to protect the receiver anonymity, because any authorized receiver can judge whether the others are authorized or not. This means that the authorized receivers may be attacked by other authorized receivers. Meanwhile, Wang et al. also made an improvement on Fan *et al.*'s scheme. However, in 2014, Li *et al.* [34] analyzed Wang *et al.*'s scheme and found that the Lagrange interpolation polynomial is still used to mix and hide the identities of the receivers, which is not able to really protect the receiver anonymity either. Because of the problem of Lagrange interpolation polynomial construction, any authorized receiver can judge whether other receivers is the authorized or not. Through analyses above, Pang *et al.*'s [31] completely anonymous multi-receiver signcryption scheme cannot realize the receiver anonymity. Then, it remains an open problem how to design a new multi-receiver signcryption scheme which can achieve the receiver anonymity and the sender anonymity at the same time.

Our contribution

Aiming at the problem discussed above, in this paper, we try to find a new construction method to design a completely anonymous multi-receiver signcryption scheme cannot realize the receiver anonymity and the sender anonymity at the same time. In order to achieve the receiver anonymity, we find a new polynomial that could be used to replace the Lagrange interpolation polynomial. With the new polynomial, we can mix the identity information of receivers to save it as ciphertext element and prevent the authorized receivers from verifying the others. That is to say, attackers not only outside the system but also inside the system can be prevented in our new scheme, which can actually realize the receiver anonymity. To protect the sender anonymity, the randomized method was also used in our scheme. Hence, our scheme simultaneously has the sender anonymity and receiver anonymity, and eliminates the anonymity problem existing in the previous scheme.

Paper organization

The rest of the paper is designed as follows. Preliminaries are given in Section 2, and Section 3 presents our new scheme. Then, we prove the security of the proposed scheme in Section 4. Section 5 gives the efficiency and performance analysis. Finally, Section 6 draws the conclusions.

Preliminaries

In this section, we will briefly review the bilinear pairings, related problems and security assumptions on which our improved scheme is based.

Bilinear pairings

Let G_1 be a cyclic additive group of large prime order q, and G_2 be a cyclic multiplicative group of the same order q. Let P be a generator of G_1. A bilinear pairing is a map e: $G_1 \times G_1 \rightarrow G_2$ and satisfies the following properties:

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in Z_q^*$.
2. Nondegenerate: There exist $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3. Computable: For all $P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q)$.

A bilinear pairing map which satisfies the above three properties is called an admissible bilinear map.

Problems and security assumptions

Here, we give mathematical hard problems and define the security assumptions on which our scheme is based.

(1) CDH (Computational Diffie-Hellman) problem: Given $(P, aP, bP) \in G_1$ for some $a, b \in Z_q^*$, to compute abP.

Definition 1: The advantage of any PPT algorithm A in solving the Computational Diffie-Hellman (CDH) problem is defined as:

$$Adv_A^{CDH} = Pr[A(P, aP, bP) = abP] \tag{1}$$

CDH assumption: For any PPT algorithm A, Adv_A^{CDH} is negligible.

(2) DBDH (Decision Bilinear Diffie-Hellman) problem: Given $(P, aP, bP, cP) \in G_1$ for unknown $a, b, c \in Z_q^*$, and $R \in G_2$, to decide whether $e(P, P)^{abc} = R$.

Definition 2: The advantage of any PPT algorithm A in solving the DBDH (Decision Bilinear Diffie-Hellman) problem is defined as:

$$Adv_A^{DBDH} = |Pr[A(P, aP, bP, cP, e(P, P)^{abc}) = 1] - Pr[A(P, aP, bP, cP, R) = 1]| \tag{2}$$

DBDH assumption: For any PPT algorithm A, Adv_A^{DBDH} is negligible.

(3) Gap-BDH (Gap Bilinear Diffie-Hellman) problem: Given $(P, aP, bP, cP) \in G_1$ for unknown $a, b, c \in Z_q^*$, to compute $e(P, P)^{abc} \in G_2$ with the help of the DBDH (Decision Bilinear Diffie-Hellman) oracle.

Definition 3: The advantage of any PPT algorithm A in solving the Gap-BDH (Gap Bilinear Diffie-Hellman) problem is defined as:

$$Adv_A^{Gap-BDH} = Pr[A(P, aP, bP, cP) = e(P, P)^{abc}] > \varepsilon \tag{3}$$

Gap-BDH assumption: For any PPT algorithm A, $Adv_A^{Gap-BDH}$ is negligible.

Security models

We shall give the security models for confidentiality, unforgeability and anonymity in Definitions 4-6, respectively.

Definition 4: IND-sMIBSC-CCA (indistinguishability of ciphertexts under selective multi-ID, chosen ciphertext attack) [13].

Suppose that there is a polynomial-time attacker named A and an anonymous ID-based multi-receiver signcryption algorithm named Π. A plays a game with a Challenger B as follows:

Setup: Challenger B performs this algorithm to generate master key s and public parameters params. Then B shall send the params to A but keep s secret. After receiving the parameter, A outputs target multiple identities $L^* = \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$.

Phase 1: Challenger B shall answer a number of different queries from adversary A in an adaptive manner as follows:

Key extract query: Queried about an identity ID that A pretends to be, B shall run the Key extract algorithm to get $D = Extract(params, s, ID)$.

Anony-signcrypt query: Adversary A runs the Anony-signcrypt algorithm to get the ciphertext $C = Anony - signcrypt(params, M, L, D_S)$, where M is the target plaintext chosen by

adversary A, $L = \{ID_1, ID_2, \cdots, ID_n\}$ is the set of the receiver identity, ID_S is the identity chosen by B and D_S is the corresponding private key.

De-signcrypt query: Adversary A shall send $B(C, ID_j)$ where C is the ciphertext produced by adversary A, ID_j is the identity chosen by B and $ID_j \in L^*$. $L^* = \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$ is the target multiple identities chosen by A. Then B shall perform the De-signcryption algorithm to get the plaintext $M = De - signcrypt(C^*, params, D_i^*)$. If M is valid, B returns it to A. Otherwise, returns "failure".

Challenge: Adversary A shall first choose target plaintext pair(M_0, M_1) and pretend a sender ID_S. When receiving the target plaintext and the private key D_S, the challenger B randomly chooses $\beta \in \{0, 1\}$ and signcrypts the message M_β to generate the ciphertext $C^* = Anony - signcrypt(params, M_\beta, L^*, D_S)$. Then, the challenger B returns C^* to A.

Phase 2: A shall query challenge B like Phase 1. Note that A cannot query the information of $(ID_1^*, ID_2^*, \cdots, ID_n^*)$ in the Key extract query and C^* in De-signcrypt query.

Guess: A guesses $\beta' \in \{0, 1\}$ and outputs it. If $\beta = \beta'$, A wins the IND-sMIBSC-CCA game. Otherwise, returns "failure".

A's guessing advantage is defined as follows:

$$Adv_{\Pi}^{IND-sMIBSC-CCA} = |Pr[\beta = \beta^{'}] - 1/2|$$

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.

Definition 5: SUF-MIBSC-CMA (strong existential unforgeability under selective multi-ID, chosen message attack) [13].

Suppose that there is a forger named F and an anonymous ID-based multi-receiver signcryption algorithm named Π. F plays a game with a challenger B as follows:

Setup: Challenger B performs this algorithm to generate master key s and public parameters params. Then B shall send the params to A but keep s secret. After receiving the parameter, F outputs target multiple identities $L^* = \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$.

Attack: The forger F may make some queries to the challenger B as phase 1 in Definition 4.

Forgery: Forger F shall output a ciphertext C^* and a set of identities $L^* = \{ID_1^*, ID_2^*, \cdots, ID_n^*\}$. If C^* can be decrypted correctly by every receiver ID_i^* where $i \in \{1, 2, \cdots, n\}$ in the set L^*, then verify the source of the sender, C^* is valid and F wins the game.

But the forger F cannot perform Key extract query to ID_i^* and C^* cannot generated by Anony-signcrypt algorithm here.

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

Definition 6: ANON-IND-sMID-CCA (anonymous indistinguishability of signcryption under selective multi-ID, chosen ciphertext attack) [25].

Suppose that there is a polynomial-time attacker named A and an anonymous ID-based multi-receiver signcryption algorithm named Π. In order to get the identity of anonymous receivers, A plays a game with a challenger B as follows:

Setup: Challenger B performs this algorithm to generate master key s and public parameters params. Then B shall send the params to A but keep s secret. After receiving the parameter, A choses target identities (ID_1^*, ID_2^*).

Phase 1: Challenger B shall answer the Key extract query and De-signcryption query from adversary A as follows:

Key extract query: Queried about an identity ID_j that A pretends to be, where $ID_j \neq (ID_1^*, ID_2^*)$, B shall run the Extract algorithm to get $D_j = Extract(parems, s, ID_j)$.

De-signcrypt query: Adversary A shall send $B(C^*, ID_i^*)$ where $i \in \{1, 2\}$ to B. Then B shall perform the De-signcryption algorithm to get the plaintext $M = De - signcrypt(C^*, params, D_i^*)$. If M is valid, B returns it to A. Otherwise, returns "failure".

Challenge: Adversary A shall first choose target plaintext M^* and the identities $\{ID_3^*, ID_4^*, \cdots, ID_n^*\}$, where $n \geq 3$. Then B shall execute the signcryption algorithm to generate the ciphertext $C^* = Anony - signcrypt(params, M^*, (ID_\beta^*, ID_3^*, ID_4^*, \cdots, ID_n^*), D_j)$. Then, the challenger B returns C^* to A.

Phase 2: A shall query challenge B like Phase 1 without querying for C^* in De-signcrypt query the information of (ID_1^*, ID_2^*) in the Key extract query.

Guess: A guesses $\beta' \in \{1, 2\}$ and outputs it. If $\beta = \beta'$, A wins the ANON-IND-sMID-CCA game.

A's guessing advantage is defined as follows:

$$Adv_{\Pi}^{ANON-IND-sMID-CCA}(A) = |Pr[\beta = \beta^{'}] - 1/2|$$

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

The proposed scheme

In this section, we will present our scheme, which includes four algorithms: Setup, Key extract, Anony-signcrypt, and De-signcrypt algorithms. Detailed description is as follows:

Setup algorithm

Here, PKG shall execute the following process:

1. PKG chooses a prime order $q(q \geq 2^l, l$ is a long integer), and then chooses G_1 (an additive group) and G_2 (a multiplicative group) with the same order q. Then it randomly picks a generator P of G_1, and constructs a bilinear mapping e: $G_1 \times G_1 \rightarrow G_2$. PKG keeps the master key s secret, which is picked up from Z_q^*. Select some integer w. Set $P_{pub} = sP \in G_1$ as the system public key. The symmetric encryption and decryption are denoted as $E_k()$ and $D_k()$ where k is the key.
2. PKG constructs five cryptographic hash functions: H_1: $\{0, 1\}^* \rightarrow G_1$; $H_2 : G_2 \longrightarrow Z_q^*$; $H_3 : Z_q^* \longrightarrow \{0, 1\}^w$; H_4: $\{0, 1\}^w \rightarrow \{0, 1\}^{|M|}$; $H_5 : G_1 \times G_1 \times \{0, 1\}^w \times Z_q^* \times Z_q^* \times \cdots \times Z_q^* \longrightarrow Z_q^*$.
3. PKG publishes the system parameters $params = \{q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3, H_4, H_5, E_k(), D_k()\}$.

Key extract algorithm

PKG shall execute this algorithm to generate ID_i's private key with s, params and an identity $ID_i \in \{0, 1\}^*$. Then, PKG shall also return ID_i's private key. That means ID_i has registered himself at PKG:

1. Compute ID_i's public key $Q_i = H_1(ID_i)$.
2. Compute ID_i's public key $D_i = sH_1(ID_i) = sQ_i$.

Anony-signcrypt algorithm

This algorithm is executed by the sender. Obtaining his private key D_S and params, the sender ID_S shall choose n receivers with identities $ID_1, ID_2, \cdots, ID_n$ and encrypt the plaintext M to generate the ciphertext C:

1. The sender firstly pick up two random integers $\gamma, \alpha \in Z_q^*$ and a bit string $\delta \in \{0, 1\}^w$, and then compute $Y = rQ_S$, $U = rP$, $X = \alpha Y$ and $J = rP_{pub}$, where Q_S is the public key of ID_S.
2. The sender computes $v_i = H_2(e(Q_i, J)$, where $Q_i = H_1(ID_i)$.
3. The sender chooses a random $p \in Z_q^*$ and constructs a polynomial $f(x)$ with degree n as follows:

$$\begin{aligned} f(x) &= \prod_{i=1}^{n}(x - v_i) + p(mod\ q) \\ &= a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \end{aligned}$$

4. Compute $V = \delta \bigoplus H_3(p)$, $Z = E_{H_4(\delta)}(M)$ and $h = H_5(X, U, Z, V, a_0, a_1, \cdots, a_{n-1})$, and then compute $W = (\alpha + h)\cdot rD_S$, where D_S is the private key of ID_S.
5. Generate the ciphertext: $C = \langle Y, U, Z, V, W, a_0, a_1, \cdots, a_{n-1}\rangle$.

De-signcrypt algorithm

This algorithm is executed by the receiver. With params, $C = \langle Y, U, Z, V, W, a_0, a_1, \cdots, a_{n-1}\rangle$, the receiver's identity ID_i and his private key D_i as input, the receiver ID_i has the ability to decrypt C as follows:

1. Compute $h = H_5(X, U, Z, V, a_0, a_1, \cdots, a_{n-1})$.
2. Public verification: The one who has not registered shall execute this step. The participant who has registered shall jump to the judgment algorithm without the verification.
   If the equation $e(W, P) = e(X + hY, P_{pub})$ holds, that is to say, the ciphertext is valid. Otherwise, the ciphertext has been damaged or it is invalid.
3. Judgment: The registered participants shall execute this step before the decryption process. If the equation $e(W, Q_i) = e(X + hY, D_i)$ holds, ID_i is one of the receivers chosen by the sender and the ciphertext is valid. Otherwise, the receiver shall quit the decryption process.
4. Compute $v_i^{'} = H_2(e(D_i, U))$ and $p = f(v_i^{'})$.
5. Compute $\delta = V \bigoplus H_3(p)$ and $K = H_4(\delta)$.
6. Decryption: $M' = D_{H_4(\delta)}(Z)$.

Every receiver who gets the ciphertext can verify the validity of the message by the public verification or judge if he is authorized by the judgment algorithm. Then, if necessary, he can decrypt the ciphertext.

Correctness and security analysis

Correctness analysis

Here, we show the correctness of the proposed scheme by stating Theorems 1-3.

Theorem 1: The public verification of the proposed scheme is correct.

Proof: Whether the equation $e(W, P) = e(X + hY, P_{pub})$ holds is used to perform the public verification because of the following:

$$\begin{aligned} e(W,P) &= e((\alpha+h)\cdot rD_S, P) \\ &= e((\alpha+h)\cdot rQ_S, sP) \\ &= e(\alpha Y + hY, sP) \\ &= e(X + hY, P_{pub}) \end{aligned}$$

Theorem 2: The judgement of the proposed scheme is correct.

Proof: Whether the equation $e(W, Q_i) = e(X + hY, D_i)$ holds is used to perform the judgement because of the following:

$$\begin{aligned} e(W,Q_i) &= e((\alpha+h)\cdot rD_S, Q_i) \\ &= e((\alpha+h)\cdot rQ_S, sQ_i) \\ &= e(\alpha Y + hY, D_i) \\ &= e(X + hY, D_i) \end{aligned}$$

Theorem 3: The decryption of the proposed scheme is correct.

Proof: The decryption of the proposed scheme is correct because of the following:

$$\begin{aligned} v_i' &= H_2(e(D_i, U)) \\ &= H_2(e(sQ_i, U)) \\ &= H_2(e(Q_i, rsP_{pub})) \\ &= H_2(e(Q_i, J)) \\ &= v_i \end{aligned}$$

Security analysis

Here, we shall prove that the proposed multi-receiver signcryption scheme is secure against the IND-sMIBSC-CCA, SUF-MIBSC-CMA and ANON-IND-sMID-CCA attacks defined in Section 2.3, which respectively shows the confidentiality, unforgeability, and anonymity.

Theorem 4: If an IND-sMIBSC-CCA attacker A has a non-negligible advantage ε to win the game defined in Definition 4 within running time t, then the DBDH problem can be solved by the challenger B in running time $t' \leq t$ with a non-negligible advantage $\varepsilon' \geq \varepsilon - nq_d/2^k$, where attacker A asks q_e queries to the Key extract query, q_s queries to the Anony-signcrypt query, and q_d queries to the De-signcrypt query. (q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}, q_{H_5}) denote the number of queries to the hash functions H_1, H_2, H_3, H_4, H_5, respectively.

Proof: An instance (P, aP, bP, cP) of the DBDH problem is given to simulate the game defined in Definition 4, and A denotes attacker, B denotes challenger. Suppose that A has a non-negligible advantage ε to break the IND-sMIBSC-CCA model, and B solves the instance of DBDH problem by interacting with A. There are five oracles H_1, H_2, H_3, H_4 and H_5 to simulate the system for B. A can queries PPT times to the oracles. B executes and answers each phase of the IND-sMIBSC-CCA game as follows:

Setup: The challenger B sets $Q = aP$ and $P_{pub} = bP$. Then, B sends $\langle G_1, G_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4, H_5, E_k, D_k \rangle$ to A as the public parameters. When receiving the parameter, A outputs target multiple identities $(ID_1^*, ID_2^*, \cdots, ID_n^*)$.

Phase 1: A proposes queries as follows to B.

Assume that the hash functions $H_i(i = 1, 2, 3, 4, 5)$ are random oracles controlled by the challenger B. For the attacker A's hash queries, the challenger B uses list $L_i(i = 1, 2, 3, 4, 5)$ to record the results of hash functions $H_i(i = 1, 2, 3, 4, 5)$, respectively.

***H_1*-query:**

1. If $ID_j \neq ID_i^*, i \in \{1, 2, \cdots, n\}$, calculate $Q_j = l_j P$; otherwise, calculate $Q_j = l_j Q$, where l_j is an integer.
2. Put it into H_1-list when no (ID_j, l_j, Q_j) exists in H_1-list.
3. B returns Q_j.

***H_2*-query:** The challenger B examines if $(P, Q_i, P_{pub}, cP, X_j)$ uses the DBDH oracle for $i \in [1, q_{H_2}]$ when he is queried with $X_j \in G_2$ for some $j = [1, q_{H_2}]$. If it exists, B shall terminate the game for $e(P, P)^{abc}$ equals $(X_j)^{l_i^{-1}}$. Otherwise, B picks a value $x_j \in Z_q^*$ at random and puts a tuple (X_j, x_j) into the list L_2. Then, the challenger B returns x_j to the adversary A.

***H_3*-query:** As an integer p_j is sent to the H_3 oracle where $j \in [1, q_{H_3}]$, B shall pick a string $w_j \in \{0, 1\}^w$ at random and puts the tuple (p_j, w_j) into the list L_3. Then, the string w_j is returned to A by the challenger B.

***H_4*-query:** When querying for the string $\delta_j \in \{0, 1\}^w$ where $j \in [1, q_{H_4}]$, B shall pick a string $z_j \in \{0, 1\}^{|M|}$ at random and puts the tuple (δ_j, z_j) into the list L_4. Then, the challenger B returns the bit string z_j to the attacker A.

***H_5*-query:** Receiving the tuple $\langle X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}}\rangle$ where $j \in [1, q_{H_5}]$, B picks a value h_j in Z_q^* at random and puts the tuple $\langle X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}}, h_j\rangle$ into the list L_5. Then, B returns h_j.

Key extract query: A chooses an identity $ID_j \neq ID_i^*$ where $i \in \{1, 2\}$ and sends it to challenger B, then B scans the list L_1 to find if there is the tuple (ID_j, l_j, Q_j) in L_1. If it was, B shall calculate $D_j = l_j P_{pub} (= l_j bP = bQ_j)$. Otherwise, the challenger B selects a $l_j \in Z_q^*$ at random, and calculates $Q_j = l_j P$ as well as $Dj = l_j P_{pub}$. At the same time, the challenger B puts a tuple (ID_j, l_j, Q_j) into the list L_1. Finally, B sends D_j back to the attacker A.

Anony-signcrypt query: When receiving the anonymous signcryption query with (M, ID_S, L) from A, B checks whether there exist $ID_S \neq ID_i^* (i = 1, 2, \cdots, n)$. If $ID_S \neq ID_i^* (i = 1, 2, \cdots, n)$, B can get the private key of ID_S from Key extract query. Then, A can get ciphertext C from Anony-signcrypt query. Otherwise, perform the following tasks:

1. Select $\gamma, \alpha \in Z_q^*$ and $\delta \in \{0, 1\}^w$ at random, then compute $Y = \gamma l_S P$, $U = \gamma P$, $X = \alpha Y$, $J = \gamma P_{pub}$.
2. Compute $\upsilon_i = H_2(e(Q_i, J))$, where $Q_i = H_1(ID_i)$ is the public key of the receiver.
3. Choose $p \in Z_q^*$ at random and structure a polynomial $f(x)$ with degree n as follows:

$$\begin{aligned} f(x) &= \prod_{i=1}^{n} (x - \upsilon_i) + p(mod\ q) \\ &= a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n. \end{aligned}$$

4. Compute $V = \delta \bigoplus H_3(p)$, $Z = E_{H_4(\delta)}(M)$ and $h = H_5(X, U, Z, V, a_0, a_1, \cdots, a_{n-1})$, and then compute $W = (\alpha + h) l_S P_{pub}$.
5. Generate the ciphertext: $C = \langle Y, U, X, Z, V, W, a_0, a_1, \cdots, a_{n-1}\rangle$.

De-signcrypt query: The attacker A queries B and send $B(C_j, ID_i^*)$ where $i \in \{1, 2\}$ and $C_j = \langle Y_j, U_j, X_j, Z_j, V_j, W_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}} \rangle$ When receiving the decryption query, B executes the following steps:

1. Check the list L_5 to find the tuple $\langle X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}}$. If it was found, B can get (Z_j, V_j) from L_5. Otherwise, B returns "failure".
2. Construct the polynomial $f(x) = a_{j_0} + a_{j_1} x + \cdots + a_{j_{n-1}} x^{n-1} + x^n$.
3. Searching the tuple (ID_j, l_j, Q_j) in the list L_1.
4. For $l = 1, 2, \cdots, q_{H_2}$, perform as follows:
   a. Search the tuple (X_l, x_l) from the list L_2.
   b. Examine whether $(P, Q_i, P_{pub}, U_j, X_j)$ uses the DBDH oracle by verifying the equation $e(P, P)^{l_j \, b\gamma} = X_j$.
   c. If the step above is true, calculate $p_l = f(x_l)$, $\delta_j' = V_j \bigoplus H_3(p_i)$, and $M_j = D_{H_4}(\delta_j')(Z_j)$.
5. Test whether the equation $e(W_j, P) = e(X_j + h_j Y_j, P_{pub})$ or the equation $e(W_j, Q_i) = e(X_j + h_j Y_j, D_i)$ holds where $h_j = H_5(X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}})$. If it holds, then return M_j to A.
6. Otherwise, B sends "failure" to A, which means that there is not a valid ciphertext generated following the proposed scheme.

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, the challenger B randomly chooses $\beta \in \{0, 1\}$ and signcrypts the message M_β. B finally creates a target ciphertext $C^* = \langle Y, U, X, Z, V, a_0, a_1, \cdots, a_{n-1} \rangle$, where $Y = \gamma l_S P$, $U = \gamma P$, $X = \alpha Y$, $Z = E_{H_4(\delta)}(M)$, $V = \delta \bigoplus H_3(p)$ and $W = (\alpha + h) l_S P_{pub}$, then returns C^* to A.

Phase 2: A shall query challenge B like Phase 1. Note that A cannot query the information of $(ID_1^*, ID_2^*, \cdots, ID_n^*)$ in the Key extract query and C^* in De-signcrypt query.

Guess: The attacker A gives its guess $\beta' \in \{0, 1\}$. If $\beta' = \beta$, B wins the game because the equation $\Psi = e(P_{pub}, P_1)^\alpha = e(P, P)^{abc}$ holds. Otherwise, B outputs "failure".

According the above discussion, we can get the advantage of B as following equation. For q_d times De-signcrypt query, the probability for B to reject the valid plaintext is less than $nq_d/2^k$. So, if A wins the game, B's advantage is

$$\begin{aligned} \varepsilon' &= |Pr[A(aP, bP, cP, w) = 1] - Pr[A(aP, bP, cP, e(P, P)^{abc}) = 1]| \\ &\geq |\varepsilon + 1/2 - nq_d/2^k - 1/2| \\ &= \varepsilon - nq_d/2^k \end{aligned}$$

Theorem 5: If a SUF-sMIBSC-CMA forger F has a non-negligible advantage ε to win the game defined in Definition 5 within time t, then the challenger B can solve the CDH problem with an advantage $\varepsilon' \geq \varepsilon - q_s/2^k$ in running time $t' \leq t$, where the forger F can ask at most q_e Key extract queries, q_s Anony-signcrypt queries and q_d De-signcrypt queries. $(q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}, q_{H_5})$ denote the number of queries to the hash functions H_1, H_2, H_3, H_4, H_5, respectively.

Proof: An instance (P, aP, bP) of the CDH problem is given to simulate the game defined in Definition 5, and F denotes the forger, B denotes challenger. Suppose that F has a non-negligible advantage ε to break the SUF-sMIBSC-CMA model, and B solves the instance of CDH problem by interacting with F. There are five oracles H_1, H_2, H_3, H_4 and H_5 to simulate the system for B. F can queries PPT times to the oracles. B executes and answers each phase of this game as follows:

Setup: The challenger B sets $P_{pub} = bP$ and sends $\langle G_1, G_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4, H_5, E_k, D_k\rangle$ to F as the public parameters. When receiving the parameter, F outputs target multiple identities $(ID_1^*, ID_2^*, \cdots, ID_n^*)$.

Attack: F does several queries to B. These queries are the same as those in Phase 1 of Theorem 4.

Forgery: The forger F outputs a new ciphertext $C = \langle Y, U, X, Z, V, W, a_0, a_1, \cdots, a_{n-1}\rangle$. If the forgery succeeds, the equation $e(W^*, P) = e(X^* + h \cdot \gamma Q_S^*, P_{pub})$ holds. Define $Q_S^* = l_S^* P = aP$, then compute $W^* = (h+\alpha)\gamma D_S^* = (h+\alpha) l_S^* bP = (h+\alpha)abP$. Now, we will easily get the solution of CDH problem: $abP = W^*(\alpha + h)^{-1}$.

Here, we consider the advantage of F's success. For q_s queries to the Anony-signcrypt queries, the probability for B to answer a failure Anony-signcrypt query is less than $q_s/2^k$. So, if the forger F wins the game, B's advantage is $\varepsilon' \geq \varepsilon - q_s/2^k$.

Theorem 6: If an ANON-IND-sMID-CCA attacker A has a non-negligible advantage ε to win the game defined in Definition 6 within running time t, then the Gap-BDH problem can be solved by the challenger B with a non-negligible advantage $\varepsilon' \geq (\varepsilon - q_d/2^l)/nq_{H_2}$, where $(q_\varepsilon, q_d, q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}, q_{H_5})$ denote the number of Key extract queries, De-signcrypt queries, queries to the hash functions H_1, H_2, H_3, H_4, H_5, respectively. And the running time in which the scheme needs to execute is $t' \approx t + (q_\varepsilon + q_{H_1})O(t_1) + (q_{H_2} + q_{H_5})O(t_2) + q_d O(t_1 + t_2) + (q_{H_3} + q_{H_4})O(1)$, where t_1 is the time to perform a scalar multiplication in G_1 and t_2 is the time to perform a pairing e.

Proof: Receiving the instance (P, aP, bP, cP) of the Gap-BDH problem, where $a, b, c \in Z_q^*$ are unknowns, the attacker A can make at most q_g queries to compute $e(P, P)^{abc}$ by playing the game with challenger B as demonstrated in Definition 6. B answers every phase of the ANON-IND-sMID-CCA game in the following way:

Suppose that A outputs the target identities $(ID_1^*, ID_2^*, \cdots, ID_n^*)$ after receiving the params. When obtaining the identities $(ID_1^*, ID_2^*, \cdots, ID_n^*)$, B selects $S = (ID_{\beta_1}, ID_{\beta_2}, \cdots, ID_{\beta_1})$ at random where $S \subset (ID_1, ID_2, \cdots, ID_n)$.

Setup: The challenger B sets $Q = aP$, $P_{pub} = bP$ and sends the $params \equiv \{q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3, H_4, H_5, E_k(), D_k()\}$ to the attacker A. When receiving this query with ID_j, B answers these queries:

***H_1*-query:**

1. If $ID_j \neq ID_i^*, i \in \{1, 2, \cdots, n\}$, calculate $Q_j = l_j P$; otherwise, calculate $Q_j = l_j Q$, where l_j is an integer.
2. Put it into H_1-list when no (ID_j, l_j, Q_j) exists in H_1-list.
3. B returns Q_j.

***H_2*-query:** The challenger B examines if $(P, Q_i, P_{pub}, cP, X_j)$ uses the DBDH oracle for $i \in [1, q_{H_2}]$ when he is queried with $X_j \in G_2$ for some $j = [1, q_{H_2}]$. If it exists, B shall terminate the game for $e(P, P)^{abc}$ equals $(X_j)^{l_i^{-1}}$. Otherwise, B picks a value $x_j \in Z_q^*$ at random and puts a tuple (X_j, x_j) into the list L_2. Then, the challenger B returns x_j to the adversary A.

***H_3*-query:** As an integer p_j is sent to the H_3 oracle where $j \in [1, q_{H_3}]$, B shall pick a string $w_j \in \{0, 1\}^w$ at random and puts the tuple (p_j, w_j) into the list L_3. Then, the string w_j is returned to A by the challenger B.

***H_4*-query:** When querying for the string $\delta_j \in \{0, 1\}^w$ where $j \in [1, q_{H_4}]$, B shall pick a string $z_j \in \{0, 1\}^{|M|}$ at random and puts the tuple (δ_j, z_j) into the list L_4. Then, the challenger B returns the bit string z_j to the attacker A.

***H_5*-query:** Receiving the tuple $\langle X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}}\rangle$ where $j \in [1, q_{H_5}]$, B picks a value $h_j \in Z_q^*$ at random and puts the tuple $\langle X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}}, h_j\rangle$ into the list L_5. Then, B returns h_j.

Phase 1: Challenger B shall answer the Key extract query and De-signcrypt query from attacker A as follows:

Key extract query: A chooses an identity $ID_j \neq ID_i^*$ where $i \in \{1, 2\}$ and sends it to challenger B, then B scans the list L_1 to find if there is the tuple (ID_j, l_j, Q_j) in L_1. If it was, B shall calculate $D_j = l_j P_{pub} (= l_j bP = bQ_j)$. Otherwise, the challenger B selects a $l_j \in Z_q^*$ at random, and calculates $Q_j = l_j P$ as well as $D_j = l_j P_{pub}$. At the same time, the challenger B puts a tuple (ID_j, l_j, Q_j) into the list L_1. Finally, B sends D_j back to the attacker A.

De-signcrypt query: The attacker A queries B and send $B(C_j, ID_i^*)$ where $i \in \{1, 2, \cdots, n\}$ and $C_j = \langle Y_j, U_j, X_j, Z_j, V_j, W_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}}\rangle$ When receiving the decryption query, B executes the following steps:

1. Check the list L_5 to find the tuple $\langle X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}}\rangle$. If it was found, B can get (Z_j, V_j) from L_5. Otherwise, B returns "failure".
2. Construct the polynomial $f(x) = a_{j_0} + a_{j_1} x + \cdots + a_{j_{n-1}} x^{n-1} + x^n$.
3. Searching the tuple (ID_j, l_j, Q_j) in the list L_1.
4. For $l = 1, 2, \cdots, q_{H_2}$, perform as follows:
   a. Search the tuple (X_l, x_l) from the list L_2.
   b. Examine whether $(P, Q_i, P_{pub}, U_j, X_j)$ uses the DBDH oracle by verifying the equation $e(P, P)^{l_j\, b\gamma} = X_j$.
   c. If the step above is true, calculate $p_l = f(x_l)$, $\delta_j' = V_j \bigoplus H_3(p_i)$, and $M_j = D_{H_4}(\delta_j')(Z_j)$.
5. Test whether the equation $e(W_j, P) = e(X_j + h_j Y_j, P_{pub})$ or the equation $e(W_j, Q_i) = e(X_j + h_j Y_j, D_i)$ holds where $h_j = H_5(X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}})$. If it holds, then return M_j to A.
6. Otherwise, B sends "failure" to A, which means that there is not a valid ciphertext generated following the proposed scheme.

Challenge: A sends the plaintext M to B. Then B executes the following steps:

1. Select $\delta \in \{0, 1\}^w$ at random.
2. Set $U = \gamma P = cP$.
3. As $i = 1, 2, \cdots, n$, B shall check the tuples (ID_j, l_j, Q_j) in the list L_1 and compute $v_i = H_2(e(D_i, U))$.
4. Choose $p \in Z_q^*$ at random and structure a polynomial $f(x)$ as follows:

$$\begin{aligned} f(x) &= \prod_{i=1}^{n} (x - v_i) + p(mod\ q) \\ &= a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n. \end{aligned}$$

5. B returns the ciphertext C^* to A.

Phase2: A shall query challenge B like Phase 1 without querying the information of S in the Key extract query and C^* in De-signcrypt query.

Guess: The attacker A gives its guess $\beta' \in \{1, 2, \cdots, n\}$. At the same time, the challenger B picks a tuple (X_j, x_j) at random from the list L_2 where $j \in \beta'$, and chooses the tuple (ID_j, l_j, Q_j) from the list L_1. Finally, B outputs $(X_j)^{l_2^{-1}}$ as the solution to the given instance of the Gap-BDH problem.

Here, we shall discuss the advantage of challenger B. For answering the De-signcrypt query, the challenger B shall check $\langle X_j, U_j, Z_j, V_j, a_{j_0}, a_{j_1}, \cdots, a_{j_{n-1}} \rangle$ in L_5, and send back "failure" if it is not found. That is to say, the right value of H_5 hash function can be guessed by the attacker A. In this case, B may fail at the most probability of q_d/q with q_d queries to the De-signcrypt oracle. In phase Guess, the challenger B shall output the right answer $e(P, P)^{abc}$ at the least probability of $2/nq_{H_2}$, where q_{H_2} is the time of the H_2 hash oracle query, and n is the number of multiple identities. Hence, the Gap-BDH problem can be solved with a non-negligible advantage $\varepsilon' \geq (\varepsilon - q_d/2^l)/nq_{H_2}$, where ε is the non-negligible advantage of attacker A. And the required computation time is $t' \approx t + (q_\varepsilon + q_{H_1})O(t_1) + (q_{H_2} + q_{H_5})O(t_2) + q_d O(t_1 + t_2) + (q_{H_3} + q_{H_4})O(1)$, for answering queries in the simulation game above.

Functional comparison and efficiency analysis

In this section, we will evaluate the functional and efficiency comparison of our scheme with the existing schemes.

Functional comparison

In terms of the funcation, we compare our scheme with some existing schemes in the sender anonymity, receiver anonymity, decryption fairness and public verification, respectively. The comparison is shown in Table 1.

As is shown in Table 1, the schemes [15, 17, 20] cannot protect the sender anonymity. Though the schemes [26–29] can ensure the sender anonymity to some degree, they could suffer from the cross-comparison attack and the joint conspiracy attack for the use of ring signature.

Table 1 shows that the schemes [15, 17, 20, 26–29, 31] cannot reach the receiver anonymity. For the schemes [15, 17, 20, 26–29], the receivers' identities are stored in the ciphertext in the form of plaintext, which can lead to the leakage of receivers' privacy. The scheme [31] also cannot realize the receiver anonymity for the use of the Lagrange interpolation polynomial, each authorized receiver can judge whether anyone else is authorized or not. Meanwhile, the

Table 1. Comparison of the functions.

Schemes	Sender anonymity	Receiver anonymity	Decryption fairness	Public verification
[15]	No	No	No	No
[17]	No	No	No	No
[20]	No	No	No	No
[26]	Yes(*)	No	No	No
[27]	Yes(*)	No	No	No
[28]	Yes(*)	No	No	No
[29]	Yes(*)	No	No	No
[31]	Yes	No	Yes	Yes
[*Proposed*]	Yes	Yes	Yes	Yes

(*) denotes that the scheme could suffer from the cross-comparison attack and the joint conspiracy attack.

doi:10.1371/journal.pone.0166173.t001

schemes [15, 17, 20, 26–29] cannot realize the fair decryption and public verification properties.

As Table 1 shows, our proposed scheme owns these four functions of the sender anonymity, receiver anonymity, decryption fairness, and public verification. The randomized method were used in our scheme, which uses the public key of the sender multiplied by a random value to hide the identity of the sender and avoid the cross-comparison attack and the joint conspiracy attack. In terms of the weakness of the receiver anonymity existed in Lagrange interpolation polynomial, we adopt the new polynomial method which can solve the problem that the authorized receiver can judge the identity of other receivers. So, our scheme simultaneously owns the sender anonymity and the receiver anonymity, which achieves the complete anonymity. In addition, the decryption fairness and public verification properties are also guaranteed in our scheme.

Efficiency analysis

For the efficiency, we compare our scheme with several existing schemes in terms of computation complexity and ciphertext length from two aspects: signcryption and de-signcryption. The comparison is shown in Tables 2 and 3 respectively, where E stands for bilinear pairing operation, A stands for the addition operation in G_1, Mu stands for the scalar multiplication in G_1, Ex stands for the exponentiation in G_2, H stands for hash operation in the encryption step, S stands for symmetric encryption and $Param$ stands for the number of parameters in the ciphertext. In our scheme, the operation of the polynomial can be pre-processed, so these operations are excluded when considering computational complexity.

As is shown in Table 2, we can see that our proposed scheme used one bilinear pairing operation E. Though the bilinear pairing operation has high cost, our scheme controls it within acceptable limits by comparing with others. In terms of hash operation, because of lower cost than other operation, it is within acceptable limits. Encryption algorithm S is used in our scheme, which can be chosen according to practical applications. So, it is easy to reasonably control its communication cost. Meanwhile, our scheme has obvious improvement in operation A, scalar multiplication, exponentiation and ciphertext operation. It can be seen that our scheme has better efficiency in signcryption.

Table 2. Comparison of the signcryption efficiency.

Schemes	*E*	*A*	*Mu*	*Ex*	*H*	*S*	*Param*	Ciphertext length
[15]	1	$n+1$	$n+5$	1	2	0	10	$(n+2)\|G_1\| + \|G_2\| + \|M\| + n\|ID\|$
[17]	2	$n+1$	$n+4$	2	2	1	8	$(n+2)\|G_1\| + \|M\| + n\|ID\| + \|Z_q\|$
[20]	0	$n+1$	$n+3$	1	2	0	$n+9$	$3\|G_1\| + \|M\| + n\|ID\|$
[26]	0	$3m+n-2$	$2m+n+2$	1	$m+2$	0	11	$(m+n+2)\|G_1\| + \|M\| + (m+n)\|ID\|$
[27]	1	$2m-3$	$2m+2$	0	$m+2$	0	10	$2\|G_1\| + m\|G_2\| + 2\|M\| + m\|Z_q\|$
[28]	1	$4m-2$	$4m$	0	$m+2$	0	10	$(m+2)\|G_1\| + \|M\|$
[29]	0	$3m+n-2$	$2m+n+2$	1	$m+2$	0	11	$(m+n+2)\|G_1\| + \|M\| + (m+n)\|ID\|$
[31]	1	2	6	1	2	0	10	$(n+4)\|G_1\| + \|M\|$
[*Proposed*]	1	0	5	0	$n+3$	1	13	$4\|G_1\| + \|M\| + w + nZ_q$

$|G_1|$: the length of the elements in G_1; $|Z_q|$: the length of the elements in Z_q;
$|ID|$: the length of identity information; $|M|$: the length of the plaintext M;
m: the number of senders; n: the number of receivers; w: the bit length of a string

doi:10.1371/journal.pone.0166173.t002

Table 3. Comparison of the signcryption efficiency.

Schemes	Public verification	Judgment	Decryption
[15]	$3E+2A+3Mu+3H$	$3E+2A+3Mu+3H$	$3E+2A+3Mu+3H$
[17]	$2E+Ex+Mu+2H$	$2E+Ex+Mu+2H$	$4E+2T_a+Ex+3H+T_s$
[20]	$3E+2A+(3n+3)Mu+2Ex+(n+1)H$	$3E+2A+(3n+3)Mu+2Ex+(n+1)H$	$3E+2A+(3n+3)Mu+2Ex+(n+1)H$
[25]	$2E+A+Mu+H$	$2E+A+Mu+H$	$2E+nA+(n-1)Mu+2H$
[26]	$2E+(2m-1)T_a+Mu+mH$	$4E+2mA+(m+1)Mu+(m+1)H$	$4E+2mA+(m+1)Mu+(m+1)H$
[27]	$3E+(m+1)T_a+2mMu+(m+2)H$	*N/A*	$3E+(m+1)T_a+2mMu+(m+2)H$
[28]	$4E+2mT_a+mT_m+(m+2)H$	*N/A*	$4E+2mT_a+mMu+(m+2)H$
[29]	$(M+5)E+A+(m+\|M\|+2)Mu+2H$	$(M+5)E+A+(m+\|M\|+2)Mu+2H$	$(M+5)E+A+(m+\|M\|+2)Mu+2H$
[31]	$2E+A+Mu+H$	$2E+A+Mu+H$	$2E+nA+(n-1)Mu+2H$
[*Proposed*]	$2E+A+Mu+H$	$2E+A+Mu+H$	$E+S+3H$

$|M|$: the length of the plaintext M;
m: the number of senders; n: the number of receivers.

doi:10.1371/journal.pone.0166173.t003

On the other hand, in the de-signcryption process, there are generally three algorithms affecting the efficiency: public verification, judgment, and decryption. We will compare the proposed scheme with the existing schemes about these three algorithms, respectively.

As shown in Table 3, our scheme and sheme [31] have obviously higer efficiency in public verification and authorization judgement comparing with the other schemes [15, 17, 20, 26–29], where N/A indicates that the scheme only considered the single receiver environment, which is tansfered via unicast channel. In this case, it is unnecessary to judge whether the receiver is authorized or not. Meanwhile, our scheme has higher efficiency than others in decryption.

From the above analysis, though our scheme has unobvious improvement on the efficiency in general, it owns the complete anonymity containing the sender and receiver anonymity, which is an excellent contribution we think. In our scheme, any receiver can only judge whether the ciphertext is from a reliable sender or not, rather than actually getting the real identity of the sender. Attackers not only outside the system but also inside the system can be prevented in our new scheme.

Besides the above theoretical analysis on efficiency, we shall also give some experiment results to compare our scheme with the existing ones more intuitively. Like the work [35–37], we shall also pay attention to those time-consuming operations and overlook the other ones that do not consume much time. We define the following notations in Table 4, and borrow the experiment testing results from [35–37].

Then, with the results in Table 4, the efficiency comparison of our scheme with the existing ones can be shown by Tables 5 and 6.

Table 4. Notation and definition of diffident time complexities.

Notations	Definition and conversion
T_M	Time required for executing a modular multiplication operation.
T_E	Time required for executing a bilinear pairing operation, $T_E \approx 87T_M$.
T_A	Time required for executing a point addition of two points in G_1, $T_A \approx 0.12T_M$.
T_{Mul}	Time required for executing a scalar multiplication in G_1, $T_{Mul} \approx 29T_M$.
T_{Exp}	Time required for executing a exponentiation in G_2, $T_{Exp} \approx 43.5T_M$.
T_H	Time required for executing a hash operation, $T_H \approx 29T_m$.

doi:10.1371/journal.pone.0166173.t004

Table 5. Time complexity comparison of signcryption.

Schemes	Time complexity of signcryption
[15]	$(29.12n + 333.62)T_M$
[17]	$(29.12n + 435.62)T_M$
[20]	$(29.12n + 188.62)T_M$
[26]	$(87.36m + 29.12n + 159.26)T_M$
[27]	$(87.24m + 192.64)T_M$
[28]	$(145.48m + 144.76)T_M$
[29]	$(87.36m + 29.12n + 159.26)T_M$
[31]	$362.74T_M$
Proposed	$(29n + 319)T_M$

doi:10.1371/journal.pone.0166173.t005

Table 6. Time complexity comparison of de-signcryption.

Schemes	Public verification	Judgment	Decryption
[15]	$435.24T_M$	$435.24T_M$	$435.24T_M$
[17]	$304.5T_M$	$304.5T_M$	$478.14T_M$
[20]	$(116n + 464.24)T_M$	$(116n + 464.24)T_M$	$(116n + 464.24)T_M$
[26]	$(58.24m + 173.88)T_M$	$(58.24m + 406)T_M$	$(58.24m + 406)T_M$
[27]	$(87.12m + 319.12)T_M$	N/A	$(87.12m + 319.12)T_M$
[28]	$(58.24m + 406)T_M$	N/A	$(58.24m + 406)T_M$
[29]	$(116m + \|M\|m + 117.12)T_M$	$(116m + \|M\|m + 117.12)T_M$	$(116m + \|M\|m + 117.12)T_M$
[31]	$232.12T_M$	$232.12T_M$	$(29.12n + 203)T_M$
Proposed	$232.12T_M$	$232.12T_M$	$174T_M$

$|M|$: the length of the plaintext M; m: the number of senders; n: the number of receivers.

doi:10.1371/journal.pone.0166173.t006

Tables 5 and 6 also show the relative high efficiency of our scheme when compared with the exiting schemes with the same functions.

Conclusion

A novel multi-receiver signcryption scheme with complete anonymity is proposed in this paper. By using a new polynomial technology, our scheme actually achieves the receiver anonymity. Attackers not only outside the system but also inside the system can be prevented in our new scheme. Meanwhile, in the process of signcryption, the sender used the randomized method to hide its public key, which ensures the sender anonymity. So, our scheme simultaneously owns the sender anonymity and the receiver anonymity, which achieves the complete anonymity. In addition, the decryption fairness and public verification properties are guaranteed in our scheme. This new scheme can be applied better to secure broadcast, network meeting, paying-TV and data sharing on the cloud.

Author Contributions

Conceptualization: LP HL.

Data curation: XY.

Formal analysis: LP XY HZ YH HL.

Funding acquisition: LP HL.

Investigation: XY HZ YH.

Methodology: LP XY YH HL.

Project administration: LP.

Resources: LP.

Software: XY.

Supervision: LP.

Validation: LP XY HL.

Visualization: YH.

Writing – original draft: LP XY YH.

Writing – review & editing: LP XY YH.

References

1. Bellare M, Boldyreva A, Micali S. Public-key encryption in a multi-user setting: security proofs and improvements [C]. Eurocrypt 2000, Springer-Verlag, LNCS 1807, pp. 259–274. doi: 10.1007/3-540-45539-6_18
2. Kurosawa K. Multi-recipient public-key encryption with shortened ciphertext [C]. PKC 2002, Springer-Verlag, LNCS 2274, pp. 48–63.
3. Bellare M, Boldyreva A, Staddon J. Multi-recipient encryption schemes: security notions and randomness re-use [C]. PKC 2003, Springer-Verlag, LNCS 2567, pp. 85–99.
4. Baek J, Safavi-Naini R, Susilo W. Efficient multi-receiver identity-based encryption and its application to broadcast encryption [C]. PKC 2005, Springer-Verlag, LNCS 3386, pp. 380–397. doi: 10.1007/978-3-540-30580-4_26
5. Chatterjee S, Sarkar P. Multi-receiver identity-based key encapsulation with shortened ciphertext. In Proceedings of INDOCRYPT 2006, LNCS 4329, pp: 394–408.
6. Ming Y, Shen X. Multi-receiver Identity-Based Key Encapsulation in the Standard Model[C].. Information Science and Management Engineering (ISME), 2010 International Conference of. IEEE, pp: 382–385.
7. Park JH, Kim KT, Lee DH. Cryptanalysis and improvement of a multi-receiver identity-based key encapsulation at INDOCRYPT'06. In Proceedings of ASIACCS'08, 2008, pp: 373–380.
8. Qin L, Cao Z, Dong X. Multi-receiver identity-based encryption in multiple PKG environment[C]. 2008 IEEE Global Telecommunications Conference. 2008.
9. Li F, Khan M, Alghathbar K, Takagi T. Identity-based online/offline signcryption for low power devices. Journal of Network and Computer Applications, 2012, 35(1): 340–347. doi: 10.1016/j.jnca.2011.08.001
10. Li F, Fahad M, Khan M, Takagi T. Lattice-based Signcryption. Concurrency and Computation: Practice and Experience, 2013, 25(14): 2112–2122. doi: 10.1002/cpe.2826
11. Li F, Khan M. A Biometric Identity-based Signcryption Scheme. Future Generation Computer Systems, 2012, 28(1): 306–310. doi: 10.1016/j.future.2010.11.004
12. Li F, Khan M. A Survey of Identity-Based Signcryption. IETE Technical Review, 2011, 28(3): 265–272. doi: 10.4103/0256-4602.81236
13. Duan S, Cao Z. Efficient and provably secure multi-receiver identity-based signcryption [C]. ACISP 2006, Springer-Verlag, LNCS 4058, pp. 195–206. doi: 10.1007/11780656_17
14. Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost (encryption) [C]. In Advances in Cryptology-CRYPTO'97, 1997, Spring-Verlag, LNCS 1294, pp. 165–179. doi: 10.1007/BFb0052234
15. Yu Y, Yang B, Huang X, et al. Efficient identity-based signcryption scheme for multiple receivers [C]. ATC 2007, Springer-Verlag, LNCS 4610, pp. 13–21. doi: 10.1007/978-3-540-73547-2_4

16. Yang X, Li M, Wei L, et al. New ECDSA-verifiable multi-receiver generalization signcryption [C]. High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on. IEEE, pp. 1042–1047.
17. Elkamchouchi H, Abouelseoud Y. MIDSCYK: an efficient provably secure multi-recipient identity-based signcryption scheme [J]. ICNM 2009, pp. 70–75.
18. Li F, Xiong H, Nie X. A new multi-receiver ID-based signcryption scheme for group communications[C]. Communications, Circuits and Systems, 2009. ICCCAS 2009. International Conference on. IEEE, 2009: 296–300.
19. Li F, Hu Y, Liu Sh. Efficient and provably secure multi-recipient signcryption from bilinear pairings [J]. Wuhan University Journal of Natural Sciences, 2007, 12(1): 17–20. doi: 10.1007/s11859-006-0133-y
20. Selvi S, Vivek S, Srinivasan R. An efficient identity-based signcryption scheme for multiple receivers [C]. PKC IWSEC 2009, Springer-Verlag, LNCS 5824, pp. 71–88. doi: 10.1007/978-3-642-04846-3_6
21. Li Z, Xu X, Li C. Multi-recipient signcryption algorithm for communication of mobile Ad Hoc networks [C]. NCIS 2012, Springer-Verlag, pp. 388–394. doi: 10.1007/978-3-642-35211-9_51
22. Fan C, Huang L, Ho P. Anonymous multi-receiver identity-based encryption [J]. IEEE Transactions on Computers, 2010, 59(9): 1239–1249. doi: 10.1109/TC.2010.23
23. Pang L, Li H, Wang Y. nMIBAS: A novel multi-receiver ID-based anonymous signcryption with decryption fairness [J]. Computing and Informatics, 2013, 32 (3): 441–460.
24. Khullar S, Richhariya Vivek, Richhariya Vineet. An efficient identity based multi-receiver signcryption scheme using ECC [J]. IJACT 2013, 2(4): 189–193.
25. Pang L, Gao L, Li H, et al. Anonymous multi-receiver ID-based signcryption scheme [J]. IET Information Security, 2015, 9(3): 194–201. doi: 10.1049/iet-ifs.2014.0360
26. Lal S, Kushwah P. Anonymous ID based signcryption scheme for multiple receivers [J]. IACR Cryptology ePrint Archive, 2009, pp. 345–354.
27. Huang X, Susilo W, Mu Y, et al. Identity based ring signcryption scheme: cryptographic primitive for preserving privacy and authenticity in the ubiquitous world [J]. AINA 2005, pp. 649–654.
28. Zhang J, Gao S, Chen H, et al. A novel ID-based anonymous signcryption scheme [C]. Proceedings of the Advances in Data and Web Management Joint International Conferences. Suzhou, China, 2009, pp. 604–610.
29. Zhang B, Xu Q. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model [C]. AST/UCMA/ISA/ACN. Springer-Verlag, LNCS 6059. 2010, pp. 15–27. doi: 10.1007/978-3-642-13577-4_2
30. Qin H, Dai Y, Wang Z. Identity-based multi-receiver threshold signcryption scheme [J]. Security and Communication Networks, 2011, 4(11):1331–1337. doi: 10.1002/sec.259
31. Pang L, Li H, Gao L, Wang Y. Completely anonymous multi-recipient signcryption scheme with public verification [J]. PLoS ONE, 2013, 8(5): e63562. doi: 10.1371/journal.pone.0063562 PMID: 23675490
32. Wang H, Zhang Y, Xiong H, et al. Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme [J]. IET Information Security, 2012, 6(1): 20–27. doi: 10.1049/iet-ifs.2010.0252
33. Zhang J, Xu Y. Comment on anonymous multi-receiver Identity-based encryption scheme [J]. INCoS 2012, pp. 473–476.
34. Li H, Pang L. Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme [J]. IET Information Security, 2014, 8(1): 8–11. doi: 10.1049/iet-ifs.2012.0354
35. Islam S, Biswas G. Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography [J]. International Journal of Computer Mathematics, 2013, 90(11): 2244–2258. doi: 10.1080/00207160.2013.776674
36. Islam S, Biswas G. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks [J]. Annals of télécommunications-annales des telecommunications, 2012, 67 (11-12): 547–558. doi: 10.1007/s12243-012-0296-9
37. Cao X, Kou W, Du X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges[J]. Information Sciences, 2010, 180(15): 2895–2903. doi: 10.1016/j.ins.2010.04.002