Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage

Kaitai Liang, Willy Susilo, *Senior Member, IEEE* and Joseph K. Liu[+]

***Abstract*—The need of secure big data storage service is more desirable than ever to date. The basic requirement of the service is to guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously. Moreover, the service also should provide practical and fine-grained encrypted data sharing such that a data owner is allowed to share a ciphertext of data among others under some specified conditions. This paper, for the first time, proposes a privacy-preserving ciphertext multi-sharing mechanism to achieve the above properties. It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext senders/recipients. Furthermore, the paper shows that the new primitive is secure against chosen-ciphertext attacks in the standard model.**

Keywords: Privacy, anonymity, proxy re-encryption, big data.

I. Introduction

To date many individuals and companies choose to upload their data to clouds since the clouds supports considerable data storage service but also efficient data processing capability. Accordingly, it is unavoidable that trillions of personal and industrial data are flooding the Internet. For example, in some smart grid scenario, a governmental surveillance authority may choose to supervise the electricity consumption of a local living district. A great amount of electricity consumed data of each family located inside the district will be automatically transferred to the authority via Internet period by period. The need of big data storage, therefore, is more desirable than ever.

A basic security requirement of big data storage is to guarantee the confidentiality of the data. Fortunately, some existing cryptographic encryption mechanisms can be employed to fulfill the requirement. For instance, Public Key Encryption (PKE) allows a data sender to encrypts the data under the public key of receiver such that no one except the valid recipient can gain access to the data. Nevertheless, this does not satisfy all the requirements of users in the scenario of big data storage.

Consider the following scenario. We suppose a hospital stores its patients' medical records in a cloud storage system and meanwhile, the records are all encrypted so as to avoid the cloud server from accessing to any patient's medical information. After a record is encrypted and further uploaded to the cloud, only those specified doctors can gain access to the record. By using some traditional PKE, Identity-Based Encryption (IBE), or Attribute-Based Encryption (ABE), the confidentiality of the record can be protected effectively.

By trivially employing traditional encryption mechanisms (to guarantee the confidentiality of medical record), nevertheless, we cannot prevent some sensitive personal information from being leaked to the cloud server but also the public. This is because traditional encryption systems do not consider the anonymity of a ciphertext sender/receiver. Accordingly, someone, could be anyone with capability of obtaining a ciphertext (e.g. cloud server), may know whose public key the ciphertext is encrypted under, namely who is the owner of the ciphertext, such that the patient associated with the ciphertext can be easily identified. Similarly, the recipient/destination of the ciphertext, e.g., Cardiology Dept., can be known from the ciphertext without any difficulty as well. This seriously disgraces the privacy of patient.

Moreover, a patient might be transferred to more than one medical department in different treatment phases. The corresponding medical record then needs to be converted to the ciphertexts corresponding to various receivers so as to be shared among the departments. Therefore, the update of ciphertext recipient is desirable. Precisely speaking, a fine-grained ciphertext update for receivers is necessary in the sense that a ciphertext can be conditionally shared with others. The medical record owner, e.g., the patient, has rights to decide who can gain access to the record, and which kinds of data are allowed for access. For example, the patient can choose to specify that only the medical record described with "teeth" can be read by a dentist. This fine-grained control prevents a data sharing mechanism from being limited to the "all-or-nothing" share mode.

This research work aims to solve the above problems. To preserve anonymity, some well-known encryption mechanisms are proposed in the literature, such as anonymous IBE [8]. By employing these primitives, the source and the destination of data can be protected privately. However, the primitives cannot support the update of ciphertext receiver.

There are some naive approaches to update ciphertext's recipient. For instance, data owner can employ the decrypt-then-re-encrypt mode. Nonetheless, this is applicable to the scenario where there is only a small amount of data. If the encrypted data is either a group of sequences of genome information or a network audit log, the decryption and re-

[+]Joseph K. Liu is the corresponding author.

K. Liang is with the Department of Computer Science, Aalto University, Finland (e-mail: kaitai.liang@aalto.fi).

W. Susilo, is with Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia (e-mail: wsusilo@uow.edu.au).

J.K. Liu is with Faculty of Information Technology, Monash University, Australia (e-mail: joseph.liu@monash.edu).

encryption might be time consumed and computation costly. Moreover, this mode also suffers from a limitation that the data owner has to be on-line all the time. Alternatively, a fully trusted third party with knowledge of the decryption key of the data owner may be delegated to handle the task. Nevertheless, this strongly relies on the fully trust of the party. Besides, the anonymity of the ciphertext receiver cannot be achieved as the party needs to know the information of recipient to proceed the re-encryption. Therefore, both of the approaches do not scale well in practice.

Introduced by Mambo and Okamoto [26] and further defined in [5], Proxy Re-Encryption (PRE) is proposed to tackle the dilemma of data sharing. It allows a semi-trusted party, called proxy, to transform a ciphertext intended for a user into a ciphertext of the same message intended for another user without leaking knowledge of either the decryption keys or the message. The workload of data owner is now transferred to the proxy, and the "on-line all the time" requirement is unnecessary.

This work concentrates on the identity-based cryptographic setting. To employ PRE in the IBE setting, [17] defined the notion of Identity-Based Proxy Re-Encryption (IBPRE), which offers a practical solution for access control in networked file storage [17], and secure email with IBE [17]. To capture privacy-preserving property and ciphertext's recipient update simultaneously, [30] proposed an anonymous IBPRE system, which is CCA security in the Random Oracle Model (ROM).

The valuable work [30] introduces the first anonymous IBPRE in the literature and meanwhile, it leaves us interesting and meaningful open problems. The work only supports one-time ciphertext receiver update, while multiple receivers update is desirable in practice. On the other hand, the work provides an "all-or-nothing" share mode that limits the flexibility of data sharing.

A. Our Contributions

In this paper, we aim to propose a ciphertext sharing mechanism with the following properties:

- *Anonymity*: given a ciphertext, no one knows the identity information of sender and receiver.
- *Multiple receiver-update*: given a ciphertext, the receiver of the ciphertext can be updated in multiple times. In this paper, we refer to this property as "multi-hop".
- *Conditional sharing*: a ciphertext can be fine-grained shared with others if the pre-specified conditions are satisfied.

Achievements. We investigate a new notion, AMH-IBCPRE. We formalize the definition and security model by incorporating the definitions in [31], [32]. In the security model, we allow the corrupted users to be adaptively chosen by an adversary, while the adversary must output the challenge identity at the outset of security game. Moreover, we define four security models for different practical purposes.

- The security model of MH-IBCPRE is the basic one, in which a challenger plays the game with the adversary to launch Chosen-Ciphertext Attacks (CCA) to the original ciphertext and re-encrypted ciphertext in order to solve a hard problem.
- We also consider the case where a proxy colludes with delegatee to compromise the underlying message and the secret key of delegator. Here, the protection of the message is very difficult to achieve as the delegatee can always decrypt the corresponding ciphertext for the proxy. The secret key of the delegator, however, is possible to be secured.
- For the definition of collusion attacks model, we allow an adversary to acquire all re-encryption keys, and the adversary wins the game if it outputs a valid secret key of an uncorrupted user. We note that our definition is in the selective model in which the adversary has to output a target identity at the outset of the game.
- As to the security model of anonymity, it is complicated in the sense that we categorize the game into two subgames: one is the anonymity for delegator (i.e. given the original ciphertext an adversary cannot output the identity of delegator), the other is the anonymity of re-encryption key (i.e. an adversary cannot distinguish a valid re-encryption key from a random one belonging to re-encryption key space).

We next propose a concrete construction for unidirectional AMH-IBCPRE, in which it achieves multiple ciphertext receiver update, conditional data sharing, anonymity and collusion-safe (i.e. holding against collusion attacks) simultaneously in asymmetric bilinear group. Note the functionality of our system is generally described in Fig 1. We state that the new primitive is applicable to many real-world applications, such as secure email forwarding, electronic encrypted data sharing, where both anonymity and flexible encrypted data sharing are needed. We also show that the scheme is CCA-secure in the standard model under the decisional P-Bilinear Diffie-Hellman assumption. To the best of our knowledge, our system is the first of its kind in the literature.

B. Related Work

Following the concept of delegation of decryption rights introduced by Mambo and Okamoto [26], Blaze et al. [5] formalized the concept of PRE, and proposed a seminal bidirectional PRE scheme. Afterwards, many PRE schemes have been proposed, such as [2], [3], [11], [18], [24], [19], [22], [25], [20].

Employing traditional PRE in the context of IBE, Green and Ateniese [17] initially introduced the notion of IBPRE, and proposed two unidirectional IBPRE schemes in the ROM: one is CPA secure and the other holds against CCA. Later on, two CPA-secure IBE-PRE schemes (in the types of PKE-IBE and IBE-IBE) [27] have been proposed. Afterwards, some IBPRE systems have been proposed for various requirements (e.g. [34], [28]).

In the multiple ciphertext receiver update[1] scenario, Green and Ateniese [17] proposed the first MH-IBPRE scheme with CPA security. Later on, a RCCA-secure MH-IBPRE scheme

[1]We refer to multiple ciphertext receiver update to a notion called Multi-Hop (MH) in this paper.

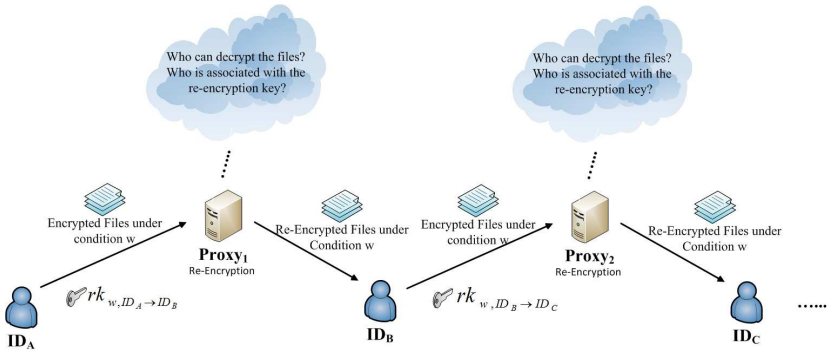


Fig. 1: Anonymous Multi-Hop Identity-Based Conditional Proxy Re-Encryption

without random oracles was proposed by Chu and Tzeng [12]. These schemes, however, are not collusion-safe. To solve the problem, Shao and Cao [31] proposed a CCA-secure MH-IBPRE in the standard model with collusion-safe property.

To hide the information leaked from re-encryption key, Ateniese et al. [1] defined the notion of key-privacy (i.e. an adversary cannot identify delegator and delegatee even given re-encryption key). Later on, Shao et al. [33] revised the security model introduced in [1]. To prevent a ciphertext from being traced, Emura et al. [15] proposed a unidirectional IBPRE scheme in which an adversary cannot identify the source from the destination ciphertext. To ensure the privacy of both delegator and delegatee, Shao et al. [32] proposed the first Anonymous PRE (ANO-PRE) system. The system guarantees that an adversary cannot identify the recipient of original and re-encrypted ciphertext even given the corresponding re-encryption key. In 2012, Shao [30] also proposed the first anonymous IBPRE with CCA security in the ROM.

In the context of IBE/ABE, some well-known systems supporting anonymity that have been proposed, such as [8], [9], [16], [29]. Leveraging them may partially fulfill our goals. However, we need to focus on the combination of anonymity and ciphertext update properties. Therefore, the aforementioned systems are not taken in comparison below.

Here, we compare our work with the some related systems, and summarize the comparison of properties in Table I. While multiple ciphertext receiver update (denoting as M.U.), conditional (data) share, collusion resistance (denoting as C.R.), anonymity, and without random oracle (denoting as W.R.O.), have all five been partially achieved by previous schemes, there is no effective CCA-secure proposal that achieves all properties simultaneously in the standard model. This paper, for the first time, fills the gap.

TABLE I: Functionality and Security Comparison

Sch.	Security	W.R.O.	M.U.	C.R.	Conditional Share	Anonymity
[17]	CPA	✗	✓	✗	✗	✗
[12]	RCCA	✓	✓	✗	✗	✗
[31]	CCA	✓	✓	✓	✗	✗
[30]	CCA	✗	✗	✓	✗	✓
Ours	CCA	✓	✓	✓	✓	✓

II. System Definition and Threat Models

A. System Definition

Definition 1: A unidirectional Multi-Hop Identity-Based Conditional Proxy Re-Encryption (MH-IBCPRE) scheme consists of the following algorithms:

1) $(mpk, msk) \leftarrow Setup(1^k)$: on input a security parameter k, output a master public key mpk and a master secret key msk. For simplicity, we omit mpk in the expression of the following algorithms.
2) $sk_{ID} \leftarrow KeyGen(msk, ID)$: on input msk, and an identity $ID \in \{0,1\}^*$, output a secret key sk_{ID}.
3) $rk_{w,ID_i \to ID_{i'}} \leftarrow ReKeyGen(ID_i, sk_{ID_i}, ID_{i'}, w)$: on input a delegator's identity ID_i and the corresponding secret key sk_{ID_i}, a delegatee's identity $ID_{i'}$, and a condition $w \in \{0,1\}^*$, output a re-encryption key $rk_{w,ID_i \to ID_{i'}}$ from ID_i to $ID_{i'}$ under condition w.
4) $C_{1,ID_i,w} \leftarrow Enc(ID_i, w, m)$: on input an identity ID_i, a condition w and a message m, output a 1-level ciphertext $C_{1,ID_i,w}$ under identity ID_i and w.
5) $C_{l+1,ID_{i'},w} \leftarrow ReEnc(rk_{w,ID_i \to ID_{i'}}, C_{l,ID_i,w})$: on input $rk_{w,ID_i \to ID_{i'}}$, and an l-level ciphertext $C_{l,ID_i,w}$ under identity ID_i and w, output an $(l+1)$-level ciphertext $C_{l+1,ID_{i'},w}$ under identity $ID_{i'}$ and w or $\perp$ for failure, where $l \geq 1, l \in \mathbb{N}$.
6) $m \leftarrow Dec(sk_{ID_i}, C_{l,ID_i,w})$: on input sk_{ID_i}, and an l-level ciphertext $C_{l,ID_i,w}$ under identity ID_i and w, output a message m or $\perp$ for failure, where $l \geq 1, l \in \mathbb{N}$.

Correctness: For any $k, l \in \mathbb{N}$, any identities $ID_i, ID_{i'} \in \{0,1\}^*$, $i \in \{1, ..., l\}$, any condition $w \in \{0,1\}^*$ and any message $m \in \{0,1\}^k$, if $(mpk, msk) \leftarrow Setup(1^k)$, $sk_{ID} \leftarrow KeyGen(msk, ID)$, for all ID used in the system, $rk_{w,ID_i \to ID_{i'}} \leftarrow ReKeyGen(ID_i, sk_{ID_i}, ID_{i'}, w)$, $C_{1,ID_i,w} \leftarrow Enc(ID_i, w, m)$, and $C_{l,ID_{i'},w} \leftarrow ReEnc(rk_{w,ID_i \to ID_{i'}}, w, C_{l-1,ID_i,w})$, we have

$$Dec(sk_{ID_1}, w, C_{1,ID_1,w}) = m;$$
$$Dec(sk_{ID_i}, w, ReEnc(rk_{w,ID_{i-1} \to ID_i}, w,$$
$$ReEnc(rk_{w,ID_{i-2} \to ID_{i-1}}, w, ...,$$
$$ReEnc(rk_{w,ID_1 \to ID_2}, w, Enc(ID_1, w, m))))...) = m.$$

B. Threat Models

We define four models in terms of the selective condition and selective identity chosen ciphertext security (IND-sCon-sID-CCA), collusion resistance, the anonymity of the original ciphertext and anonymity of the re-encryption key in this section. Before proceeding, we define some notations.

- **Delegation Chain.** There is a set of re-encryption keys $RK = \{rk_{w,ID_{i_1}\rightarrow ID_{i_2}}, ..., rk_{w,ID_{i_{l-1}}\rightarrow ID_{i_l}}\}$ under the same condition w, for any re-encryption key $rk_{w,ID_{i_j}\rightarrow ID_{i_{j+1}}}$ in RK, $ID_{i_j} \neq ID_{i_{j+1}}$. We say that there exists a delegation chain under w from identity ID_{i_1} to identity ID_{i_l}, denoted as $w|ID_{i_1} \rightarrow ... \rightarrow ID_{i_l}$. Note this delegation chain includes the case where $ID_{i_1} = ID_{i_l}$. Besides, we use $w|ID$ to indicate a ciphertext under w and ID, and for a single identity ID we use $\perp |ID$ to denote it.
- **Uncorrupted/Corrupted Identity.** If the secret key of an identity is compromised by an adversary, the identity is a corrupted identity. Else, it is an uncorrupted identity.
- **Uncorrupted Delegation Chain.** Suppose there is a delegation chain under w from ID_i to ID_j (i.e. $w|ID_i \rightarrow ... \rightarrow ID_j$). If there is no corrupted identity in the chain, it is an uncorrupted delegation chain. Else, it is corrupted. The delegation chain is built up once either a related re-encryption key is generated or a corresponding re-encryption is constructed.

Definition 2: A unidirectional MH-IBCPRE scheme is IND-sCon-sID-CCA-secure if no PPT adversary $\mathcal{A}$ can win the game below with non-negligible advantage. In the game, $\mathcal{B}$ is the game challenger and k is the security parameter.

1) **Init.** $\mathcal{A}$ outputs a challenge identity $ID^* \in \{0,1\}^*$ and a challenge condition $w \in \{0,1\}^*$.
2) **Setup.** $\mathcal{B}$ runs $setup(1^k)$ and returns mpk to $\mathcal{A}$.
3) **Phase 1.** $\mathcal{A}$ is given access to the following oracles.
   a) $\mathcal{O}_{sk}(ID)$: given an identity ID, output $sk_{ID} \leftarrow KeyGen(msk, ID)$.
   b) $\mathcal{O}_{rk}(ID_i, ID_{i'}, w)$: on input two distinct identities ID_i and $ID_{i'}$, and a condition w, output $rk_{w,ID_i\rightarrow ID_{i'}} \leftarrow ReKeyGen(ID_i, sk_{ID_i}, ID_{i'}, w)$, where $sk_{ID_i} \leftarrow KeyGen(msk, ID_i)$.
   c) $\mathcal{O}_{re}(ID_i, ID_{i'}, w, C_{l,ID_i,w})$: on input two distinct identities ID_i and $ID_{i'}$, a condition w, and an l-level ciphertext $C_{l,ID_i,w}$ under ID_i and w, output $C_{l+1,ID_i,w} \leftarrow ReEnc(rk_{w,ID_i\rightarrow ID_{i'}}, C_{l,ID_i,w})$, where $rk_{w,ID_i\rightarrow ID_{i'}} \leftarrow ReKeyGen(ID_i, sk_{ID_i}, ID_{i'}, w)$, $sk_{ID_i} \leftarrow KeyGen(msk, ID_i)$.
   d) $\mathcal{O}_{dec}(ID_i, C_{l,ID_i,w})$: on input an identity ID_i, and an l-level ciphertext $C_{l,ID_i,w}$, output $m \leftarrow Dec(sk_{ID_i}, C_{l,ID_i,w})$, where $sk_{ID_i} \leftarrow KeyGen(msk, ID_i)$.

   In this phase the followings are forbidden to issue:
   - $\mathcal{O}_{sk}(ID)$ for any ID, if there is an uncorrupted delegation chain under w^* from ID^* to ID, or $ID^* = ID$.
   - $\mathcal{O}_{rk}(ID_i, ID_{i'}, w^*)$ for any $ID_i, ID_{i'}$, if there is an uncorrupted delegation chain under w^* from ID^* to ID_i or $ID^* = ID_i$, but $ID_{i'}$ is in a corrupted delegation chain.
4) **Challenge.** $\mathcal{A}$ outputs two equal length messages m_0, m_1, and a set of identities $\{ID_{i_j}\}_{j=1}^{j=l^*-1}$ to $\mathcal{B}$. $\mathcal{B}$ computes C_{l^*,ID^*,w^*} as

$$ReEnc(ReKeyGen(ID_{i_{l^*-1}}, sk_{ID_{i_{l^*-1}}}, ID^*, w^*),$$
$$ReEnc(ReKeyGen(ID_{i_{l^*-2}}, sk_{ID_{i_{l^*-2}}}, ID_{i_{l^*-1}}, w^*),$$
$$..., ReEnc(ReKeyGen(ID_{i_1}, sk_{ID_{i_1}}, ID_{i_2}, w^*),$$
$$Enc(ID_{i_1}, w^*, m_b)))),$$

   where $l^* \geq 2, l^* \in \mathbb{N}, b \in_R \{0,1\}$. Note that we here put ID^* to the l^* level of the ciphertext. This shows no difference from putting it in the first level of the ciphertext since the system supports multi-hop property.
5) **Phase 2.** Same as in **Phase 1** except the followings:
   a) $\mathcal{O}_{re}(ID_i, ID_{i'}, w^*, C_{l,ID_i,w^*})$: if (ID_i, C_{l,ID_i,w^*}) is a derivative of (ID^*, C_{l^*,ID^*,w^*}), and $ID_{i'}$ is in a corrupted delegation chain. As of [11], a derivative of (ID^*, C_{l^*,ID^*,w^*}) is defined as follows.
      i. (ID^*, C_{l^*,ID^*,w^*}) is a derivative of itself.
      ii. If (ID_i, C_{l,ID_i,w^*}) is a derivative of (ID^*, C_{l^*,ID^*,w^*}), and $(ID_{i'}, C_{l',ID_{i'},w^*})$ is a derivative of (ID_i, C_{l,ID_i,w^*}), then $(ID_{i'}, C_{l',ID_{i'},w^*})$ is a derivative of (ID^*, C_{l^*,ID^*,w^*}), where $l' \geq l \geq l^*$.
      iii. If $\mathcal{A}$ has issued a re-encryption key query to $\mathcal{O}_{rk}$ on $(ID_i, ID_{i'}, w)$ to obtain the re-encryption key $rk_{w,ID_i\rightarrow ID_{i'}}$, and achieved $C_{(l+1,ID_{i'},w)} \leftarrow ReEnc(rk_{w,ID_i\rightarrow ID_{i'}}, C_{(l,ID_i,w)})$, then $(ID_{i'}, C_{(l+1,ID_{i'},w)})$ is a derivative of $(ID_i, C_{(l,ID_i,w)})$.
      iv. If $\mathcal{A}$ can execute $C_{(l+1,ID_{i'},w)} \leftarrow ReEnc(ReKeyGen(ID_i, sk_{ID_i}, ID_{i'}, w), C_{(l,ID_i,w)})$ on its own, then $(ID_{i'}, C_{(l+1,ID_{i'},w)})$ is a derivative of $(ID_i, C_{(l,ID_i,w)})$, where $sk_{ID_i} \leftarrow KeyGen(msk, ID_i)$.
      v. If $\mathcal{A}$ has issued a re-encryption query on $(ID_i, ID_{i'}, w, C_{(l,ID_i,w)})$ and obtained $C_{(l+1,ID_{i'},w)}$, then $(ID_{i'}, C_{(l+1,ID_{i'},w)})$ is a derivative of $(ID_i, C_{(l,ID_i,w)})$.
   b) $\mathcal{O}_{dec}(ID_i, w^*, C_{l,ID_i,w^*})$: if (ID_i, C_{l,ID_i,w^*}) is a derivative of (ID^*, C_{l^*,ID^*,w^*}). We state that by derivative we mean the issued ciphertext cannot have any delegation link record (including given re-encryption key/re-encrypted ciphertext histories reflected in the delegation chain) related to ID^* and w^*.
6) **Guess.** $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b' = b$, $\mathcal{A}$ wins.

The advantage of $\mathcal{A}$ is defined as $\epsilon = Adv^{IND\text{-}sCon\text{-}sID\text{-}CCA}_{MH\text{-}IBCPRE,\mathcal{A}}(1^k) = |Pr[b' = b] - \frac{1}{2}|$.

We now proceed to collusion resistance that guarantees that an adversary cannot compromise the entire secret key of a delegator even if it colludes with the delegatee.

Definition 3: A unidirectional MH-IBCPRE scheme holds against selective collusion attacks if the advantage $Adv^{CR}_{\mathcal{A}}(1^k)$ is negligible for any PPT adversary $\mathcal{A}$ in the following

experiment. Set $O_1 = \{\mathcal{O}_{sk}, \mathcal{O}_{rk}\}$ and $Adv_{\mathcal{A}}^{CR}(1^k)$ as

$$Pr[sk_{ID^*} \in \Omega : (ID^*, State) \leftarrow \mathcal{A}(1^k); (mpk, msk) \leftarrow Setup(1^k); sk_{ID^*} \leftarrow \mathcal{A}^{O_1}(mpk, State)]$$

where k is the security parameter, $State$ is the state information, ID^* is the target and uncorrupted identity, $\mathcal{O}_{sk}$ and $\mathcal{O}_{rk}$ are the oracles defined in Definition 2, Ω is the valid secret key space, and sk_{ID^*} is the valid secret key of ID^*. If $\mathcal{A}$ issues ID^* to $\mathcal{O}_{sk}$, output $\perp$.

Below we define the anonymity of the original ciphertext (ANO-OC) for MH-IBCPRE, that is, given the original ciphertext, an adversary cannot tell the identity of delegator.

Definition 4: A unidirectional MH-IBCPRE scheme achieves ANO-OC if the advantage $Adv_{\mathcal{A}}^{ANO\text{-}OC}(1^k)$ is negligible for any PPT adversary $\mathcal{A}$ in the following experiment. Set $O_2 = \{\mathcal{O}_{sk}, \mathcal{O}_{rk}, \mathcal{O}_{re}, \mathcal{O}_{dec}\}$, and $Adv_{\mathcal{A}}^{ANO\text{-}OC}(1^k)$ as

$$|Pr[b = b' : (w^*, ID_0^*, ID_1^*, State_1) \leftarrow \mathcal{A}(1^k); (mpk, msk) \leftarrow Setup(1^k); (m, State_2) \leftarrow A^{O_2}(mpk, State_1); b \in_R \{0,1\}; C_{1,ID_b^*,w^*} \leftarrow Enc(ID_b^*, w^*, m); b' \leftarrow A^{O_2}(C_{1,ID_b^*,w^*}, State_2);] - \frac{1}{2}|,$$

where k is the security parameter, $State_1, State_2$ are the state information, ID_0^*, ID_1^* are two distinct uncorrupted identities, C_{1,ID_b^*,w^*} is constructed by the game challenger, $\mathcal{O}_{sk}$, $\mathcal{O}_{rk}$, $\mathcal{O}_{re}$, $\mathcal{O}_{dec}$ are the oracles with the following constraints. In $\mathcal{O}_{sk}$, the oracle outputs $\perp$ if there is an uncorrupted delegation chain under w^* from ID_b^* to ID or $ID_b^* = ID$. In $\mathcal{O}_{rk}$, the oracle outputs $\perp$ if there is an uncorrupted delegation chain under w^* from ID_b^* to ID_i or $ID_b^* = ID_i$, and $ID_{i'}$ is in a corrupted delegation chain. For $\mathcal{O}_{re}$, if the issued ciphertext is a derivative of $(ID_b^*, C_{1,ID_b^*,w^*})$, and $ID_{i'}$ is in a corrupted delegation chain, output $\perp$. For $\mathcal{O}_{dec}$, if the issued ciphertext is a derivative of $(ID_b^*, C_{1,ID_b^*,w^*})$, output $\perp$.

Finally, we define the anonymity of the re-encryption key (ANO-RK), in which an adversary cannot distinguish a real re-encryption key from a random one.

Definition 5: A unidirectional MH-IBCPRE scheme achieves ANO-RK if no PPT adversary $\mathcal{A}$ can win the game below with non-negligible advantage.

1) **Init.** $\mathcal{A}$ outputs a delegator's identity ID', a challenge delegatee's identity ID^*, and a challenge condition w^*.
2) **Setup.** Same as Definition 2.
3) **Phase 1.** $\mathcal{A}$ is allowed to issue queries to $\mathcal{O}_{sk}, \mathcal{O}_{rk}, \mathcal{O}_{re}$ and $\mathcal{O}_{dec}$ which are the oracles defined Definition 2 with the same restrictions.
4) **Challenge.** If the following queries
   - $\mathcal{O}_{sk}(ID_i)$ for any ID_i, if there is an uncorrupted delegation chain under w^* from ID^* to ID_i, or $ID^* = ID_i$.
   - $\mathcal{O}_{rk}(ID_i, ID_j, w^*)$ for any ID_i, ID_j, if there is an uncorrupted delegation chain under w^* from ID^* to ID_i or $ID^* = ID_i$, but ID_j is in a corrupted delegation chain.

   are never made, $\mathcal{B}$ flips a coin-toss for $b \in \{0,1\}$. Then $\mathcal{B}$ sets the re-encryption key $rk_{w^*,ID' \to ID^*}$ as a random key from the re-encryption key space if $b = 0$ and computes $rk_{w^*,ID' \to ID^*} \leftarrow ReKeyGen(ID', sk_{ID'}, ID^*, w^*)$ otherwise. Finally, $\mathcal{B}$ outputs $rk_{w^*,ID' \to ID^*}$ to $\mathcal{A}$.
5) **Phase 2.** Same as **Phase 1** except the followings:
   a) $\mathcal{O}_{sk}(ID_i)$ for any ID_i, if there is an uncorrupted delegation chain under w^* from ID^* to ID_i, or $ID^* = ID_i$;
   b) $\mathcal{O}_{rk}(ID_i, ID_j, w^*)$ for any ID_i, ID_j, if there is an uncorrupted delegation chain under w^* from ID^* to ID_i or $ID^* = ID_i$, but ID_j is in a corrupted delegation chain;
   c) $\mathcal{O}_{re}(ID_i, ID_{i'}, w^*, C_{l,ID_i,w^*})$: if (ID_i, C_{l,ID_i,w^*}) is a (derivative of) ciphertext generated by a re-encryption key in the delegation chain under w^* from ID^* to ID_i, and $ID_{i'}$ is in a corrupted delegation chain; and
   d) $\mathcal{O}_{dec}(ID_i, w^*, C_{l,ID_i,w^*})$: if (ID_i, C_{l,ID_i,w^*}) is a (derivative of) ciphertext generated by a re-encryption key in the delegation chain under w^* from ID^* to ID_i.
6) **Guess.** $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b' = b$, $\mathcal{A}$ wins.

The advantage of $\mathcal{A}$ is defined as $Adv_{\mathcal{A}}^{ANO\text{-}RK}(1^k) = |Pr[b' = b] - \frac{1}{2}|$.

Remark. As sated in [1], the anonymity of the re-encrypted ciphertext is implied by the anonymity of the re-encryption key, we hence omit the details here.

III. Preliminaries

A. Asymmetric Pairings

Let $BSetup$ be an algorithm that on input the security parameter k, outputs the parameters of a bilinear map as $(q, g, \hat{g}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, where $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are multiplicative cyclic groups of prime order q, where $|q| = k$, and g is a random generator of $\mathbb{G}_1$, $\hat{g}$ is a random generator of $\mathbb{G}_2$. The mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ has three properties: (1) *Bilinearity*: for all $a, b \in_R \mathbb{Z}_q^*$, $e(g^a, \hat{g}^b) = e(g, \hat{g})^{ab}$; (2) *Non-degeneracy*: $e(g, \hat{g}) \neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ is the unit of $\mathbb{G}_T$; (3) *Computability*: e can be efficiently computed. Note that G_1 and G_2 are not the same.

Asymmetric Decisional BDH (ADBDH) Problem [14]. Given a tuple $(g, g^a, g^c, \hat{g}, \hat{g}^a, \hat{g}^b) \in \mathbb{G}_1^3 \times \mathbb{G}_2^3$ and $T \in \mathbb{G}_T$, decide whether $T = e(g, \hat{g})^{abc}$.

(Asymmetric) Decisional $\mathcal{P}$-BDH Problem [14]. Given a tuple $(g, g^a, g^{ab}, g^c, \hat{g}, \hat{g}^a, \hat{g}^b) \in \mathbb{G}_1^4 \times \mathbb{G}_2^3$ and $T \in \mathbb{G}_T$, decide whether $T = e(g, \hat{g})^{abc}$.

Definition 6: **ADBDH Assumption [14]**. We say that an algorithm $\mathcal{A}$ has advantage $Adv_{\mathcal{A}}^{ADBDH} = \epsilon$ in solving the $ADBDH$ problem in $(\mathbb{G}_1, \mathbb{G}_2)$ if $|Pr[\mathcal{A}(g, g^a, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, e(g,\hat{g})^{abc}) = 0] - Pr[\mathcal{A}(g, g^a, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, T) = 0]| \geq \epsilon$, where the probability is over the random choice of generators $g \in \mathbb{G}_1$ and $\hat{g} \in \mathbb{G}_2$, the random choice of exponents $a, b, c \in \mathbb{Z}_q^*$, $T \in \mathbb{G}_T$, and the random bits used by $\mathcal{A}$. We say that the ADBDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no PPT algorithm has advantage ϵ in solving the ASBDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.

Definition 7: **(Asymmetric) Decisional $\mathcal{P}$-BDH Assumption [14]**. We say that an algorithm $\mathcal{A}$ has advantage $Adv_{\mathcal{A}}^{\mathcal{P}\text{-}BDH} = \epsilon$ in solving the decisional $\mathcal{P}$-BDH problem

in $(\mathbb{G}_1, \mathbb{G}_2)$ if $|Pr[\mathcal{A}(g, g^a, g^{ab}, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, g^{abc}) = 0] - Pr[\mathcal{A}(g, g^a, g^{ab}, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, T) = 0]| \geq \epsilon$, where the probability is over the random choice of generators $g \in \mathbb{G}_1$ and $\hat{g} \in \mathbb{G}_2$, the random choice of exponents $a, b, c \in \mathbb{Z}_q^*$, $T \in \mathbb{G}_1$, and the random bits used by $\mathcal{A}$. We say that the decisional $\mathcal{P}$-BDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no PPT algorithm has advantage ϵ in solving the decisional $\mathcal{P}$-BDH problem.

B. Building Blocks

Strongly Existential Unforgeable One-Time Signatures. A strongly existential unforgeable (sUF) one-time signature [4] consists of the following algorithms:

1) $(K_s, K_v) \leftarrow Sig.KG(1^k)$: on input a security parameter $k \in \mathbb{N}$, the algorithm outputs a signing/ verification key pair (K_s, K_v).
2) $\sigma \leftarrow Sign(K_s, M)$: on input the signing key K_s and a message $M \in \Gamma_{Sig}$, the algorithm outputs a signature σ, where Γ_{Sig} is the message space of a signature scheme.
3) $1/0 \leftarrow Ver(K_v, \sigma, M)$: on input the verification key K_v, a signature σ and a message M, the algorithm outputs 1 when σ is a valid signature of M, and output 0 otherwise.

One-time Symmetric Encryption. A one-time symmetric encryption [13] consists of the following algorithms. Note let $\mathcal{K}_D$ be the key space $\{0,1\}^{poly(1^k)}$, and SYM be a symmetric encryption scheme, where $poly(1^k)$ is the fixed polynomial size (bound) with respect to the security parameter k. The encryption algorithm $SYM.Enc$ intakes a key $K \in \mathcal{K}_D$ and a message M, outputs a ciphertext C. The decryption algorithm $SYM.Dec$ intakes K and C, outputs M or a symbol $\perp$.

C. An Anonymous IBE and Its Extensions

Ducas [14] introduces an efficient anonymous IBE (Du-ANO-IBE) scheme in the standard model. We review its construction below, and omit the definition and security model of Du-ANO-IBE as the details can be found in [14].

- $Setup(1^k)$: run $(q, g, \hat{g}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow BSetup(1^k)$, choose random values $\alpha, \beta, \gamma, \delta, \eta \in \mathbb{Z}_q^*$, and set $g_1 = g^\alpha$, $g_2 = g^\beta$, $h = g^\gamma$, $f = g^\delta$, $t = g^\eta$, $\hat{g}_1 = \hat{g}^\alpha$, $\hat{g}_2 = \hat{g}^\beta$, $\hat{h} = \hat{g}^\gamma$, $\hat{f} = \hat{g}^\delta$, $\hat{t} = \hat{g}^\eta$. The master secret key $msk = (\hat{g}_0 = \hat{g}^{\alpha\beta}, \hat{f}, \hat{t})$, the master public key $mpk = (g, \hat{g}, g_1, h, f, t, \hat{g}_2, \hat{h})$.
- $Extract(msk, ID)$: given msk and an identity $ID \in \mathbb{Z}_q^*$, randomly choose $r, R \in \mathbb{Z}_q^*$, output $sk_{ID} = (sk_{ID_0}, sk_{ID_1}, sk_{ID_2}) = (\hat{g}_0(\hat{h}^{ID}\hat{f})^r\hat{t}^R, \hat{g}^r, \hat{g}^R)$.
- $Enc(mpk, ID, m)$: randomly choose $s \in \mathbb{Z}_q^*$, compute $C_1 = e(g_1, \hat{g}_2)^s \cdot m$, $C_2 = g^s$, $C_3 = (h^{ID}f)^s$, $C_4 = t^s$, and output the ciphertext $C = (C_1, C_2, C_3, C_4)$, where $ID \in \mathbb{Z}_q^*$, $m \in \mathbb{G}_T$.
- $Dec(sk_{ID}, C)$: given a ciphertext $C = (C_1, C_2, C_3, C_4)$, using the private key sk_{ID} to recover the plaintext $m = C_1 \cdot e(C_3, sk_{ID_1}) \cdot e(C_4, sk_{ID_2})/e(C_2, sk_{ID_0})$.

By Theorem 1 and its corresponding security proof in [14], we have the following theorem.

Theorem 1: Du-ANO-IBE is selective-ID (sID) anonymous and secure against chosen-plaintext attacks assuming the decisional $\mathcal{P}$-BDH assumption holds.

Below we employ the BB1 HIBE technique [6] to extend Du-ANO-IBE to be a two levels encryption scheme without losing CPA security, where the first level is the identity, and the second level is the condition. We state that the first level is anonymous, but the second level is not.

- $Setup(1^k)$: let $w \in \mathbb{Z}_q^*$ be a condition, and choose α, β, γ, δ_1, δ_2, $\eta \in_R \mathbb{Z}_q^*$, and set $g_1 = g^\alpha$, $g_2 = g^\beta$, $h = g^\gamma$, $f_1 = g^{\delta_1}$, $f_2 = g^{\delta_2}$, $t = g^\eta$, $\hat{g}_1 = \hat{g}^\alpha$, $\hat{g}_2 = \hat{g}^\beta$, $\hat{h} = \hat{g}^\gamma$, $\hat{f}_1 = \hat{g}^{\delta_1}$, $\hat{f}_2 = \hat{g}^{\delta_2}$, $\hat{t} = \hat{g}^\eta$. The master secret key $msk = (\hat{g}_0 = \hat{g}^{\alpha\beta}, \hat{f}_1, \hat{t})$, the master public key $mpk = (g, \hat{g}, g_1, h, f_1, f_2, t, \hat{g}_2, \hat{f}_2, \hat{h})$.
- $Extract(msk, ID)$: set $sk_{ID} = (sk_{ID_0}, sk_{ID_1}, sk_{ID_2}, sk_{ID_3}) = (\hat{g}_0(\hat{h}^{ID}\hat{f}_1)^{r_1}(\hat{h}^w\hat{f}_2)^{r_2}\hat{t}^R, \hat{g}^{r_1}, \hat{g}^{r_2}, \hat{g}^R)$, where r_1, r_2, $R \in \mathbb{Z}_q^*$. Given $sk_{ID} = (sk_{ID_0}, sk_{ID_1}, sk_{ID_2})$ which is generated in the algorithm $Extract$ of Du-ANO-IBE, one can easily derive the above secret key by using the BB1 construction technique. To achieve the consistency of algorithm description, we here use the "same" secret key generation expression.
- $Enc(mpk, ID, m, w)$: set $C_1 = e(g_1, \hat{g}_2)^s \cdot m$, $C_2 = g^s$, $C_3 = (h^{ID}f_1)^s$, $C_4 = t^s$ and $C_5 = (h^w f_2)^s$, where $s \in \mathbb{Z}_q^*$.
- $Dec(sk_{ID}, C)$: compute $m = C_1 \cdot e(C_3, sk_{ID_1}) \cdot e(C_5, sk_{ID_2}) \cdot e(C_4, sk_{ID_3})/e(C_2, sk_{ID_0})$.

We refer to the above system as 2-level Du-ANO-HIBE. As stated in [14], Du-ANO-IBE can be extended to 2-level system to achieve CCA security via BB1 HIBE construction technique. The above system is exactly the converted 2-level system except that the second level is a condition instead of a verification key (of a one-time signature). Here the CPA security of 2-level Du-ANO-HIBE still relies on the decisional $\mathcal{P}$-BDH assumption, and the corresponding proof is straightforward to reuse the proof technique presented in [14]. Therefore, we have the following theorem.

Theorem 2: 2-level Du-ANO-HIBE is anonymous and CPA secure assuming the decisional $\mathcal{P}$-BDH assumption holds.

D. A CCA-Secure 3-Level Du-ANO-HIBE

Here we convert 2-level Du-ANO-HIBE to achieve CCA security by using the CHK transformation [10]. Following the BB1 HIBE construction, a 3-level CCA-secure anonymous system, which is anonymous relative to the first level but not the second and third levels, can be built as follows.

- $Setup(1^k)$: same as the algorithm $Setup$ of 2-level Du-ANO-HIBE except the followings. Choose random values $\delta_3 \in \mathbb{Z}_q^*$, and set $f_3 = g^{\delta_3}$ and $\hat{f}_3 = \hat{g}^{\delta_3}$. Choose an sUF one-time signature scheme $(Sig.KG, Sign, Ver)$ and set the verification key K_v is in $\mathbb{Z}_q^*$, where k_1 is the security parameter. The master public key $mpk = (g, \hat{g}, g_1, h, f_1, f_2, f_3, t, \hat{g}_2, \hat{f}_2, \hat{f}_3, \hat{h}, (Sig.KG, Sign, Ver))$.
- $Extract(msk, ID)$: set $sk_{ID} = (sk_{ID_0}, sk_{ID_1}, sk_{ID_2}, sk_{ID_3}, sk_{ID_4}) = (\hat{g}_0(\hat{h}^{ID}\hat{f}_1)^{r_1}(\hat{h}^w\hat{f}_2)^{r_2}(\hat{h}^{K_v}\hat{f}_3)^{r_3}\hat{t}^R, \hat{g}^{r_1}, \hat{g}^{r_2}, \hat{g}^{r_3}, \hat{g}^R)$, where r_1, r_2, r_3, $R \in \mathbb{Z}_q^*$. To achieve consistency of description, we keep the secret key generation in one algorithm. Actually, given the secret key of 2-level Du-ANO-HIBE, one can easily derive the above key.

- $Enc(mpk, ID, m, K_v)$: choose $s \in_R \mathbb{Z}_q^*$ and a one-time signature key pair $(K_s, K_v) \leftarrow Sig.KG(1^k)$, set $C_0 = K_v$, $C_1 = e(g_1, \hat{g}_2)^s \cdot m$, $C_2 = g^s$, $C_3 = (h^{ID} f_1)^s$, $C_4 = t^s$, $C_5 = (h^w f_2)^s$, $C_6 = (h^{K_v} f_3)^s$, $C_7 = Sign(K_s, (C_1, C_2, C_3, C_4, C_5, C_6))$.
- $Dec(sk_{ID}, C)$: given a ciphertext $C = (C_0, C_1, C_2, C_3, C_4, C_5, C_6, C_7)$, first verify whether $e(\hat{h}^{K_v} \hat{f}_3, C_2) = e(\hat{g}, C_6)$ and $Ver(K_v, C_7, (C_1, C_2, C_3, C_4, C_5, C_6)) = 1$ hold. If the equations do not hold, output $\perp$. Otherwise, compute $m = C_1 \cdot e(C_3, sk_{ID_1}) \cdot e(C_5, sk_{ID_2}) \cdot e(C_6, sk_{ID_3}) \cdot e(C_4, sk_{ID_4}) / e(C_2, sk_{ID_0})$.

We refer to the above system as 3-level Du-ANO-HIBE. By Theorem 2 and the security argument in [14], we have:

Theorem 3: If 2-level Du-ANO-HIBE is sID anonymous and CPA secure, and $(Sig.KG, Sign, Ver)$ is an sUF one-time signature scheme, 3-level Du-ANO-HIBE is sID anonymous and CCA secure.

The proof is straight forward to reuse the technique in [14].

IV. System Construction

A. Construction Details

We allow condition and identities to be arbitrary length, but they should be hashed by a Target Collision Resistant (TCR) hash function [13] $H_0 : \{0,1\}^* \to \mathbb{Z}_q^*$ beforehand.

- $Setup(1^k)$. Given k, run $(q, g, \hat{g}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow BSetup(1^k)$. Let $w \in \mathbb{Z}_q^*$ be a condition. Choose α, β, γ, δ_1, δ_2, δ_3, $\eta \in_R \mathbb{Z}_q^*$, and set $g_1 = g^\alpha$, $g_2 = g^\beta$, $h = g^\gamma$, $f_1 = g^{\delta_1}$, $f_2 = g^{\delta_2}$, $f_3 = g^{\delta_3}$, $t = g^\eta$, $\hat{g}_1 = \hat{g}^\alpha$, $\hat{g}_2 = \hat{g}^\beta$, $\hat{h} = \hat{g}^\gamma$, $\hat{f}_1 = \hat{g}^{\delta_1}$, $\hat{f}_2 = \hat{g}^{\delta_2}$, $\hat{f}_3 = \hat{g}^{\delta_3}$, $\hat{t} = \hat{g}^\eta$. Choose two TCR hash functions: $H_1 : \{0,1\}^k \to \mathbb{Z}_q^*$, $H_2 : \mathbb{G}_T \to \{0,1\}^{poly(1^k)}$, and a CCA-secure one-time symmetric key encryption $SYM = (SYM.Enc, SYM.Dec)$. Let $(Sig.KG, Sign, Ver)$ be a sUF one-time signature scheme and assume any verification key K_v in $\mathbb{Z}_q^*$. The master secret key $msk = (\hat{g}_0 = \hat{g}^{\alpha\beta}, \hat{f}_1, \hat{t})$, the master public key $mpk = (q, k, g, \hat{g}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, h, f_1, f_2, f_3, t, \hat{g}_2, \hat{f}_2, \hat{f}_3, \hat{h}, H_1, H_2, SYM, (Sig.KG, Sign, Ver))$.
- $Extract(msk, ID)$. Given msk and an identity $ID \in \mathbb{Z}_q^*$, choose $r, R \in_R \mathbb{Z}_q^*$, output $sk_{ID} = (sk_{ID_0}, sk_{ID_1}, sk_{ID_2}) = (\hat{g}_0 (\hat{h}^{ID} \hat{f}_1)^r \hat{t}^R, \hat{g}^r, \hat{g}^R)$. After receiving the secret key from PKG, the user can check the key as: $e(g, sk_{ID_0}) \stackrel{?}{=} e(g_1, \hat{g}_2) \cdot e(h^{ID} f_1, sk_{ID_1}) \cdot e(t, sk_{ID_2})$.
- $Enc(ID_i, w, m)$. Choose $s_0 \in_R \mathbb{Z}_q^*$ and a one-time signature key pair $(K_s, K_v) \leftarrow Sig.KG(1^k)$, compute $C_0 = K_v$, $C_1 = e(g_1, \hat{g}_2)^{s_0} \cdot m$, $C_2 = g^{s_0}$, $C_3 = (h^{ID_i} f_1)^{s_0}$, $C_4 = t^{s_0}$, $C_5 = (h^w f_2)^{s_0}$, $C_6 = (h^{K_v} f_3)^{s_0}$, $C_7 = Sign(K_s, (C_1, C_2, C_3, C_4, C_5, C_6))$, and output the 1-st level ciphertext $C_{1,ID_i,w} = (C_0, C_1, C_2, C_3, C_4, C_5, C_6, C_7)$, where $ID_i \in \mathbb{Z}_q^*$, $m \in \mathbb{G}_T$ and w is implicitly included in the ciphertext.
- $ReKeyGen(ID_i, sk_{ID_i}, ID_{i'}, w)$. Choose $\theta_1^{(l)} \in_R \mathbb{G}_T$, $\rho^{(l)}, s_1^{(l)}, \bar{r}_1^{(l)} \in_R \mathbb{Z}_q^*$ and a one-time signature key pair $(K_s^{(l)}, K_v^{(l)}) \leftarrow Sig.KG(1^k)$, compute $rk_{w,ID_i \to ID_{i'}}$: $rk_0^{(l)} = (sk_{ID_{i_0}} (\hat{h}^w \hat{f}_2)^{\rho^{(l)}})^{H_1(\theta_1^{(l)})}$, $rk_1^{(l)} = (\hat{g}^{\rho^{(l)}})^{H_1(\theta_1^{(l)})}$, $rk_2^{(l)} = sk_{ID_{i_1}}^{H_1(\theta_1^{(l)})}$, $rk_3^{(l)} = sk_{ID_{i_2}}^{H_1(\theta_1^{(l)})}$, $rk_4^{(l)} = e(g_1, \hat{g}_2)^{s_1^{(l)}} \cdot \theta_1^{(l)}$, $rk_5^{(l)} = g^{s_1^{(l)}}$, $rk_6^{(l)} = (h^{ID_{i'}} f_1)^{s_1^{(l)}}$, $rk_7^{(l)} = t^{s_1^{(l)}}$, $rk_8^{(l)} = (h^w f_2)^{s_1^{(l)}}$, $rk_9^{(l)} = (h^{K_v^{(l)}} f_3)^{s_1^{(l)}}$, $rk_{10}^{(l)} = K_v^{(l)}$, $rk_{11}^{(l)} = Sign(K_s^{(l)}, (rk_4^{(l)}, rk_5^{(l)}, rk_6^{(l)}, rk_7^{(l)}, rk_8^{(l)}, rk_9^{(l)}))$, $rk_{12}^{(l)} = (h^{ID_{i'}} f_1)^{\bar{r}_1^{(l)}}$, $rk_{13}^{(l)} = g^{\bar{r}_1^{(l)}}$, $rk_{14}^{(l)} = t^{\bar{r}_1^{(l)}}$, $rk_{15} = h^{\bar{r}_1^{(l)}}$, $rk_{16}^{(l)} = e(g_1, \hat{g}_2)^{\bar{r}_1^{(l)}}$, $rk_{17}^{(l)} = f_2^{\bar{r}_1^{(l)}}$, $rk_{18}^{(l)} = f_3^{\bar{r}_1^{(l)}}$, where $ID_i, ID_{i'} \in \mathbb{Z}_q^*$ and $l \in \{1, ..., poly(1^k)\}$.
- $ReEnc(rk_{w,ID_i \to ID_{i'}}, C_{l,ID_i,w})$.

1) If $l = 1$,

a) Verify

$$e(\hat{h}^{K_v} \hat{f}_3, C_2) \stackrel{?}{=} e(\hat{g}, C_6),$$
$$e(\hat{h}^w \hat{f}_2, C_2) \stackrel{?}{=} e(\hat{g}, C_5),$$
$$Ver(K_v, C_7, (C_1, C_2, C_3, C_4, C_5, C_6)) \stackrel{?}{=} 1. \quad (1)$$

If Eq. (1) does not hold, output $\perp$. Otherwise, proceed.

b) Choose $\theta_2^{(1)} \in_R \mathbb{G}_T$, $s_2^{(1)} \in_R \mathbb{Z}_q^*$ and a one-time signature key pair $(\bar{K}_s^{(1)}, \bar{K}_v^{(1)}) \leftarrow Sig.KG(1^k)$, compute $C_7^{(1)} = \frac{e(C_2, rk_0^{(1)}) / e(C_5, rk_1^{(1)})}{e(C_3, rk_2^{(1)}) \cdot e(C_4, rk_3^{(1)})}$, $\sigma^{(1)} = SYM.Enc(C_0 || C_1 || ... || C_7 || C_7^{(1)}, H_2(\theta_2^{(1)}))$, $C_8^{(1)} = rk_{16}^{s_2^{(1)}} \cdot \theta_2^{(1)}$, $C_9^{(1)} = rk_{13}^{(1) s_2^{(1)}}$, $C_{10}^{(1)} = rk_{12}^{(1) s_2^{(1)}}$, $C_{11}^{(1)} = rk_{14}^{(1) s_2^{(1)}}$, $C_{12}^{(1)} = (rk_{15}^{(1) w} rk_{17}^{(1)})^{s_2^{(1)}}$, $C_{13}^{(1)} = (rk_{15}^{(1) \bar{K}_v^{(1)}} rk_{18}^{(1)})^{s_2^{(1)}}$, $C_{14}^{(1)} = \bar{K}_v^{(1)}$, $C_{15}^{(1)} = Sign(\bar{K}_s^{(1)}, (C_8^{(1)}, C_9^{(1)}, C_{10}^{(1)}, C_{11}^{(1)}, C_{12}^{(1)}, C_{13}^{(1)}))$. Output $C_{2,ID_{i'},w} = (\sigma^{(1)}, C_8^{(1)}, C_9^{(1)}, C_{10}^{(1)}, C_{11}^{(1)}, C_{12}^{(1)}, C_{13}^{(1)}, C_{14}^{(1)}, C_{15}^{(1)}, rk_4^{(1)}, rk_5^{(1)}, rk_6^{(1)}, rk_7^{(1)}, rk_8^{(1)}, rk_9^{(1)}, rk_{10}^{(1)}, rk_{11}^{(1)})$.

2) If $l \geq 2$,

a) Verify

$$e(rk_5^{(l-1)}, \hat{h}^w \hat{f}_2) \stackrel{?}{=} e(rk_8^{(l-1)}, \hat{g}),$$
$$e(rk_5^{(l-1)}, \hat{h}^{K_v^{(l-1)}} \hat{f}_3) \stackrel{?}{=} e(rk_9^{(l-1)}, \hat{g}),$$
$$Ver(rk_{10}^{(l-1)}, rk_{11}^{(l-1)}, (rk_4^{(l-1)}, rk_5^{(l-1)}, rk_6^{(l-1)}, rk_7^{(l-1)}, rk_8^{(l-1)}, rk_9^{(l-1)})) \stackrel{?}{=} 1. \quad (2)$$
$$e(C_9^{(l-1)}, \hat{h}^w \hat{f}_2) \stackrel{?}{=} e(C_{12}^{(l-1)}, \hat{g}),$$
$$e(C_9^{(l-1)}, \hat{h}^{\bar{K}_v^{(l-1)}} \hat{f}_3) \stackrel{?}{=} e(C_{13}^{(l-1)}, \hat{g}),$$
$$Ver(C_{14}^{(l-1)}, C_{15}^{(l-1)}, (C_8^{(l-1)}, C_9^{(l-1)}, C_{10}^{(l-1)}, C_{11}^{(l-1)}, C_{12}^{(l-1)}, C_{13}^{(l-1)})) \stackrel{?}{=} 1. \quad (3)$$

If Eq. (2) and (3) do not hold, output $\perp$. Otherwise, proceed.

b) Choose $\theta_2^{(l)} \in_R \mathbb{G}_T$, $s_2^{(l)} \in_R \mathbb{Z}_p^*$ and $(\bar{K}_s^{(l)}, \bar{K}_v^{(l)}) \leftarrow Sig.KG(1^k)$, and then compute $C_{7,0}^{(l)} = \frac{e(rk_5^{(l-1)}, rk_0^{(l)}) / e(rk_8^{(l-1)}, rk_1^{(l)})}{e(rk_6^{(l-1)}, rk_2^{(l)}) \cdot e(rk_7^{(l-1)}, rk_3^{(l)})}$, $C_{7,1}^{(l)} = \frac{e(C_9^{(l-1)}, rk_0^{(l)}) / e(C_{12}^{(l-1)}, rk_1^{(l)})}{e(C_{10}^{(l-1)}, rk_2^{(l)}) \cdot e(C_{11}^{(l-1)}, rk_3^{(l)})}$, $\sigma^{(l)} = SYM.Enc(\sigma^{(l-1)} || C_8^{(l-1)} || ... || C_{15}^{(l-1)} || rk_4^{(l-1)} ||$

$...||rk_{11}^{(l-1)}||C_{7,0}^{(l-1)}||C_{7,1}^{(l-1)}, H_2(\theta_2^{(l)}))$, $C_8^{(l)} = rk_{16}^{(l)s_2^{(l)}} \cdot \theta_2^{(l)}$, $C_9^{(l)} = rk_{13}^{(l)s_2^{(l)}}$, $C_{10}^{(l)} = rk_{12}^{(l)s_2^{(l)}}$, $C_{11}^{(l)} = rk_{14}^{(l)s_2^{(l)}}$, $C_{12}^{(l)} = (rk_{15}^{(l)w} rk_{17}^{(l)})^{s_2^{(l)}}$, $C_{13}^{(l)} = (rk_{15}^{(l)\bar{K}_v^{(l)}} rk_{18}^{(l)})^{s_2^{(l)}}$, $C_{14}^{(l)} = \bar{K}_v^{(l)}$, $C_{15}^{(l)} = Sign(\bar{K}_s^{(l)}$, $(C_8^{(l)}$, $C_9^{(l)}$, $C_{10}^{(l)}$, $C_{11}^{(l)}$, $C_{12}^{(l)}$, $C_{13}^{(l)}))$. Output $C_{l,ID_{i'},w} = (\sigma^{(l)}$, $C_8^{(l)}$, $C_9^{(l)}$, $C_{10}^{(l)}$, $C_{11}^{(l)}$, $C_{12}^{(l)}$, $C_{13}^{(l)}$, $C_{14}^{(l)}$, $C_{15}^{(l)}$, $rk_4^{(l)}$, $rk_5^{(l)}$, $rk_6^{(l)}$, $rk_7^{(l)}$, $rk_8^{(l)}$, $rk_9^{(l)}$, $rk_{10}^{(l)}$, $rk_{11}^{(l)})$.

- $Dec(sk_{ID_i}, C_{l,ID_i,w})$.
  1) If $l = 1$,
     a) Verify Eq. (1). If Eq. (1) does not hold, output $\perp$. Otherwise, proceed.
     b) Compute

$$C_1 / \frac{e(C_2, sk_{ID_0})}{e(C_3, sk_{ID_1}) \cdot e(C_4, sk_{ID_2})}$$
$$= e(g_1, \hat{g}_2)^{s_0} \cdot m / \frac{e(g^{s_0}, \hat{g}_0(\hat{h}^{ID_i}\hat{f})^r \hat{t}^R)}{e((h^{ID_i}f)^{s_0}, \hat{g}^r) \cdot e(t^{s_0}, \hat{g}^R)}$$
$$= e(g_1, \hat{g}_2)^{s_0} \cdot m / e(g_1, \hat{g}_2)^{s_0} = m.$$

  2) If $l \geq 2$,
     a) Verify

$$e(rk_5^{(l)}, \hat{h}^w \hat{f}_2) \stackrel{?}{=} e(rk_8^{(l)}, \hat{g}),$$
$$e(rk_5^{(l)}, \hat{h}^{K_v^{(l)}} \hat{f}_3) \stackrel{?}{=} e(rk_9^{(l)}, \hat{g}),$$
$$Ver(rk_{10}^{(l)}, rk_{11}^{(l)}, (rk_4^{(l)}, rk_5^{(l)}, rk_6^{(l)}, rk_7^{(l)}, rk_8^{(l)}, rk_9^{(l)})) \stackrel{?}{=} 1. \quad (4)$$
$$e(C_9^{(l)}, \hat{h}^w \hat{f}_2) \stackrel{?}{=} e(C_{12}^{(l)}, \hat{g}),$$
$$e(C_9^{(l)}, \hat{h}^{\bar{K}_v^{(l)}} \hat{f}_3) \stackrel{?}{=} e(C_{13}^{(l)}, \hat{g}),$$
$$Ver(C_{14}^{(l)}, C_{15}^{(l)}, (C_8^{(l)}, C_9^{(l)}, C_{10}^{(l)}, C_{11}^{(l)}, C_{12}^{(l)}, C_{13}^{(l)})) \stackrel{?}{=} 1. \quad (5)$$

     If Eq. (4) and (5) do not hold, output $\perp$. Otherwise, proceed.
     b) Compute

$$\frac{e(rk_5^{(l)}, sk_{ID_{i'_0}})}{e(rk_6^{(l)}, sk_{ID_{i'_1}}) \cdot e(rk_7^{(l)}, sk_{ID_{i'_2}})}$$
$$= \frac{e(g^{s_1^{(l)}}, \hat{g}_0(\hat{h}^{ID_{i'}}\hat{f}_1)^r \hat{t}^R)}{e((h^{ID_{i'}}f_1)^{s_1^{(l)}}, \hat{g}^r) \cdot e(t^{s_1^{(l)}}, \hat{g}^R)}$$
$$= e(g_1, \hat{g}_2)^{s_1^{(l)}},$$

     and

$$\frac{e(C_9^{(l)}, sk_{ID_{i'_0}})}{e(C_{10}^{(l)}, sk_{ID_{i'_1}}) \cdot e(C_{11}^{(l)}, sk_{ID_{i'_2}})}$$
$$= \frac{e(g^{\bar{s}_2^{(l)}}, \hat{g}_0(\hat{h}^{ID_{i'}}\hat{f}_1)^r \hat{t}^R)}{e((h^{ID_{i'}}f_1)^{\bar{s}_2^{(l)}}, \hat{g}^r) \cdot e(t^{\bar{s}_2^{(l)}}, \hat{g}^R)}$$
$$= e(g_1, \hat{g}_2)^{\bar{s}_2^{(l)}},$$

     where $\bar{s}_2^{(l)} = s_2^{(l)} \cdot \bar{r}_1^{(l)}$.
     c) Compute two values $\theta_1^{(l)} = rk_4^{(l)} / e(g_1, \hat{g}_2)^{s_1^{(l)}}$, and $\theta_2^{(l)} = C_8^{(l)} / e(g_1, \hat{g}_2)^{\bar{s}_2^{(l)}}$. Recover $\sigma^{(l-1)}||C_8^{(l-1)}||....||C_{15}^{(l-1)}||rk_4^{(l-1)}||...||rk_{11}^{(l-1)}||C_{7,0}^{(l-1)}||C_{7,1}^{(l-1)} = SYM.Dec(\sigma^{(l)}, H_2(\theta_2^{(l)}))$.
     d) Compute

$$C_{7,0}^{(l-1)(H_1(\theta_1^{(l)}))^{-1}}$$
$$= (e(g_1, \hat{g}_2)^{s_1^{(l-1)}})^{(H_1(\theta_1^{(l)}))(H_1(\theta_1^{(l)}))^{-1}}$$
$$= e(g_1, \hat{g}_2)^{s_1^{(l-1)}},$$

     and $\theta_1^{(l-1)} = rk_4^{(l-1)} / e(g_1, \hat{g}_2)^{s_1^{(l-1)}}$ if Eq. (2) holds.
     e) Compute

$$C_{7,1}^{(l)(H_1(\theta_1^{(l)}))^{-1}}$$
$$= (e(g_1, \hat{g}_2)^{\bar{s}_2^{(l-1)}})^{(H_1(\theta_1^{(l)}))(H_1(\theta_1^{(l)}))^{-1}}$$
$$= e(g_1, \hat{g}_2)^{\bar{s}_2^{(l-1)}},$$

     and $\theta_2^{(l-1)} = C_8^{(l-1)} / e(g_1, \hat{g}_2)^{\bar{s}_2^{(l-1)}}$ if Eq. (3) holds.
     f) For $1 \leq j \leq l-2$, from $l-2$ to 1, compute $\theta_1^{(j)}$ and $\theta_2^{(j)}$ as in the previous steps.
     g) Recover

$$C_0||C_1||....||C_7||C_7^{(1)} = SYM.Dec(\sigma^{(1)}, H_2(\theta_2^{(1)})).$$

     Compute

$$C_1 / C_7^{(1)(H_1(\theta_1^{(1)}))^{-1}}$$
$$= e(g_1, \hat{g}_2)^{s_0} \cdot m / e(g_1, \hat{g}_2)^{s_0 H_1(\theta_1^{(1)})(H_1(\theta_1^{(1)}))^{-1}}$$
$$= m,$$

     if Eq. (1) holds.

Convert to be single-hop. It is not difficult to convert the current construction to become a single-hop system by eliminating the respective ciphertext and re-encryption key components $C_{12}^{(l)}$ and $rk_8^{(l)}$ in the algorithms $ReEnc$ and $ReKeyGen$, where $l = 1$. Without these necessary components, the resulting re-encrypted ciphertext cannot be further converted.

Support multi-condition. The system can be extended to support multi-condition for re-encryption control. We will concatenate all conditions together, and put the resulting concatenation into a TCR hash function H_0, and further regard the hash value as a keyword exponent w.

B. Security Analysis

Theorem 4: Our AMH-IBCPRE scheme is IND-sCon-sID-CCA secure assuming the decisional $\mathcal{P}$-BDH assumption holds, $(Sig.KG, Sign, Ver)$ is a sUF one-time signature scheme, SYM is a CCA-secure one-time symmetric key encryption and H_1, H_2 are TCR hash functions.

Please refer to Appendix A for the proof of Theorem 4.

Theorem 5: Our AMH-IBCPRE scheme is selective collusion resistant.

Please refer to Appendix B for the proof of Theorem 5.

Theorem 6: Our AMH-IBCPRE scheme achieves ANO-OC assuming the decisional $\mathcal{P}$-BDH assumption holds, $(Sig.KG, Sign, Ver)$ is a sUF one-time signature scheme, SYM is a CCA-secure one-time symmetric key encryption and H_1, H_2 are TCR hash functions.

Please refer to Appendix C for the proof of Theorem 6.

Theorem 7: Our AMH-IBCPRE scheme achieves ANO-RK assuming the decisional $\mathcal{P}$-BDH assumption holds, $(Sig.KG, Sign, Ver)$ is a sUF one-time signature scheme, SYM is a CCA-secure one-time symmetric key encryption and H_1, H_2 are TCR hash functions.

Please refer to Appendix D for the proof of Theorem 7.

V. Conclusions

We introduced a novel notion, anonymous multi-hop identity-based conditional proxy re-encryption, to preserve the anonymity for ciphertext sender/receiver, conditional data sharing and multiple recipient-update. We further proposed a concrete system for the notion. Meanwhile, we proved the system CCA-secure in the standard model under the decisional P-bilinear Diffie-Hellman assumption. To the best of our knowledge, our primitive is the first of its kind in the literature.

VI. Acknowledgements

Kaitai Liang is supported by Privacy-aware retrieval and modelling of genomic data (PRIGENDA, No. 13283250), Academy of Finland, Finland. Willy Susilo is partially supported by the Australian Research Council Discovery Project ARC DP130101383. Joseph K. Liu is supported by National Natural Science Foundation of China (61472083).

References

[1] G. Ateniese, K. Benson, and S. Hohenberger. Key-private proxy re-encryption. In *CT-RSA '09*, vol. 5473 of *LNCS*, pp. 279–294. Springer, 2009.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *NDSS '05*, pp. 29–43. Springer, 2005.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM TISSEC*, 9(1):1–30, 2006.

[4] M. Bellare and S. Shoup. Two-tier signatures, strongly unforgeable signatures, and fiat-shamir without random oracles. In *PKC*, vol. 4450 of *LNCS*, pp. 201–216. Springer, 2007.

[5] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In *EUROCRYPT '98*, pp. 127–144. Springer, 1998.

[6] D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In *EUROCRYPT '04*, vol. 3027 of *LNCS*, pp. 223–238. Springer, 2004.

[7] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *EUROCRYPT '05*, vol. 3494 of *LNCS*, pp. 440–456. Springer, 2005.

[8] X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In *CRYPTO*, vol. 4117 of *LNCS*, pp. 290–307. Springer, 2006.

[9] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy. Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data. In *PKC*, vol. 5443 of *LNCS*, pp. 196–214. Springer, 2009.

[10] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In *Eurocrypt '04*, vol. 3027 of *LNCS*, pp. 207–222. Springer, 2004.

[11] R. Canetti and S. Hohenberger. Chosen-ciphertext secure proxy re-encryption. In *CCS*, pp. 185–194. ACM, 2007.

[12] C.-K. Chu and W.-G. Tzeng. Identity-based proxy re-encryption without random oracles. In *ISC '07*, vol. 4779 of *LNCS*, pp. 189–202. Springer, 2007.

[13] R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. Comput.*, 33(1):167–226, January 2004.

[14] L. Ducas. Anonymity from asymmetry: new constructions for anonymous HIBE. In *CT-RSA '10*, vol. 5985 of *LNCS*, pp. 148–164. Springer, 2010.

[15] K. Emura, A. Miyaji, and K. Omote. An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system. In *EuroPKI '10*, vol. 6711 of *LNCS*, pp. 77–92. Springer, 2011.

[16] C.-I. Fan, L.-Y. Huang, and P.-H. Ho. Anonymous multireceiver identity-based encryption. *Computers, IEEE Transactions on*, 59(9):1239–1249, Sept 2010.

[17] M. Green and G. Ateniese. Identity-based proxy re-encryption. In *ACNS '07*, vol. 4512 of *LNCS*, pp. 288–306. Springer, 2007.

[18] A. Ivan and Y. Dodis. Proxy cryptography revisited. In *NDSS '03*, 2003.

[19] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie. A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing. *IEEE Transactions on Information Forensics and Security*, 9(10):1667–1680, 2014.

[20] K. Liang, M. H. Au, W. Susilo, D. S. Wong, G. Yang, and Y. Yu. An adaptively cca-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. In *ISPEC*, vol. 8434 of *LNCS*, pp. 448–461. Springer, 2014.

[21] K. Liang, C. Chu, X. Tan, D. S. Wong, C. Tang, and J. Zhou. Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. *Theor. Comput. Sci.*, 539:87–105, 2014.

[22] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo. An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing. In *ESORICS*, vol. 8712 of *LNCS*, pp. 257–272. Springer, 2014.

[23] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In *ICISC*, vol. 7839 of *LNCS*, pp. 231–246. Springer, 2012.

[24] B. Libert and D. Vergnaud. Unidirectional chosen-ciphertext secure proxy re-encryption. In *PKC '08*, vol. 4939 of *LNCS*, pp. 360–379. Springer, 2008.

[25] R. Lu, X. Lin, J. Shao, and K. Liang. Rcca-secure multi-use bidirectional proxy re-encryption with master secret security. In *ProvSec '14*, vol. 8782 of *LNCS*, pp. 194–205. Springer, 2014.

[26] M. Mambo and E. Okamoto. Proxy cryptosystems: Delegation of the power to decrypt ciphertexts. *IEICE Transactions*, E80-A(1):54–63, 1997.

[27] T. Matsuo. Proxy re-encryption systems for identity-based encryption. In *Pairing '07*, vol. 4575 of *LNCS*, pp. 247–267. Springer, 2007.

[28] T. Mizuno and H. Doi. Secure and efficient IBE-PKE proxy re-encryption. *IEICE Transactions*, E94-A(1):36–44, 2011.

[29] Y. Rao and R. Dutta. Recipient anonymous ciphertext-policy attribute based encryption. In *Information Systems Security*, vol. 8303 of *LNCS*, pages 329–344. Springer, 2013.

[30] J. Shao. Anonymous id-based proxy re-encryption. In *ACISP*, vol. 7372 of *LNCS*, pp. 364–375. Springer, 2012.

[31] J. Shao and Z. Cao. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity- based encryption. *Inform. Sci.*, 2012. http://dx.doi.org/10.1016/j.ins.2012.04.013.

[32] J. Shao, P. Liu, G. Wei, and Y. Ling. Anonymous proxy reencryption. *Security and Communication Networks*, 5(5):439–449, May 2012.

[33] J. Shao, P. Liu, and Y. Zhou. Achieving key privacy without losing CCA security in proxy re-encryption. *The Journal of Systems and Software*, 2011. http://doi:10.1016/j.jss.2011.09.034.

[34] Q. Tang, P. Hartel, and W. Jonker. Information security and cryptology. chapter Inter-domain Identity-Based Proxy Re-encryption, pages 332–347. Springer, 2009.

[35] B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT*, vol. 3494 of *LNCS*, pp. 114–127. Springer, 2005.

[36] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In *CRYPTO*, vol. 5677 of *LNCS*, pp. 619–636. Springer, 2009.

APPENDIX

A. Proof of Theorem 4

Proof: If an adversary $\mathcal{A}$ can break the IND-sConsID-CCA security of our scheme, we construct a reduction algorithm $\mathcal{B}$ to break the CCA security of 3-level Du-ANO-HIBE. Let $\mathcal{B}_1$ be the challenger of the 3-level Du-ANO-HIBE in the CCA experiment. $\mathcal{B}$ maintains the following tables.

1) DCT: records the tuples $(w|ID_i, ..., ID_j, tag)$, which are the delegation chains under condition w from ID_i to ID_j, where tag denotes that the chain is either uncorrupted ("1") or corrupted ("0"), $i, j \in \{1, ..., poly(1^k)\}$.
2) SKT: records the tuples (ID_i, sk_{ID_i}), which are the information of the secret keys (obtained in the simulation).
3) RKT: records the tuples $(ID_i,\ ID_{i'},\ w,\ rk_{w,ID_i \to ID_{i'}},\ \theta_1)$, which are the results of the queries to $\mathcal{O}_{rk}$, where tag denotes that the re-encryption key is either a valid key ("1") or a random key ("0").
4) RET: records the tuples $(ID_i,\ ID_{i'},\ w,\ C_{(l+1,ID_{i'},w)},\ tag)$, which are the results of the queries to $\mathcal{O}_{re}$, where tag denotes that the re-encrypted ciphertext is generated under a valid re-encryption key ("1"), a random key ("0") or generated without using any re-encryption key ("$\perp$").

1) **Init.** $\mathcal{A}$ outputs ID^* and w^* to $\mathcal{B}$, $\mathcal{B}$ then forwards them as well as a self-chosen K_v^{*2} to $\mathcal{B}_1$.
2) **Setup.** $\mathcal{B}_1$ sends $mpk = (g,\ \hat{g},\ g_1,\ h,\ f_1,\ f_2,\ f_3,\ t,\ \hat{g}_2,\ \hat{f}_2,\ \hat{f}_3,\ \hat{h},\ (Sig.KG,\ Sign,\ Ver))$ to $\mathcal{B}$. Then $\mathcal{B}$ chooses two TCR hash function H_1, H_2 and a CCA-secure one-time symmetric key encryption SYM as in the real scheme, adds them to mpk and forwards the resulting mpk to $\mathcal{A}$.
3) **Phase 1.** $\mathcal{A}$ issues a series of queries.
   a) $\mathcal{O}_{sk}(ID)$: if there is a tuple (ID, sk_{ID}) in SKT, $\mathcal{B}$ returns sk_{ID} to $\mathcal{A}$. Otherwise, $\mathcal{B}$ works as follows.
      - If $ID^* = ID$ or ID is in $(w^*|ID^*, ..., 1) \in DCT$ holds, $\mathcal{B}$ outputs $\perp$.
      - Otherwise, $\mathcal{B}$ forwards the query to the secret key extraction oracle of 3-level Du-ANO-HIBE, $\mathcal{O}_{extract}$, obtains the secret key and forwards the key to $\mathcal{A}$. Finally, $\mathcal{B}$ adds (ID, sk_{ID}) to SKT.
   b) $\mathcal{O}_{rk}(ID_i,\ ID_{i'},\ w)$: if there is a tuple $(ID_i,\ ID_{i'},\ w,\ rk_{w,ID_i \to ID_{i'}},\ \theta_1^{(l)},\ *)$ in RKT, $\mathcal{B}$ returns $rk_{w,ID_i \to ID_{i'}}$ to $\mathcal{A}$. Otherwise, $\mathcal{B}$ works as follows.
      - If $(ID^* = ID_i$ or ID_i in $(w^*|ID^*, ..., 1) \in DCT) \wedge ID_{i'}$ in $(w^*|*, ..., 0) \in DCT$ hold, then $\mathcal{B}$ outputs $\perp$, where $w^* = w$.
      - If $ID^* = ID_i \wedge ID_{i'}$ in $(w^*|*, ..., 1) \in DCT$ hold, $\mathcal{B}$ sets $rk_0^{(l)} = \sigma_1$, $rk_1^{(l)} = \sigma_2$, $rk_2^{(l)} = \sigma_3$, $rk_3^{(l)} = \sigma_4$, and constructs the rest of components as in the real scheme, where $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in_R \mathbb{G}_2$, $w^* = w$. $\mathcal{B}$ sends the re-encryption key to $\mathcal{A}$, and adds $(ID_i,\ ID_j,\ w,\ rk_{w,ID_i \to ID_{i'}},\ \theta_1^{(l)},\ 0)$ to RKT.
      - If $ID^* = ID_i \wedge w^* \neq w$ hold, $\mathcal{B}$ sends $ID = (ID^*, w)$ to $\mathcal{O}_{extract}$, and obtains sk_{ID} which are identical to $rk_0^{(l)H_1(\theta_1^{(l)})^{-1}}, rk_1^{(l)H_1(\theta_1^{(l)})^{-1}}$, $rk_2^{(l)H_1(\theta_1^{(l)})^{-1}}$ and $rk_3^{(l)H_1(\theta_1^{(l)})^{-1}}$. $\mathcal{B}$ then generates the rest of components of the re-encryption key as in the real scheme, and adds $(ID_i,\ ID_j,\ w,\ rk_{w,ID_i \to ID_{i'}},\ \theta_1^{(l)},\ 1)$ to RKT.
      - Otherwise, $\mathcal{B}$ queries ID_i to $\mathcal{O}_{extract}$ to obtain the secret key sk_{ID_i}, next generates the re-encryption key as in the real scheme and responds the key to $\mathcal{A}$, and finally adds (ID_i, sk_{ID_i}) and $(ID_i, ID_{i'}, w, rk_{w,ID_i \to ID_{i'}}, \theta_1^{(l)}, 1)$ to SKT and RKT, respectively, where $\theta_1^{(l)} \in_R \mathbb{G}_T$. Note if (ID_i, sk_{ID_i}) is in SKT, $\mathcal{B}$ uses sk_{ID_i} to generate the re-encryption key as in the real scheme.
   c) $\mathcal{O}_{re}(ID_i, ID_{i'}, w, C_{l,ID_i,w})$:
      - If the first case of step b) does not hold, $\mathcal{B}$ can first construct the re-encryption key as in step b) and then generate the re-encrypted ciphertext using the re-encryption key. Finally, $\mathcal{B}$ responds the ciphertext to $\mathcal{A}$ and adds $(ID_i,\ ID_j,\ w,\ rk_{w,ID_i \to ID_{i'}},\ \theta_1^{(l)},\ *)$ and $(ID_i,\ ID_{i'},\ w,\ C_{(l+1,ID_{i'},w)},\ *)$ to RKT and RET, respectively.
      - Otherwise
        i) If $l = 1$, $\mathcal{B}$ first verifies whether Eq. (1) holds. If not $\mathcal{B}$ outputs $\perp$. Otherwise, $\mathcal{B}$ queries $((ID_i, w, K_v), C_{1,ID_i,w}))$ to the decryption oracle of 3-level Du-ANO-HIBE, denoted as $\mathcal{O}_{decrypt}$, and obtains the underlying message. With knowledge of the message, $\mathcal{B}$ can recover the hiding factor $K_0 = e(g_1, \hat{g}_2)^{s_0}$. $\mathcal{B}$ further calculates $C_7^{(1)} = K_0^{H_1(\theta_1^{(1)})}$, constructs symmetric encryption $\sigma^{(1)}$ with $\theta_2^{(1)}$, generates the ciphertext $C_8^{(1)}, ..., C_{15}^{(1)}$ under $ID_{i'}$ to hide $\theta_2^{(1)}$ and the ciphertext $rk_4^{(1)}, ..., rk_{11}^{(1)}$ under $ID_{i'}$ to hide $\theta_1^{(1)}$ as in the real scheme, where $\theta_1^{(1)}, \theta_2^{(1)} \in_R \mathbb{G}_T$. Finally, $\mathcal{B}$ responds the re-encrypted ciphertext to $\mathcal{A}$ and adds $(ID_i,\ ID_{i'},\ w,\ C_{(2,ID_{i'},w)},\ \perp)$ to RET.
        ii) If $l \geq 2$, $\mathcal{B}$ first verifies whether Eq. (2) and Eq. (3) hold. If not $\mathcal{B}$ outputs $\perp$. Otherwise, $\mathcal{B}$ constructs the corresponding re-encrypted ciphertext in the identical method as above except that $C_{7,0}^{(l)}$, $C_{7,1}^{(l)}$ should be generated like the way of generating $C_7^{(1)}$.
        Note the queries issued by $\mathcal{A}$ should follow the restrictions defined in Definition 2.
   d) $\mathcal{O}_{dec}(ID_i, w, C_{l,ID_i,w})$: if $C_{l,ID_i,w}$ is a derivative of the challenge ciphertext, $\mathcal{B}$ outputs $\perp$. Since $\mathcal{B}$ can access to the decryption oracle $\mathcal{O}_{decrypt}$, then it can easily tell any derivative.
      - If $l = 1$, that is, $C_{1,ID_i,w}$ is the first level ciphertext without any re-encryption. $\mathcal{B}$ first verifies whether Eq. (1) holds. If not, $\mathcal{B}$ outputs $\perp$ and proceeds otherwise.
        i) If $(ID_i, sk_{ID_i}) \in SKT$, then $\mathcal{B}$ recovers m using sk_{ID_i} as in the real scheme.
        ii) Otherwise, $\mathcal{B}$ queries $((ID_i, w, K_v), C_{1,ID_i,w}))$

[2]Note this verification key will not be used in the query phases but in the challenge phase.

to $\mathcal{O}_{decrypt}$, and returns m.

- If $l \geq 2$, that is, $C_{l,ID_i,w}$ is the re-encrypted ciphertext. $\mathcal{B}$ first verifies whether Eq. (4) and Eq. (5) hold. If not, $\mathcal{B}$ outputs $\perp$ and proceeds otherwise.
  - i) If $w^* = w$ and $ID^* = ID_i$, $\mathcal{B}$ issues $ID = (ID^*, w^*, \bar{K}_v^{(l)})$ to $\mathcal{O}_{extract}$, and obtains sk_{ID}. $\mathcal{B}$ then recovers $\theta_1^{(l)}, \theta_2^{(l)}$ as in the algorithm Dec of 3-level Du-ANO-HIBE, and further recovers m as in the real scheme.
  - ii) Else, $\mathcal{B}$ forwards $(rk_4^{(l)}, ..., rk_{11}^{(l)})$ and $(C_8^{(l)}, ..., C_{15}^{(l)})$ to $\mathcal{O}_{decrypt}$ and then obtains $\theta_1^{(l)}, \theta_2^{(l)}$. $\mathcal{B}$ uses $\theta_1^{(l)}$ and $\theta_2^{(l)}$ to recover $\theta_1^{(i)}, \theta_2^{(i)}$ for $1 \leq i \leq l-1$ from $l-1$ to 1. Next, $\mathcal{B}$ recovers $(C_0, ..., C_7)$ by using $\theta_2^{(1)}$, computes K_0 with $\theta_1^{(1)}$, and finally recovers m as in the real scheme.
    Note $\mathcal{B}$ can recover $\theta_1^{(i)}, \theta_2^{(i)}$ on its own if $(ID_i, sk_{ID_i}) \in SKT$ for any $i, 1 \leq i \leq l$.

4) **Challenge.** $\mathcal{A}$ outputs m_0, m_1 and $\{ID_{i_j}\}_1^{j=l^*-1}$ to $\mathcal{B}$. $\mathcal{B}$ first generates the ciphertext $C_{l^*-1,ID_{i_{l^*-1}},w^*}$ for m_b as in the real scheme, where all re-encryption keys and the first level ciphertext C_{1,ID_{i_1},w^*} can be easily constructed with knowledge of $sk_{ID_{i_j}}$ (which can be obtained from $\mathcal{O}_{extract}$), and $b \in \{0,1\}$. $\mathcal{B}$ further chooses $(\theta_{1,0}^{(l^*)}, \theta_{1,1}^{(l^*)}), (\theta_{2,0}^{(l^*)}, \theta_{2,1}^{(l^*)}) \in_R \mathbb{G}_T$, and forwards them to $\mathcal{B}_1$. $\mathcal{B}_1$ returns $rk_4^{(l^*)}$, ..., $rk_{11}^{(l^*)}$ and $C_8^{(l^*)}$, ..., $C_{15}^{(l^*)}$ for $\theta_{1,\hat{b}}^{(l^*)}$ and $\theta_{2,\bar{b}}^{(l^*)}$, respectively, where $\hat{b}, \bar{b} \in \{0,1\}$. $\mathcal{B}$ then generates the re-encryption key $rk_{w^*,ID_{i_{l^*-1}} \to ID^*}$ components $rk_0^{(l^*)}, rk_1^{(l^*)}, rk_2^{(l^*)}, rk_3^{(l^*)}$ (with $\theta_{1,\hat{b}}^{(l^*)}$), and $C_{7,0}^{(l^*)}, C_{7,1}^{(l^*)}, \sigma^{(l^*)}$ (with $\theta_{2,\hat{b}}^{(l^*)}$) as in the real scheme. $\mathcal{B}$ finally returns C_{l^*,ID^*,w^*} to $\mathcal{A}$.
5) **Phase 2.** Same as in **Phase 1**.
6) **Guess.** $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs.

$\mathcal{B}$ chooses a challenge verification key K_v^* beforehand, and this verification key cannot be used in the simulations. Therefore, $\mathcal{B}$'s advantage is at least $\frac{\epsilon(q_{rk}+q_{re}+q_{dec})}{4q}$, and the running time of $\mathcal{B}$ is $O(time(\mathcal{A}))$, where q_{rk}, q_{re}, q_{dec} are the total numbers of re-encryption key extraction, re-encryption and decryption queries, respectively. ■

B. Proof of Theorem 5

Proof: In the game of Definition 2, an adversary $\mathcal{A}$ is allowed to gain access to the re-encryption keys $rk_{w,ID^* \to ID_{i'}}$ and $rk_{w,ID_{i'} \to ID_{i''}}$, where w is not the challenge condition, $ID_{i'}$ is honest and $ID_{i''}$ is corrupted by $\mathcal{A}$. Suppose our AMH-IBCPRE system is not collusion resistant, $\mathcal{A}$ can compromise the secret key $sk_{ID_{i'}}$ with knowledge of $sk_{ID_{i''}}$ and $rk_{w,ID_{i'} \to ID_{i''}}$. $\mathcal{A}$ further compromise sk_{ID^*} with knowledge of $sk_{ID_{i'}}$ and $rk_{w,ID^* \to ID_{i'}}$. Given the challenge ciphertext C_{l^*,ID^*,w^*}, the adversary $\mathcal{A}$ can easily retrieve the value of the bit b by using sk_{ID^*}. The IND-sCon-sID-CCA security fails here that contradicts our security notion. Therefore, the IND-sCon-sID-CCA security implies collusion resistance. ■

C. Proof of Theorem 6

Proof: If an adversary $\mathcal{A}$ can break the ANO-OC security of our scheme, we construct an algorithm $\mathcal{B}$ to solve the decisional $\mathcal{P}$-BDH problem by using $\mathcal{A}$.

- **Init.** Same as the proof of Theorem 4 except the followings. $\mathcal{A}$ outputs ID_0^* and ID_1^* to $\mathcal{B}$, and $\mathcal{B}$ forwards ID_b^* to $\mathcal{B}_1$, where $b \in \{0,1\}$.
- **Setup.** Same as the proof of Theorem 4.
- **Phase 1.** Same as the proof of Theorem 4.
- **Challenge.** When $\mathcal{A}$ decides that **Phase 2** is over, then it outputs m to $\mathcal{B}$. $\mathcal{B}$ chooses a random message m' fro message space, and sets $m_1 = m$, $m_0 = m'$. $\mathcal{B}$ next forwards m_0, m_1 to $\mathcal{B}_1$, obtains the ciphertext C_{1,ID_b^*,w^*} for $m_{\bar{b}}$ from $\mathcal{B}_1$, where $\bar{b} \in \{0,1\}$. Then $\mathcal{B}$ forwards C_{1,ID_b^*,w^*} to $\mathcal{A}$.
- **Phase 2.** Same as **Phase 1**.
- **Guess.** $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs.

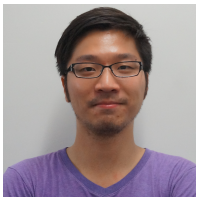
The probability analysis is the same as that of Theorem 4. Therefore, the advantage of $\mathcal{B}$ is at least $\frac{Adv_{\mathcal{A}}^{ANO\text{-}OC}(1^k)(q_{rk}+q_{re}+q_{dec})}{2q}$, and the running time of $\mathcal{B}$ is $O(time(\mathcal{A}))$. ■

D. Proof of Theorem 7

Proof: Supposing there is an adversary $\mathcal{A}$ who can break the ANO-RK security of our scheme, we can construct an algorithm $\mathcal{B}$ to solve the decisional $\mathcal{P}$-BDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$ by using $\mathcal{A}$.

- **Init.** Same as the proof of Theorem 4 except that $\mathcal{A}$ outputs ID', ID^* to $\mathcal{B}$, and $\mathcal{B}$ next forwards ID^* to $\mathcal{B}_1$.
- **Setup.** Same as the proof of Theorem 4.
- **Phase 1.** $\mathcal{A}$ is allowed to issue queries to the oracles $\mathcal{O}_{sk}$, $\mathcal{O}_{rk}$, $\mathcal{O}_{re}$, $\mathcal{O}_{dec}$ as in the **Phase 1** of the proof of Theorem 4.
- **Challenge.** When $\mathcal{A}$ decides that **Phase 1** is over, $\mathcal{B}$ flips a coin $b \in \{0,1\}$. If $b = 0$, $\mathcal{B}$ sets $rk_0^{(l)} = \sigma_1^{H_1(\theta_{1,\hat{b}}^{(l)})}$, $rk_1^{(l)} = \sigma_2^{H_1(\theta_{1,\hat{b}}^{(l)})}$, $rk_2^{(l)} = \sigma_3^{H_1(\theta_{1,\hat{b}}^{(l)})}$, $rk_3^{(l)} = \sigma_4^{H_1(\theta_{1,\hat{b}}^{(l)})}$, and issues $\theta_{1,0}^{(l)}, \theta_{1,1}^{(l)} \in_R \mathbb{G}_T$ to $\mathcal{B}_1$, where $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in_R \mathbb{G}_2$ and $\hat{b} \in \{0,1\}$. $\mathcal{B}_1$ returns $rk_4^{(l)}$, ..., $rk_{11}^{(l)}$ for $\theta_{1,\hat{b}}^{(l)}$. $\mathcal{B}$ next constructs the rest of re-encryption key's components (i.e. $rk_{12}^{(l)}$, ..., $rk_{18}^{(l)}$) as in the real scheme. That is, such a re-encryption key is a random key from the re-encryption key space. Otherwise, $\mathcal{B}$ constructs the re-encryption key $rk_{w^*,ID' \to ID^*}$ as above except that $rk_0^{(l)}, rk_1^{(l)}, rk_2^{(l)}, rk_3^{(l)}$ are constructed as in the real scheme with knowledge $sk_{ID'}$ which can be obtained from $\mathcal{O}_{extract}$. Finally, $\mathcal{B}$ responds $rk_{w^*,ID' \to ID^*}$ to $\mathcal{A}$.
- **Phase 2.** Same as **Phase 1**.
- **Guess.** $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs.

Similar to the analysis in the proof of Theorem 6, $\mathcal{B}$'s advantage is at least $\frac{Adv_{\mathcal{A}}^{ANO\text{-}RK}(1^k)(q_{rk}+q_{re}+q_{dec})}{2q}$, and the running time of $\mathcal{B}$ is $O(time(\mathcal{A}))$. ■



Kaitai Liang received the B.Eng. degree and the M.S. degree from South China Agricultural University, China. He received the Ph.D. degree in the Department of Computer Science, City University of Hong Kong (2014). He is currently a post-doctoral researcher at Department of Computer Science, Aalto university in Finland. His research interest is applied cryptography; in particular, cryptographic protocols, encryption/signature, and RFID. He is also interested in privacy enhanced technology, security of big data and Internet of Things.

Willy Susilo received the Ph.D. degree in computer science from the University of Wollongong, Wollongong, Australia. He is a Professor with the School of Computer Science and Software Engineering and the Director of Centre for Computer and Information Security Research, University of Wollongong. He has been awarded the prestigious ARC Future Fellow awarded by the Australian Research Council. His main research interests include cryptography and information security. He has served as a program committee member in major international conferences.

Joseph K. Liu received the Ph.D. degree in information engineering from the Chinese University of Hong Kong in July 2004, specializing in cyber security, protocols for securing wireless networks, privacy, authentication, and provable security. He is now a senior lecturer at Monash University, Australia. His current technical focus is particularly cyber security in the cloud computing paradigm, smart city, lightweight security, and privacy enhanced technology. He has published more than 80 referred journal and conference papers and received the Best Paper Award from ESORICS 2014. He has served as the program chair of ProvSec 2007, 2014, Pairing 2015, and as the program committee of more than 35 international conferences.