Heterogeneous hybrid signcryption for multi-message and multi-receiver

Shufen Niu*, Ling Niu, Xiyuan Yang, Caifen Wang, Xiangdong Jia

College of Computer Science and Engineering, Northwest Normal University, Lanzhou, Gansu, China

* sfniu76@nwnu.edu.cn

Abstract

To achieve secure communication in heterogeneous cryptography systems, we present a heterogeneous hybrid signcryption scheme. The proposed scheme allows a sender in an identity-based cryptography system to send multi-message to multi-receiver in a certificateless cryptography system with different master keys. At the same time, all users are mapped to a distinct pseudo-identity for conditional identity privacy preservation. A trusted authority could trace the real identity when necessary. Compared with existing schemes, the proposed scheme is more practical for actual applications. In addition, the proposed scheme has indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen message attacks under the random oracle model.

Introduction

Diverse network systems have appeared with the development of technology. These systems utilize different cryptography techniques, such as public key infrastructure (PKI), identity-based cryptography (IBC), and certificateless cryptography (CLC). A cryptographic scheme should be constructed for secure communication in heterogeneous systems. Zheng [1] firstly proposed signcryption, a novel cryptographic primitive that functions as both digital signature and public key encryption in a single logical step that significantly costs lower than the traditional signature-then-encryption approach. Signcryption schemes are used to simultaneously achieve confidentiality, integrity, authentication, and non-repudiation for resource-constrained devices over low-bandwidth communication channels. Given those advantageous characteristics, heterogeneous signcryption is investigated. There are two types of heterogeneous signcryption between PKI and IBC: in type I, a sender in the PKI setting transmits a message to a receiver in the IBC setting; in type II, a sender in the IBC setting transmits a message to a receiver in the PKI setting. To achieve secure communication, Sun et al. [2] proposed type I schemes; these schemes, however, can only achieve outsider security. In 2011, Huang et al. [3] proposed a type II signcryption scheme with internal security. In 2013, Li et al. [4] proposed types I and II schemes that meet internal security requirements. Related heterogeneous signcryption paradigms have received considerable attention in recent years [5–8].

It is a practical way for large messages to use hybrid encryption perform secure communication. Hybrid encryption separates encryption into two parts: one part uses public key
techniques to encrypt a one-time symmetric key, and the other part uses the symmetric key to encrypt the actual message. The public key encryption part of the algorithm is the key encapsulation mechanism (KEM), whereas the symmetric key encryption part is the data encapsulation mechanism (DEM). In 2003, a formal treatment of this paradigm originated in the work of Cramer and Shoup [9]. Dent [10, 11] studied the use of hybrid techniques to build signcryption schemes. He generalized KEM to signcryption KEM, which includes authentication. However, he only considered insider security for authenticity. In 2008, Tan [12] proposed full insider secure signcryption KEM in the standard model. Tan’s schemes are insider-secure for both authenticity and confidentiality. In 2005, Smart [13] provided an efficient key encapsulation for multiple parties. Sun et al. [14] proposed an IBC signcryption KEM for multiple recipients. Related hybrid signcryption or hybrid multiple receivers signcryption schemes can be found in [15–18].

Considering all the above literature, it is known that none of the existing multi-recipient heterogeneous hybrid signcryption schemes for IBC to CLC. However, in today’s complex network and application environment, the information security situation is also complicated and grim. The production and collection of the mass data results in information explosion lead the network communication become more complex and low effective due to diverse system [19, 20] and mathematical models [21, 22] of equipment environment. Then there need a scheme to achieve better communication between user with strong computing power and user who has weak computing power in heterogeneous system, the scheme also should handle large messages for sender to improve the efficiency of signcryption to multi-receiver.

Motivated by the above, considering with multi-PKG signcryption [23] and conditional privacy-preserving schemes [24], we propose a heterogeneous hybrid signcryption scheme for IBC to CLC which meets: (1) The private key generator (PKG) and key generation center (KGC) can produce different master keys and system parameters for different cryptography environments, which are more practical for heterogeneous systems. (2) The scheme is insider-secure for both authenticity and confidentiality, and the formal definitions and security models for heterogeneous hybrid signcryption scheme are also given. (3) Each user maps a distinct pseudo-identity to achieve conditional identity privacy preservation. A trusted authority could trace the real identity when necessary. (4) Use hybrid signcryption to implement a sender signcrypt multi-message to multi-receiver in once signcryption.

The rest of this paper is organized as follows: preliminary information is given in section 2. The framework and security model are presented in section 3. The heterogeneous hybrid signcryption for multi-message and multi-receiver (MHHSC) scheme is proposed in section 4. The security proof is presented in section 5. The performance evaluation of the proposed scheme is discussed in section 6. Finally, the conclusion is provided in section 7.

Preliminary

In this section, we describe bilinear maps and hard problems. Let consider two cyclic groups $G_1$ and $G_2$ with the same prime order $q$, and let $P$ is a generator of $G_1$. A bilinear map $e: G_1 \times G_1 \rightarrow G_2$ need satisfy the following properties:

1. Bilinearity: For all $P, Q, R \in G_1$, and $a, b \in \mathbb{Z}_q^*$, $e(P + R, Q) = e(P, Q)e(R, Q)$. Also $e(aP, bQ) = e(P, Q)^{ab}$.
2. Non-degeneracy: There exists $P, Q \in G_1$, such that $e(P, Q) \neq 1$.
3. Computability: $e(P, Q)$ can be computed for $P, Q \in G_1$. 

Preliminary information is given in section 2. The framework and security model are presented in section 3. The heterogeneous hybrid signcryption for multi-message and multi-receiver (MHHSC) scheme is proposed in section 4. The security proof is presented in section 5. The performance evaluation of the proposed scheme is discussed in section 6. Finally, the conclusion is provided in section 7.
Definition 1. Given two groups $G_1$ and $G_2$ of the same prime order $q$, a bilinear map $e: G_1 \times G_1 \rightarrow G_2$, and a generator $P$ of $G_1$, the decisional bilinear Diffie-Hellman (DBDH) problem is to decide whether $T = e(P, P)^{abc}$ for given $(P, aP, bP, cP)$ and $T \in G_2$.

Definition 2. Variants decisional bilinear Diffie-Hellman (VDBDH) problem is to decide whether $T = e(P, P)^{abc - 1}$ for given $(P, aP, bP, cP, c^{-1}P)$ and $T \in G_2$.

Definition 3. Variants computational bilinear Diffie-Hellman (VCBDH) problem is to compute $T = e(P, P)^{abd - 1}$ for given $(P, aP, bP, dP, d^{-1}P)$.

Framework and security model for MHHSC

MHHSC KEM

MHHSC KEM consists of five algorithms:

- **Setup**: With a security parameter $\ell$ as the input, the PKG and KGC generate their own master key and output the system parameters $params$.

- **Anony-IBC-KG**: The algorithm runs by the PKG of the IBC system. With a user’s real identity $RID_A$ and $ID_{A,i}$ as the input, the algorithm generates the corresponding private key $sk_A$ and pseudo-identity $ID_A$.

- **Anony-CLC-KG**: The algorithm runs by the KGC of the CLC system. With a user’s real identity $RID_B$ and $ID_{B,i}$ as the input, the algorithm generates the corresponding partial private key $D_{B,i}$, secret key $sk_{B,i}$, public key $pk_{B,i}$ and pseudo-identity $ID_{B,i}$.

- **Encap**: Give the sender’s identity $(Q_A, ID_A)$, and private key $sk_A$, receiver identity $(pk_{B_i}, ID_{B,i}, Q_{B_i}(i = 1, 2, \cdots, n))$, the algorithm outputs the encapsulation key $K$ and encapsulation $\varphi$.

- **Decap**: Give the sender’s identity $(Q_A, ID_A)$, receiver secret key, and public key $(D_{B,i}, sk_{B,i})$, $(pk_{B_i}, ID_{B,i})$, the algorithm outputs the encapsulation key $K$ or the symbol $\perp$.

DEM

DEM is a symmetric encryption scheme that requires security for confidentiality and unforgeability. DEM consists of the following two algorithms:

- **Enc**: Take message $M$ and encapsulation key $K$ as input, the ciphertext $C$ is then output. We denote this as $C \leftarrow DEM.Enc(K, M)$.

- **Dec**: Take a key $K$ and the ciphertext $C$ as input, the message $M$ or error symbol $\perp$ is output.

MHHSC HSC

The proposed MHHSC scheme consists of MHHSC KEM and DEM as follows:

- **Setup, Anony-IBC-KG, and Anony-CLC-KG**: Same as 3.1 MHHSC KEM.

- **Signcrypt**: Use Encap in 3.1 MHHSC KEM to obtain $(K, \varphi)$, use Enc in 3.2 DEM to obtain a ciphertext $C$, output $\sigma \leftarrow (C, \varphi)$.

- **Unsigncrypt**: Use Decap in 3.1 MHHSC KEM to obtain $K$, use Dec in 3.2 DEM to obtain message $M$, then check the equation. If it holds, receive $M$. Otherwise, output the symbol $\perp$. 


Security notions

In the proposed scheme, the confidentiality property is defined based on the concept of indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2), which considers two types of adversaries with different capabilities. A type I adversary acts as a dishonest user, whereas a type II adversary acts as a malicious KGC that can obtain the master secret key of KGC. The authenticity property is defined based on existential unforgeability against adaptive chosen message attacks (EUF-CMA).

Definition 4. (Confidentiality) A heterogeneous hybrid signcryption scheme is said achieved IND-CCA2, if no probabilistic polynomial time adversary \( A_1 \) has a non-negligible advantage in the following game:

**Setup:** The challenger \( C \) runs the Setup algorithm and sends system parameters and public keys to \( A_1 \), whereas the KGC’s master key is kept secret. \( ID_{B_i}^b(i = 1, 2, \cdots, n) \) is the target identity.

**Phase 1.** \( A_1 \) can ask several kinds of queries to the following random oracles:

- **Partial private key query:** Submit a query on \( ID_{B_i} \). If \( ID_{B_i} \neq ID_{B_i}^b(i = 1, 2, \cdots, n) \), then return \( D_{B_i} \). Otherwise, \( C \) aborts.

- **Unsigncrypt query:** Submit an unsigncrypt query under \( ID_{A_i}, ID_{B_i} \) and ciphertext \( \sigma \). If \( ID_{B_i} \neq ID_{B_i}^b(i = 1, 2, \cdots, n) \), then \( C \) runs the formal unsigncrypt algorithm and returns the answer. Otherwise, \( C \) searches the list and computes \( M \). Then, check the equation. If holds, \( M \) is returned. Otherwise, \( \bot \) is output.

**Challenge:** \( C \) decides when the Phase 1 ends. \( A_1 \) selects two plaintexts \( M_0, M_1 \) of the same length, and \( ID_{A_i}, ID_{B_i}(i = 1, 2, \cdots, n) \) to \( C \), which wants to challenge. If \( ID_{B_i} \neq ID_{B_i}^b(i = 1, 2, \cdots, n) \), \( C \) fails and aborts. \( A_1 \) is not allowed to query the partial private key of \( ID_{B_i}^b \). Then, \( C \) selects \( b \in \{0, 1\} \) and runs the corresponding algorithms to obtain the ciphertext \( \sigma \) transmits to \( A_1 \).

**Phase 2.** \( A_1 \) can perform queries as in Phase 1. \( A_1 \) cannot query the key extraction for the target identities and should not query the unsigncrypt of \( \sigma' \).

**Guess:** Finally, \( A_1 \) produces a bit \( b' \), \( A_1 \) wins the game if \( b' = b \).

Definition 5. (Confidentiality) A heterogeneous hybrid signcryption scheme is said achieved IND-CCA2, if no probabilistic polynomial time adversary \( A_2 \) has a non-negligible advantage in the following game:

**Setup:** The challenger \( C \) runs the Setup algorithm that sends system parameters and public keys to \( A_2 \). \( ID_{B_i}^b(i = 1, 2, \cdots, n) \) is the target identity.

**Phase 1.** \( A_2 \) can ask several queries to the following random oracles:

- **Public key query:** Submit a public key query on \( ID_{B_i} \). If \( ID_{B_i} \neq ID_{B_i}^b(i = 1, 2, \cdots, n) \), update PK-list with \( (ID_{B_i}, \bot, cP) \), and return \( pk_{B_i} \).

- **Unsigncrypt query:** Submit an unsigncrypt query under \( ID_{A_i}, ID_{B_i} \) and ciphertext \( \sigma \). If \( ID_{B_i} \neq ID_{B_i}^b(i = 1, 2, \cdots, n) \), \( C \) runs the formal unsigncrypt algorithm and returns the answer. Otherwise, \( C \) searches the list and computes \( M \). Then, check the equation. If the equation holds, return \( M \). Otherwise, \( \bot \) is output.

**Challenge:** \( C \) decides when Phase 1 ends. \( A_2 \) selects two plaintexts \( m_0, m_1 \) of the same length, and \( ID_{A_i}, ID_{B_i}(i = 1, 2, \cdots, n) \) to \( C \), which wants to challenge. If \( ID_{B_i} \neq ID_{B_i}^b(i = 1, 2, \cdots, n) \), \( C \) fails and aborts. \( A_2 \) is not allowed to query for the secret key of
Heterogeneous hybrid signcryption

The MHHSC scheme will be discussed in this section. The proposed scheme involves four parties: PKG, KGC, sender \( ID_A \), and \( n \) receivers \( \{ ID_B \}_{i=1}^n \), allowing \( ID_A \) to send \( m \) messages to \( n \) receivers \( \{ ID_B \}_{i=1}^n \). KDF in scheme denotes a key extract function in \( G_1 \). Moreover, PKG and KGC can calculate pseudo-identities for users in their system, key pairs or partial private keys of all users are generated by PKG or KGC via the pseudo-identities.

- **Setup**: Let \( G_1 \) and \( G_2 \) be two cyclic groups with prime order \( q \), where \( G_1 \) is additive and \( G_2 \) is multiplicative, and \( P \) is the generator of \( G_1 \). Let \( e: G_1 \times G_1 \rightarrow G_2 \) be an admissible bilinear map, a key extract function \( KDF: \{ 0, 1 \}^{l_m} \rightarrow G_1 \) (\( l_m \) is the length of a key).

1. PKG randomly selects \( s_1 \in Z_q^* \) and two hash functions: \( H_0: G_1 \rightarrow \{ 0, 1 \}^*, H_1: \{ 0, 1 \}^* \rightarrow G_1 \) computes \( P_1 = s_1 P \), where \( s_1 \) is a master secret key that only the PKG knows.
2. KGC randomly selects \( s_2 \in Z_q^* \) and four hash functions: \( H_2: G_1 \rightarrow \{ 0, 1 \}^*, H_3: \{ 0, 1 \}^* \rightarrow G_1, H_4 : G_2 \rightarrow Z_q^*, H_5 : \{ 0, 1 \}^* \rightarrow Z_q^* \) calculates \( P_2 = s_2 P \), where \( s_2 \) is a master secret key that only the KGC known.

Public params = \( <e, P, P_1, P_2, G_1, G_2, H_0, H_1, H_2, H_3, H_4, H_5, KDF> \) and keep \( s_1, s_2 \) secret respectively.

- **Anony-IBC-KG**: Users in IBC obtain their private key as follows:

1. Sender \( A \) randomly selects \( k_A \in Z_q^* \) calculates \( ID_{A, 1} = k_A P \) and transmits \( (RID_A, ID_{A, 1}) \) to PKG, where \( RID_A \) is the real identity of sender \( A \). PKG calculates \( ID_{A, 2} = RID_A \oplus H_0(s_1, ID_{A, 1}, T) \), where \( T \) denotes the valid period of this pseudo-identity. Finally, the identity on sender \( A \) is \( ID_A = (ID_{A, 1}, ID_{A, 2}, T) \).
PKG generates a private key for IBC users as $sk_A = s_A^{-1} Q_A$, where $Q_A = H_1(ID_A)$. $(sk_A, Q_A, ID_A)$ is sent to $A$ via a secure path.

- **Anony-CLC-KG:** Users in CLC obtain their partial private key as follows:
  1. Receiver $B_i(i \in \{1, 2, \cdots, n\})$ randomly selects $k_{Bi} \in Z_q^*$ calculates $ID_{B,i} = k_{Bi} P$ and transmits $(RID_{Bi}, ID_{B,i})$ to KGC, where $RID_{Bi}$ is the real identity of receiver $B_i$. KGC calculates $ID_{B,i} = RID_{Bi} \oplus H_2(s_{ID_{Bi}}, T_i)$, where $T_i$ denotes the valid period of this pseudo-identity. Finally, the identity of receiver $B_i$ is $ID_{Bi} = (ID_{B,i}, ID_{B,i}, T_i)$.
  2. KGC generates the partial private key for CLC users as $ID_{Bi} = s_{ID_{Bi}}^{-1} Q_{Bi}$, where $Q_{Bi} = H_3(ID_{Bi})$. $(ID_{Bi}, Q_{Bi}, ID_{Bi})$ is sent to $B_i$ via a secure path.
  3. $B_i$ randomly selects the secret value $x_{Bi} \in Z_q^*$ to compute $sk_{Bi} = x_{Bi} D_{Bi}, pk_{Bi} = x_{Bi} P$.

- **Signcrypt:** A sender $A$ signcrypts $n$ messages $m_i (i = 1, 2, \cdots, n)$ to $n$ receiver $B_i(i = 1, 2, \cdots, n)$ as follows:
  1. Randomly selects $r_1, r_2 \in Z_q^*$, and computes $U_1 = r_1 P_2, U_2 = r_1 Q_A$.
  2. Compute $V_i = e(P, Q_{Bi})^{r_1}, R_i = e(pk_{Bi}, Q_{Bi})^{r_2}, \phi_i = r_2 \oplus H_4(V_i)$ and let $\phi = (\phi_1, \phi_2, \cdots, \phi_n)$.
  3. Compute $C = DEM.Enc(K, M)$ where $K = KDF(r_2)$ and $M = (m_1 \oplus R_1, m_2 \oplus R_2, \cdots, m_n \oplus R_n)$.
  4. Compute $h_1 = H_5(U_1, U_2, M, R_n, V_n, ID_A, ID_B)$.
  5. Compute $S_i = (r_1 + h_i) sk_A$ and let $S = (S_1, S_2, \cdots, S_n)$. Return ciphertext $\sigma = (C, \phi \leftarrow (U_1, U_2, S, \phi))$.

- **Unsigncrypt:** After receiving a ciphertext $\sigma = (C, \phi \leftarrow (U_1, U_2, S, \phi))$, the receiver $B_i(i \in \{1, 2, \cdots, n\})$ decrypts $\sigma$ as follows:
  1. Compute $V_i = e(U_1, D_{Bi}), R_i = e(U_1, sk_{Bi})$ and obtain $r_2 = \phi_i \oplus H_4(V_i)$.
  2. Recover $M = DEM.Dec(K, C)$ where $K = KDF(r_2)$. Receiver $B_i$ recovers own message $m_i = (m_1 \oplus R_1) \oplus R_i$.
  3. Compute $h_1 = H_5(U_1, U_2, M, R_n, V_n, ID_A, ID_B)$.
  4. Accept the message if and only if the following equation holds:
    $$e(P_1, S_i) = e(P, U_2 + h_i Q_A).$$

Note that conditional privacy preservation for each user is mapped to a distinct pseudo-identity $ID_U = (ID_{U,1}, ID_{U,2}, T)$. PKG or KGC can retrieve the real identity from any pseudo-identity by $RID_U = ID_{U,2} \oplus H_1(sID_{U,1}, T)$ for any disputed event. In addition, the pseudo-identity $ID_U$ is generated by both users and PKG or KGC. Hence, only the PKG or KGC that knows the master secret $s$ can retrieve the real identity $RID_U$ from $ID_U$.

**Security proof**

In this section, we prove that the proposed IBC to CLC hybrid scheme achieves the security requirements of confidentiality and unforgeability. To demonstrate the security of our scheme, we assume that the adversary asks $q_H$ queries to $H_i$ for $i = 1, 2, 3, 4, 5, q_u$ queries to
unsigncryption; \( q_s \) queries to the signcryption; \( q_{pk} \) queries to the partial private key; \( q_{sk} \) queries to the secret key; \( q_{pk} \) queries to the public key extraction; and \( q_{pkv} \) queries to the public key replacement.

**Confidentiality**

Theorem 1. The above MHHSC scheme is secure against adaptive chosen ciphertext attacks in the standard model assuming that the VDBDH and DBDH problems are difficult.

This theorem follows lemmas 1 and 2. Lemma 1 reveals that adversary \( A_1 \) cannot distinguish \( M \). Lemma 2 proves that although adversary \( A_2 \) can obtain \( M \), it cannot distinguish message \( m_i \) for \( ID_B \).

Lemma 1. In the random oracle, if there is an IND-CCA2 adversary \( A_1 \) has an advantage \( \epsilon \) against MHHSC, then there is an algorithm \( C \) that solves the VDBDH problem with an advantage \( e^{-(q_s^3 - q_{pk}^3 - q_{pkv})^2/q^2} \).

**Proof.** We construct a simulator \( C \) that use \( A_1 \) to decide whether \( T = e(P, P)^{abc^{-1}} \) by providing a random instance \((P, aP, bP, cP, c^{-1} P, T)\) as the VDBDH problem. This proof consider the indistinguishability of \( M \).

**Setup**: At the beginning, \( C \) sets \( P_2 = cP \) and proves the system parameters to the attacker \( A_1 \). The target identity is \( ID_B^i \) \((i = 1, 2, \ldots, n)\).

**Phase 1**. \( A_1 \) requests a number of queries. \( C \) keeps the \( H_i \)-list \((i = 1, 2, 3, 4, 5) \) and \( PK \)-list which are used to record answers to the corresponding \( H_i \) query and public key query.

- **H_3 query**: Input an identity ID_{B_j} if ID_{B_j} \( \neq ID_{B_j}^i \) \((i = 1, 2, \ldots, n)\), randomly select \( t_j \in Z_q^* \), calculate \( Q_{B_j} = t_j P \). Otherwise, \( Q_{B_j} = bP \) place \((ID_{B_j}, t_j, Q_{B_j})\) in the \( H_5 \)-list, and return \( Q_{B_j} \).
- **H_4 query**: If \( (V_j, h_4) \) exists in the \( H_4 \)-list, return \( h_4 \). Otherwise, check if VDBDH oracle returns 1 when queried with the tuple \((aP, bP, c^{-1} P, V_j)\). If this is the case, \( C \) returns \( V_j = e(P, P)^{abc^{-1}} \) and stops. Otherwise, randomly select \( h_4 \in Z_q^* \) update the \( H_4 \)-list, and return \( h_4 \).
- **H_i (i = 0, 1, 2, 5) query**: Upon receiving an \( H_i \) query, if the corresponding query exists in the \( H_i \)-list, return it to \( A_1 \). Otherwise, \( C \) randomly selects an integer as the query result and returns it to \( A_1 \). Meanwhile, \( C \) places the query result into the \( H_i \)-list.

- **Partial private key query**: Upon receiving a partial private key query on ID_{B_j}, if ID_{B_j} \( \neq ID_{B_j}^i \) \((i = 1, 2, \ldots, n)\), retrieves the corresponding \((ID_{B_j}, t_j, Q_{B_j})\) from the \( H_3 \)-list and sets \( D_{B_j} = t_j c^{-1} P \) return \( D_{B_j} \). Otherwise, \( C \) aborts.
- **Public key query**: When \( C \) receives a public key query on ID_{B_j}, if there exists \((ID_{B_j}, x_{B_j}, p_{kB_j})\) in the \( PK \)-list, then \( C \) returns \( p_{kB_j} \); otherwise, \( C \) randomly selects \( x_{B_j} \in Z_q^* \), computes \( p_{kB_j} = x_{B_j} P \), places \((ID_{B_j}, x_{B_j}, p_{kB_j})\) into the \( PK \)-list, and returns \( p_{kB_j} \) as the answer.
- **Replace public key**: When \( C \) receives a replace public key query on ID_{B_j}, \( C \) first finds \((ID_{B_j}, x_{B_j}, p_{kB_j})\) on the \( PK \)-list, then \( C \) updates the \( PK \)-list with the \( ID_{B_j} \)-tuple \((ID_{B_j}, \perp, p_{kB_j})\) and sets \( x_{B_j} = \perp, p_{kB_j} = p_{kB_j} \).
- **Secret key query**: When \( C \) receives a secret key query on ID_{B_j}, if \( C \) replaces public key of ID_{B_j}, then \( C \) returns \( \perp \). Otherwise, there exists \((ID_{B_j}, x_{B_j}, p_{kB_j})\) in the \( PK \)-list and returns \( x_{B_j} \) as answer.
- **Unsigncrypt query**: When receiving an unsigncrypt query under ID_{A}, ID_{B} and ciphertext \( \sigma \), if ID_{B_j} \( \neq ID_{B_j}^i \) \((i = 1, 2, \ldots, n)\), \( C \) runs the formal unsigncrypt algorithm and return
the answer. Otherwise, \( C \) goes through the \( H_3 \)-list with \( (V_j, h_j) \) to find a value such that \( h_j \) meets the VDBDH oracle returns 1 when queried on the tuple \((bP, c^{-1}P, U_j, V_j)\). If such a tuple exists, return \( h_j \) and computer \( r_2 = q_h \oplus h_j, K = KDF(r_2) \). Recover \( M = \text{DEM}.\text{Dec}(K, C) \), use \( H_5 \) query to obtain \( h_j \), then check equation \( e(P, s_j) = e(P, U_j \oplus h_j Q_A) \). If holds, return \( M \). Otherwise, output \( \bot \).

**Challenge:** After the first stage, \( A_1 \) outputs two plaintexts \( M_0, M_1 \) and \( ID_A, ID_B (j = 1, 2, \cdots, n) \) to \( C \). If \( ID_{B_j} \neq ID_{B_j} (i = 1, 2, \cdots, n) \), then \( C \) fails and aborts. Otherwise, \( C \) randomly chooses \( x' \in Z_q, \varphi_j \in Z_q^* \), obtains \( h_j \) from \( H_5 \) query, sets \( U'_i = aP, \) and computes \( U_i' = -h_j Q_A + x' P \). Obtain \( r'_j = \varphi_j \oplus T \) (where \( T \) is \( C \) candidate for the VDBDH obtained from \( H_4 \) query), \( K_j = KDF(r'_j) \). Then, \( C \) randomly selects \( K_0 \in K_{\text{MHHC}} \) and \( b \in \{0, 1\} \) computes \( C' = \text{DEM}.\text{Enc}(K_0, M_{b_j}) \), \( s_j' = x' P \). Finally, \( C \) provides the ciphertext \( \sigma' = (C', \varphi' \leftarrow (U'_1, U'_2, s_j', \varphi'_j)) \) to \( A_1 \).

**Phase 2:** \( A_1 \) request a second series of queries as before.

**Guess:** At the end of the simulation, \( A_1 \) outputs a bit \( b' \) for which the relation \( \sigma' = \text{Sign-crypt}(M_b, sk_A, ID_B) \) holds. If \( b' = b, \) \( C \) outputs \( T = e(U_i, D_{b_j}) = e(aP, bc^{-1}P) = (P, P)^{abc^{-1}} \) as a solution of the VDBDH problem.

Then, we assess probability. The probability to fail in signcryption queries is at most \( (q_{H_1} + q_a)q/2^k \), and the probability to fail in unsigncryption queries is at most \( q/2^k \). Note that the probability for \( C \) to not to fail in first stage is \( (q_{H_1} - q_{ppk})/q_{H_1} \). Furthermore, with a probability exactly \( 1/(q_{H_1} - q_{ppk}) \), \( A_1 \) chooses to be challenged on \( ID'_{B_j} \). Thus, the advantage of \( C \) is 

\[
\varepsilon = \left(1/(q_{H_1} - q_{ppk})\right)/2^{k-1}.
\]

**Lemma 2:** In the random oracle, if there is an IND-CCA2 adversary \( A_2 \) has an advantage \( \varepsilon \) against \( \text{MHHC} \). Then an algorithm \( C \) that solves the DBDH problem with an advantage

\[
\varepsilon = \left(1/(q_{H_1} - q_{ppk})\right)/2^{k-1}.
\]

**Proof:** We construct a simulator \( C \) uses \( A_2 \) to decide whether \( T = e(P, P)^{abc} \) by providing a random instance \( (P, aP, bP, cP, T) \) as the DBDH problem. This proof considers the indistinguishability of \( m \).

**Setup:** At the beginning, \( C \) sets \( P_2 = s_2 P \) and proves the system parameters to the attacker \( A_2 \). The target identity is \( ID'_j (i = 1, 2, 3, 4, 5) \) and \( PK \)-list, which are used to record answers to the corresponding \( H_1 \)-query and public key query.

**Phase 1.** \( A_2 \) requests a number of queries. \( C \) keeps the \( H_1 \)-list \( (i = 1, 2, 3, 4, 5) \) and \( PK \)-list, which are used to record answers to the corresponding \( H_1 \)-query and public key query.

- **\( H_3 \)-query:** Input an identity \( ID_B \). If \( ID_{B_j} \neq ID_{B_j} (i = 1, 2, 3, 4, 5) \), randomly choose \( t_i \in Z_q^* \), calculates \( Q_B = t_i P \). Otherwise, calculates \( Q_B = bP \) and \( (ID_{B_j}, t_j, Q_B) \) in \( H_3 \)-list return \( Q_B \).

- **\( H_i \)-query**: Upon receiving an \( H_i \)-query, if the corresponding query exists in the \( H_1 \)-list, then return it to \( A_2 \). Otherwise, \( C \) randomly selects an integer as the query result and returns it to \( A_2 \). Meanwhile, \( C \) places the query result into the \( H_1 \)-list.

- **Public key query:** Upon receiving a public key query on \( ID_B \). If \( ID_{B_j} \neq ID_{B_j} (i = 1, 2, 3, 4, 5) \), randomly selects \( x_{B_j} \in Z_q^* \) computes \( pk_B = x_{B_j} P \) and updates the \( PK \)-list. If \( ID_{B_j} = ID_{B_j} (i = 1, 2, 3, 4, 5) \), set \( pk_B = cP \) and update the \( PK \)-list with \( (ID_{B_j}, cP) \) and return \( pk_B \).

- **Secret key query:** When \( C \) receives a secret key query on \( ID_B \) if \( ID_{B_j} = ID_{B_j} (i = 1, 2, 3, 4, 5) \) returns \( \bot \). Otherwise, there exists \( (ID_{B_j}, x_{B_j}, pk_B) \) in \( PK \)-list returns \( x_{B_j} \).
Unsigncrypt query: When receiving an unsigncrypt query under $ID_A$, $ID_B$ and ciphertext $\sigma$, $C$ can compute $V_j = e(U_j, D_B)$, obtains $r_2 = \varphi_j \oplus H_4(V_j)$, $K = KDF(r_2)$, recovers $M = DEM.Dec(K, C)$. Then, if $ID_{B_i} = ID_{B_j}(i = 1, 2, \ldots, n)$, $C$ fails and stops ($C$ cannot compute $R_j$ for $sk_B$ is only $ID_{B_j}$ can compute). Otherwise, $ID_{B_i}$ recovers its own message $m_i = (m_i \oplus R_j) \oplus R_i$. Submitting $H_5$ query to obtain $h_5$. Then, equation $e(P_i, S_i) = e(P, U_2+ h_j Q_A)$ is checked. If holds, $m_i$ is returned. Otherwise, output $\perp$.

Challenge: After the first stage, $A_2$ outputs two plaintexts $m_0, m_1$ and $ID_A, ID_B(i = 1, 2, \ldots, n)$ to $C$, if $ID_{B_i} \neq ID_{B_j}(i = 1, 2, \ldots, n)$, $C$ fails and abort. Otherwise, $C$ randomly chooses $x' \in Z_p, \phi_j' \in Z_p^*$, obtains $h_i'$ from $H_5$ query, sets $U_i = aP$, computes $U_i^j = -h_j^jQ_A + x'P$, $V_j' = e(U_j, D_B)$. Gets $r_2' = \phi_j' \oplus H_4(V_j')$, $K' = KDF(r_2')$, computes $S_j' = x'P$, $C = DEM.Enc((K', M'))$, where $M' = m_j \oplus T$. Finally, $C$ provides the ciphertext $\sigma' = (C', \phi' = (U_i', Z_2, S_i', \phi_j'))$ to $A_2$.

Phase 2. $A_2$ then requests a second series of queries as before.

Guess: At the end of the simulation, $A_2$ outputs a bit $b'$ for which believes the relation $\sigma' = \text{Signcrypt}(M', sk_B, ID_B)$ holds. If $b' = b$, $C$ outputs $T = e(pk_A, Q_B)$, $e(CP, bP)^b = (P, P)^ab$ as a solution of DBDH problem. Then, we assess probability. The probability to fail in signcryption queries is at most $q_s/2^k$, and the probability to fail in unsigncrytion queries is at most $q_u/2^k$. Note that the probability for $C$ to not to fail in first stage is $(q_{H_5} - q_{ab})/q_{H_5}$. Furthermore, with a probability exactly $1/(q_{H_5} - q_{ab})$, $A_2$ chooses to be challenged on $ID_{B_i}^j$. Thus, the advantage of $C$ is $\frac{e(q_{H_5} - q_{ab})/2^{k-1}}{q_{H_5}}$.

Unforgeability

Theorem 2. In the random oracle model, if an EUF-CMA adversary $F$ has the advantage $\epsilon$ against MHHSC, then exists an algorithm $C$ that solves the VCBFDH problem with the advantage $\frac{e(1-(q_{H_5} + q_{ab})/2^{k-1})}{q_{H_5} - q_{ab}}$.

Proof. We construct a simulator $C$ that uses $F$ to decide whether $\sigma = \text{Signcrypt}(M', sk_B, ID_B)$ holds by providing a random instance $(P, aP, bP, dP, d^{-1})$ as the VCBFDH problem.

Setup: At the beginning, $C$ sets $P_i = dP$ and provides the system parameters to the attacker $F$. The target identity is $ID_A$.

Attack: $F$ requests a number of queries. $C$ keeps the $H_1$-lists $(i = 1, 2, 3, 4, 5)$ which are used to record answers to the corresponding $H_1$ query.

- $H_1$ query: Input an identity $ID_A$. If $ID_A \neq ID_{A_i}, t \in Z_p^*$ is randomly selected, $Q_A = tP$ is calculated. Otherwise, calculate $Q_A = bP$ place $(ID_{A_i}, t, Q_A)$ into the $H_1$-list, and return $Q_A$.

- $H_2(i = 0, 2, 3, 4, 5)$ query: Upon receiving a $H_i$ query, if the corresponding query exists in the $H_2$-list, return it to $A_2$. Otherwise, $C$ randomly selects an integer as the query result and returns it to $A_2$. Meanwhile, $C$ places the query result into the $H_2$-list.

- Private key query: When $C$ receives a partial private key query on $ID_A$, if $ID_A \neq ID_{A_i}$ retrieves the corresponding $(ID_{A_i}, t, Q_A)$ from the $H_1$-list and sets $sk_A = td^{-1}P$, return $sk_A$. Otherwise, $C$ aborts.

- Signcrypt query: When receiving a signcrypt query under $ID_A$, $\{ID_{B_i}\}_{i=1}^{n}$ and $n$ messages $m_i(i = 1, 2, \ldots, n)$. If $ID_A \neq ID_{A_i}$, the formal signcrypt algorithm runs and returns ciphertext $\sigma$. Otherwise, $C$ randomly selects $x, r_2 \in Z_p^*$, computes $U_1 = xP$; $V_i = e(U_1, D_B)$, $R_i = e(U_1, sk_B)$, $\varphi_i = r_2 \oplus H_4(V_i)$ and let $\varphi = (\varphi_1, \varphi_2, \cdots, \varphi_n)$. Compute $C = DEM.Enc(K, M)$.
where $K = KDF(r_2)$ and $M = (m_1 \oplus R_1 || m_2 \oplus R_2 || \cdots || m_n \oplus R_n)$. Obtain $h_i$ from the $H_k$ query, compute $U_2 = -h_iQ_A + xP_1$, $S_i = xP$, and return ciphertext $\sigma = (C, \phi \leftarrow (U_1, U_2, S, \varphi))$.

Equation $e(P_1, S_i) = e(P, U_2 + h_iQ_A)$ holds.

**Forge**: Finally, $F$ outputs $\sigma^*$ and $ID_A, ID_B$ to $C$. If $ID_A \neq ID_{A^*}$, $C$ fails and aborts. Otherwise, by forking lemma [25], $C$ selects a different hash function $h_i$ and interacts with $F$ with the same random tape, then the adversary $F$ can provide a different forger $\sigma^*$. We know that $\sigma^*$ and $\sigma^*$ should satisfy the equation $e(P, S_i^*) = e(P, U_2 + h_iQ_A)$ and $e(P_1, S_i^*) = e(P, U_2 + h_iQ_A)$. bd$^{-1}$ is obtained, then $C$ derives the value of $e(P, P)^{abd^{-1}}$ as $e(aP, bd^{-1}P)$. Hence, $C$ successfully solves the VCBDH problem.

The probability of failing in signcryption queries is at most $(q_{H_4} + q_s)/2^{k}$. With a probability of exactly $1/(q_{H_4} - q_s)$, $F$ chooses to be challenged on $ID_A$. Then, the advantage of $C$ is $
abla^{e(1 - (q_{H_4} + q_s)/2^k)} / q_{H_4} - q_s$.

**Performance evaluation**

**Functionality comparison**

To our knowledge, no hybrid signcryption schemes have achieved heterogeneity. Therefore, we compare our scheme with existing heterogeneous signcryption schemes [6] [8] in terms of supporting multi-message, multi-recipient, identity privacy-preservation, heterogeneous system, and different master keys. Table 1 illustrates that our scheme has many excellent features. First, the scheme takes advantages of pseudo-identity to ensure the anonymity of senders and receivers. Second, the scheme supports heterogeneous systems with different master keys. Our scheme has more advantages from the functionality and system setup perspective.

Then, we compare the computational costs of scheme [8] with that of our scheme. In scheme [8], numerous additions and multiplications must be executed to computing $p_i(x)$ and $F_i$. If the steps of computing $p_i(x)$ and $F_i$ are not considered, Table 2 shows that scheme [8] still requires $7P, 6M$ and $3E$, thus indicating that it is less efficient than our scheme. Here $P$, $M$, and $E$ denote pairing, multiplication, and exponentiation operations, respectively.

### Table 1. Functionality comparison.

| Comparison items            | Our scheme | [6] | [8] |
|----------------------------|------------|----|----|
| Heterogeneous system       | Yes        | Yes| Yes|
| Master key                 | Yes        | No | Yes|
| Multi-message              | Yes        | No | No |
| Multi-recipient            | Yes        | No | Yes|
| Privacy-preservation       | Yes        | No | Yes|

https://doi.org/10.1371/journal.pone.0184407.t001

### Table 2. Computational cost.

| Scheme | Signcryption | Unsigncryption |
|--------|--------------|----------------|
| [8]    | $2P + 3M + 1E$ | $5P + 3M + 2E$ |
| Ours   | $2P + 1M + 2E$ | $4P + 1M$      |

$P$: pairing operation; $M$: multiplication operation; $E$: exponentiation operation.

https://doi.org/10.1371/journal.pone.0184407.t002
Computational overhead comparison

To provide numerical results, we implement IBC-CLC MHHSC to measure the performance of signcryption and unsigncryption operations. Our implementation is written in C using the Pairing-Based Cryptography Library (Libpbc) [26]. For the computations, we use the curve groups that are implemented in the Libpbc library. The computations are run on a PC with 3.10 GHz CPU frequency, 4 GB of RAM, and Linux operating system. In the experiment, we used elliptical curves with a base field size of 512 bits and an embedding degree of 2. The security levels are selects as $|p| = 512$.

The performing consequence of our scheme is provided in Fig 1. Including total operation, signcryption, and unsigncryption operation time of our scheme when the number of the receiver is set as $n = 1, 10, 50, 100, 200, 500, 1000$. From the figure, we can indicate that signcryption time increases with the number of recipients. However, when unsigncryption, each receiver only operates on its own message, the unsigncryption operation time is not related to the increase of the receiver. So compared with the signcryption and total operation time of the receiver for 1000, the unsigncryption operation time is 0.018, near the bottom of the axis. Therefore, we can see that our scheme can achieve more efficient communication between two systems, which have greater difference in computing power. Users in IBC can handle big data, while users in CLC only need deal with a few data, such as infrastructure-to-vehicle (I2V) communication in vehicular ad hoc networks (VANETs). Trusted authorities or road side units can be the users in IBC system, which have much more capability, and hundreds of on board units can be the users in CLC system, which ability is limited.

Conclusion

We propose a novel conditional privacy-preserving heterogeneous hybrid signcryption scheme for IBC to CLC (MHHSC), which allows to send multi-message to multi-receiver. The proposed scheme selects different master secret keys in different systems and maps a distinct
pseudo-identity for each user, only the trusted authority could trace the real identity for any disputed event when necessary, which ensures conditional privacy preservation for all users in heterogeneous systems. It is definitely more practical for actual applications, such as VANETs. Moreover, we provide the formal definition and security models for the heterogeneous hybrid signcryption scheme. Proof shows that our scheme is indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen message attacks, which is satisfied confidentiality and unforgeability in the random oracle model. Owing to today’s diverse and complex network system and application environment, our follow-up work could be propose a bidirectional heterogeneous signcryption scheme between IBC and CLC for multi-party user.

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

Conceptualization: Shufen Niu, Ling Niu, Xiyan Yang.
Data curation: Ling Niu.
Formal analysis: Ling Niu, Xiyan Yang, Caifen Wang.
Funding acquisition: Shufen Niu, Caifen Wang, Xiangdong Jia.
Investigation: Ling Niu, Xiyan Yang.
Methodology: Shufen Niu, Ling Niu.
Project administration: Shufen Niu, Xiangdong Jia.
Resources: Shufen Niu, Ling Niu.
Software: Ling Niu, Xiangdong Jia.
Supervision: Shufen Niu, Caifen Wang.
Validation: Shufen Niu.
Visualization: Ling Niu.
Writing – original draft: Shufen Niu, Ling Niu.
Writing – review & editing: Shufen Niu, Ling Niu.

References

1. Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) ≤ cost (signature) + cost (encryption). In: Advances in Cryptology-CRYPTO’97, LNCS 1294. Springer-Verlag; 1997. p. 165–179.
2. Sun Y, Li H. Efficient signcryption between TPKC and IDPKC and its multi-receiver construction. Science China Information Sciences. 2010; 53(3):557–566. https://doi.org/10.1007/s11432-010-0061-5
3. Huang Q, Wong DS, Yang G. Heterogeneous signcryption with key privacy. Computer Journal. 2011; 54(4):525–536. https://doi.org/10.1093/comjnl/bxq085
4. Li F, Zhang H, Takagi T. Efficient signcryption for heterogeneous systems. IEEE Systems Journal. 2013; 7(3):420–429. https://doi.org/10.1109/JSYST.2012.2221897
5. Zhang Y, Zhang L, Zhang Y, Wang H, Wang C. CLPKC-to-TPKI heterogeneous signcryption scheme with anonymity. Acta Electronica Sinica. 2016; 44(10):2432–2439.
6. Li F, Han Y, Jin C. Practical access control for sensor networks in the context of the Internet of Things. Computer Communications. 2016; 89(90):154–164. https://doi.org/10.1016/j.comcom.2016.03.007
7. Li F, Han Y, Jin C. Practical signcryption for secure communication of wireless sensor networks. Wireless Personal Communications. 2016; 89(4):1391–1412. https://doi.org/10.1007/s11277-016-3327-4
8. Li Y, Wang C, Zhang Y, Niu S. Privacy-preserving multi-receiver signcryption scheme for heterogeneous systems. Security and Communication Networks. 2016; 9(17):4574–4584. https://doi.org/10.1002/sec.1650
9. Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing. 2003; 33(1):167–226. https://doi.org/10.1137/S0097539702403773
10. Dent AW. Hybrid signcryption schemes with outsider security. In: Information Security-ISC 2005, LNCS 3650. Springer-Verlag; 2005. p. 203–217.
11. Dent AW. Hybrid signcryption schemes with insider security. In: Information Security and Privacy-ACISP 2005, LNCS 3574. Springer-Verlag; 2005. p. 253–266.
12. Tan CH. Insider-secure signcryption KEM/tag-KEM schemes without random oracles. In: The Third International Conference on Availability, Reliability and Security-ARES 2008. p. 1275–1281.
13. Smart NP. Efficient key encapsulation to multiple parties. In: proceedings of the 4th International Conference on Security in Communication Networks; 2005. p. 208–219.
14. Sun Y, Li H. ID-based signcryption KEM to multiple recipients. Chinese Journal of Electronics. 2011; 20(2):317–322.
15. Li F, Shirase M, Takagi T. Identity-based hybrid signcryption. In: The Fourth International Conference on Availability, Reliability and Security (ARES 2009), IEEE Computer Society; 2009. p. 534–539.
16. Li F, Shirase M, Takagi T. Certificateless hybrid signcryption. In: The 5th Information Security Practice and Experience Conference (ISPEC 2009), LNCS 5451. Springer-Verlag; 2009. p. 112–123.
17. Yu H, Yang B. Provably secure certificateless hybrid signcryption. Chinese Journal of Computers. 2015; 38(4):804–813.
18. Wang C, Jiang H, Yang X, Zhang Y, Niu S. Multi-message and multi-receiver hybrid signcryption scheme based on discrete logarithm. Computer Engineering. 2016; 42(1):150–155. Available from: http://www.ecice06.com/EN/Y2016/V42/I1/150
19. Tonguz O, Wisitpongphan N, Bai F, Mudalige P, Sadekar V. Broadcasting in VANET. In: IEEE; 2007. p.7–12.
20. Li L. Bifurcation and chaos in a discrete physiological control system. Applied Mathematics and Computation. 2015; 252(252):397–404. https://doi.org/10.1016/j.amc.2014.11.107
21. Sun G, Wang C, Wu Z. Pattern dynamics of a Gierer-Meinhardt model with spatial effects. Nonlinear Dynamics. 2017; 88(2):1–12. https://doi.org/10.1007/s11071-016-3317-9
22. Li M, Jin Z, Sun G, Zhang J. Modeling direct and indirect disease transmission using multi-group model. Journal of Mathematical Analysis and Applications. 2017; 446(2):1292–1309. https://doi.org/10.1016/j.jmaa.2016.09.043
23. Li F, Shirase M, Takagi T. Efficient multi-pkg id-based signcryption for ad hoc networks. In: Inscrypt 2008, LNCS 5487. Springer-Verlag; 2009. p. 289–304.
24. Horng SJ, Tseng SF, Huang PH, Wang X, Li T, Muhammad KK. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. Information Sciences. 2015; 317(C):48–66. https://doi.org/10.1016/j.ins.2015.04.033
25. Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology. 2000; 13(3):361–396. https://doi.org/10.1007/s001450010003
26. The pairing-based cryptography library. Available from: http://crypto.stanford.edu/pbc/