Controlled Secure Social Cloud Data Sharing Based on a Novel Identity Based Proxy Re-encryption Plus Scheme

Xu An Wang[1,2], Fatos Xhafa[3], Jianfeng Ma[2], Zhiheng Zheng[1]

[1]*Engineering University of Chinese Armed Police Force, P. R. China*
[2]*School of Cyber Engineering, Xidian University, P. R. China*
[3]*Department of Computer Science, Technical University of Catalonia, Spain*
wangxazjd@163.com,fatos@cs.upc.edu

Abstract

Currently we are witnessing a rapid integration of social networks and cloud computing, especially on storing social media contents on cloud storage due to its cheap management and easy accessing at any time and from any place. However, how to securely store and share social media contents such as pictures/videos among social groups is still a very challenging problem. In this paper, we try to tackle this problem by using a new cryptographic primitive: the identity based proxy re-encryption plus (IBPRE$^+$), which is a variant of proxy re-encryption (PRE). In PRE, by using re-encryption keys, a ciphertext computed for Alice can be transferred into a new one for Bob by a proxy. Recently, the concept of PRE plus (PRE$^+$) was introduced by Wang et al. In PRE$^+$, except the re-encryption keys are generated by the encrypter instead of the delegator, while other algorithms are almost the same as traditional PRE. The message-level based fine-grained delegation property and the weak non-transferable property can be easily achieved by PRE$^+$, while traditional PRE cannot achieve them. In this paper, the concept of PRE$^+$ is further extended to the identity based setting. Based on the 3-linear map, we first propose a new IBE scheme and a new IBPRE$^+$ scheme, we prove the security of these schemes and give the properties and performance analysis of the new IBPRE$^+$ scheme. Finally, we propose a new framework based on this new primitive for secure cloud social data sharing.

Keywords: Secure social cloud data sharing, Identity based encryption, Proxy re-encryption plus, Identity based proxy re-encryption plus, 3-linear map

1. Introduction

1.1. Social Network and Cloud Storage

Currently social networks have become commonplace in our daily life. Facebook, Twitter, Tenent etc. are huge companies focusing on social networks and their productions like QQ, Wechat, MSN for sharing photos and videos are used widely by large communities of users. Social networks can be seen as the map from real life community to the information network. Social groups as a typical feature in our social life, such as social groups of families, social groups of friends, social groups of interest, social group of workmates etc., is inherited by social networks. By connecting users and groups of users, social networks have become very huge and complex in managing the global community. Indeed, it is not easy to analyse the behaviour of this complex social community for information sharing.

Along with the rapid growth of social networks, very huge massive data sets are being generated instantly every day. For example, the Tencent company needs to store almost 5,000 billion instant messages created by the QQ users every day, and this data set increases 10% every month. The amount of these data sets can be as large as several TB/PBs every day. Thus, it is very natural to leverage cloud storage techniques to smoothly running these social networks. However, before using advanced cloud storage techniques, the user's concern on security should be taken into account. Actually there are incidents on leaking user's privacy from social cloud storage (various examples are being reported often by the press media, such as the well known case of Jennifer Lawrence's photos). Such incidents indicate that effective secure storing and sharing social data contents are very challenging problems. In this paper, aiming at tackling the user's data protection problems in social networks, we propose a framework for a controlled secure social data sharing based on a new primitive named Identity Based Proxy Re-encryption plus (IBPRE$^+$), which is a variant of proxy re-encryption technique.

1.2. Traditional IBPRE for Secure Social Cloud Storage Sharing

The concept of proxy re-encryption (PRE) was proposed by Blaze, Bleumer and Strauss [3] in 1998. In PRE, a ciphertext for Alice can be transformed into another ciphertext for Bob by a semi-trusted proxy. Furthermore anything about the underlying plaintext cannot be learned by the proxy. PRE schemes can be categorized as bidirectional and unidirectional according to the direction of transformation. By using the re-encryption key, if the proxy can transform ciphertexts from Alice to Bob and vice-versa, this kind of PRE scheme is called bidirectional. If the proxy can only transform ciphertext in one direction, this kind of PRE scheme is called unidirectional. If the ciphertext can be transformed from A to B and to C and so on, Blaze et al. [3] defined this kind of PRE scheme as multi-use one; if the ciphertext can be transformed only once, the PRE scheme is called as single-use one.

PRE has many applications, such as key escrow [24], distributed file systems [1, 2], simplification of key distribution [3], anonymous communication [10], multicast [9], cloud storage system [22, 41–43], and cloud computation [23, 25]. Recently, the research on cloud social data storage system is becoming more and more popular, which allows an enterprise to rent the cloud SaaS service to build a cheap and manageable storage system. It is much cheaper and scalable than traditional self-management solutions [26, 28–30]. Especially, Gai et al. have made lots of contribution on the hot topic of social media cloud storage, attack strategy combining spoofing and jamming, secure data transmission method for intelligent transportation system, fully homomorphic encryption [16–19, 21]. Attribute based encryption also has very important application to secure cloud storage. Yu et al. have contributed many interesting results in this area [45][44], however attribute based encryption (ABE) is different from proxy re-encryption (PRE) although they have the same property of fine-grained delegation on the decryption capability. ABE runs more like a one-to-many encryption paradigm, while one *encrypter* can communicate with different *decryptors*. Only the decryptors satisfy the access control formulae, the communication can be successful. PRE runs more like a one-to-one paradigm, the delegator shares his content to the delegatee. The advantage of PRE is that, the delegator and the delegatee do not need to change their own normal encryption algorithm, while PRE still has the ability of ciphertext transformation.

Identity based proxy re-encryption (IBPRE) is a kind of PRE scheme used in the identity based setting where the identity can be seen as the public key. In this paper, we focus on the cryptographic primitive of identity based proxy re-encryption. Fig. 1 represents the traditional identity based proxy re-encryption. Until now the generation of re-encryption key is generally determined by the delegator for almost all of the traditional IBPRE schemes. Concretely, the re-encryption key is generated by the delegator A in unidirectional IBPRE; and the key is generated by delegator A and the delegatee B together in bidirectional IBPRE.

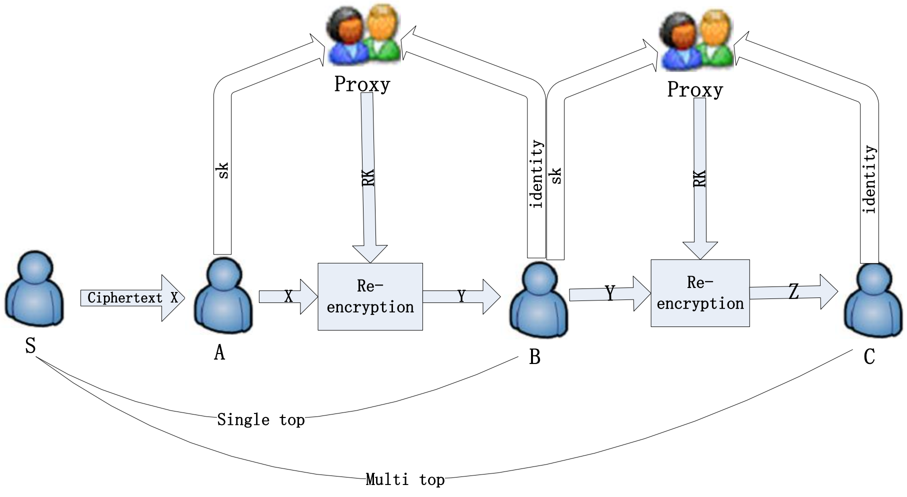

Figure 1: Traditional identity based proxy re-encryption scheme.

1.3. The Dilemma When Using Traditional IBPRE for Secure Social Cloud Data Sharing

When using traditional IBPRE for secure social cloud data sharing, there exists a dilemma which cannot be avoided. As Fig. 2 shows, data owner Alice first encrypts her private photos A/B and then outsources them to the cloud. Later, she want to share only the photo A with friend Bob by using traditional identity based proxy re-encryption. In this case, the cloud can transform the encrypted photos to be one encrypted with Bob's identity, and Bob can decrypt them to get Alice's photos. But the problem is that the cloud can implement the transformation on both photo A and photo B, while Alice only want to share photo A with Bob! This is due to the traditional IBPRE [11] only has the all-or-nothing transformation ability, although conditional IBPRE [23] can solve this problem partially, it cannot achieve the message-level based fine-grained delegation ability. In conditional or type based PRE [12–15], ciphertexts and re-encryption keys are associated with conditions, if and only if the delegator's ciphertexts satisfied with the conditions, these ciphertexts can be re-encrypted. Furthermore, the conditional re-encryption key inherits the all-or-nothing transformation ability from traditional re-encryption key. Here we give an example to demonstrate the situation.

Let us consider another scenario:

> *Suppose Alice has two group of videos, one group labelled with "family" and the other group labelled with "work" and she wants to share some videos to others. By delegating the cloud server conditional proxy re-encryption key with "family" or with "work", the cloud server can transform encrypted group of videos labelled with "family" from Alice to her husband, or it can transform encrypted group of videos labelled with "work" from Alice to her colleague. But note that the cloud server has the ability of implementing this transformation for the whole group of encrypted video, while sometimes Alice does not want to do so. Furthermore, the encryption of videos also*

needs to take "family" or "work" as the conditional input, which is not convenient to Alice.

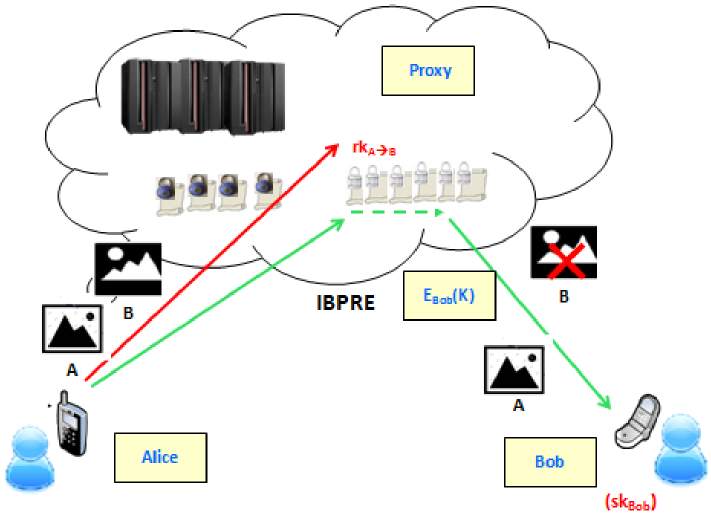

Figure 2: Data owner Alice cannot control which photo is shared with the delegatee.

1.4. New Primitive IBPRE$^+$ and Its Advantages

So how to avoid this dilemma? We use the new concept of proxy re-encryption plus (PRE$^+$) recently proposed by Wang et al. [32, 39]. In their scheme, the key is generated by the sender S. Concretely, the proxy re-encryption key is generated by using the randomness used in the encryption process. In this way the delegation granting process can be completely controlled by the sender S. Fig. 3 describes the idea of this new primitive.

In traditional identity based proxy re-encryption system, the re-encryption key is generated by A or A with B. So, A can decide whether to let B share the message sent by S, and B can let other users share the message further. But there is a concern in this process, namely, if A gives the data sharing capability to B and a proxy P, B can collude with P to get all the messages that S sends to A. Furthermore, B can grant the data sharing capability to the others. If so, the sender S cannot control which message to be learned by which person. To solve this problem, many condition-based proxy re-encryption schemes [33] were proposed, which aims to achieve a fine-grained delegation. But these schemes cannot overcome the shortcoming thoroughly. In this paper, we propose a new IBPRE$^+$ system. In our proposal, the people who can share the content of the encrypted messages can be completely controlled by the sender S.

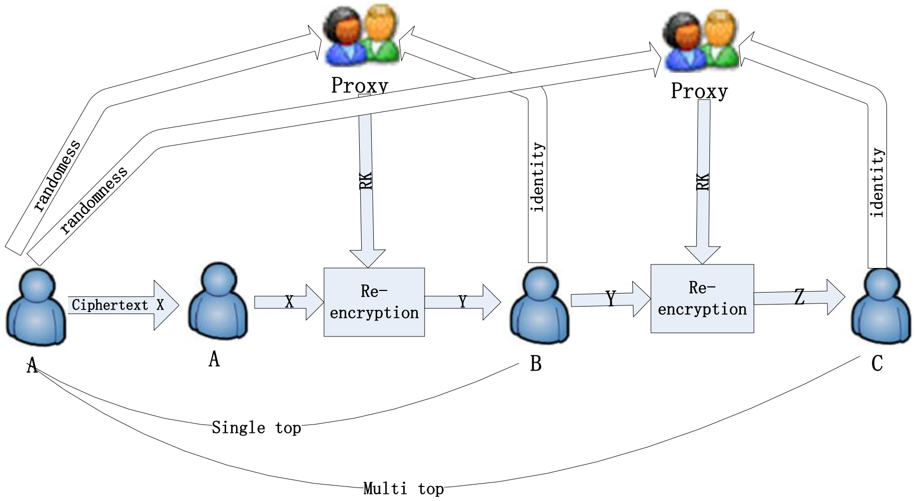

Figure 3: Identity based proxy re-encryption plus.

1.5. Our Contribution

In this paper, based on PRE$^+$ [39] and 3-linear map (3-linear map is a concrete instantiation of the recently proposed cryptographic primitive multi-linear map, which has been used in [34]), we propose a new IBPRE$^+$ scheme and analyse the proposal's security and property. To easily understand our IBPRE$^+$ scheme, the IBE scheme proposed by Boneh and Boyen [5] is first reviewed. Then, based on 3-linear map, we construct a new IBE scheme and a new IBE scheme with fixed randomness. Our IBPRE$^+$ scheme is constructed following these schemes. All these schemes have been proved secure by standard cryptographic techniques. Finally, we show how to use IBPRE$^+$ scheme to achieve flexible and secure social cloud data sharing. This paper is an extension of [40] but with significant extension, concretely we give the detailed definition and security model of IBE and IBPRE$^+$, formally prove the security of the new IBE scheme and new IBPRE$^+$ scheme, give the properties and performance analysis of our IBPRE$^+$ proposal, compare it with other related work, etc.

1.6. Organization

We give the definition and security model for IBE and IBPRE in section 2, we also give some mathematical tools and assumptions which are necessary to understand our work in this section. In section 3, we first review the BB1 IBE scheme; secondly we propose a new IBE scheme and another new IBE scheme with fixed randomness based on 3-linear map; then we give our IBPRE$^+$ proposal. In section 4, we prove the security of these schemes. In section 5, we give the properties and performance analysis of our IBPRE$^+$ scheme. In section 6 we demonstrate the application of our scheme in secure social cloud data sharing. In the last section 7, we conclude our paper.

2. Preliminaries

2.1. Definition and Security Model

2.1.1. Definition for IBE

We first recall the definition of IBE, which can be found in [4]:

1. **Setup(1^k).** This algorithm takes a security parameter as input, it outputs the private master key msk and the public parameters params.
2. **KeyGen(msk, params, ID).** This algorithm takes the master secret key msk and an identity $ID \in \{0,1\}^*$ as input, it outputs the private key sk_{ID} .
3. **Encrypt(ID, params, m).** This algorithm takes an identity $ID \in \{0,1\}^*$, a set of public parameters and a plaintext $m \in M$ as input, it outputs the ciphertext C_{ID}.
4. **Decrypt(sk_{ID}, params, C_{ID}).** This algorithm takes the ciphertext C_{ID}, params, and the secret key sk_{ID} as input, it outputs m or $\perp$.

2.1.2. Security Model for IBE

We recall the $\mathsf{IND\text{-}sID\text{-}CPA}$ security in [5, 6], it is defined by using the following game:

1. **Init:** The adversary selects the target identity ID^* which it wishes to be challenged.
2. **Setup:** The Setup algorithm is run by the challenger. The resulting system parameters params are given to the adversary and the master key is kept by itself.
3. **Phase1:** $q_1 \cdots q_m$ are issued by the adversary where q_i is one of private key queries on ID_i ($ID_i \neq ID^*$). By running algorithm KeyGen, the private key d_i is generated and responded to the adversary by the challenger. Note here each query q_i may depend on the replies to $q_1, \cdots, q_{i-1}$, these queries maybe asked adaptively.
4. **Challenge:** The adversary outputs two equal length plaintexts $M_0, M_1 \in \mathsf{M}$, once it decides that $\mathsf{Phase1}$ is over, on which it wishes to be challenged. The challenger sets the challenge ciphertext to be $\mathsf{C} = \mathsf{Encryption}(\mathsf{params}, \mathsf{ID}^*, \mathsf{M_b})$ where $b \in \{0, 1\}$ and sends it to the adversary.
5. **Phase2:** Additional queries $q_{m+1} \cdots q_n$ are issued by the adversary where q_i is one of private key queries on ID_i ($ID_i \neq ID^*$). The challenger just handles as in $\mathsf{Phase1}$. Note these queries maybe asked adaptively as in $\mathsf{Phase1}$.
6. **Guess:** Finally, a guess $b' \in \{0, 1\}$ is outputted by the adversary. The adversary wins if $b = b'$.

Such an adversary $\mathcal{A}$ refer to as an $\mathsf{IND\text{-}sID\text{-}CPA}$ adversary. The advantage of the adversary $\mathcal{A}$ in attacking the scheme $\mathcal{E}$ is

$$Adv_{\mathcal{E},\mathcal{A}} = \mid Pr[b = b'] - \frac{1}{2} \mid$$

The probability is over the random bits used by the adversary and the challenger. We say scheme $\mathcal{E}$ is $\mathsf{IND\text{-}sID\text{-}CPA}$ secure if this probability is negligible.

2.1.3. Definition for IBPRE$^+$

Based on the definition of PRE$^+$ [32, 39], we give our definition of IBPRE$^+$:

1. **Setup(1^k).** This algorithm is given a security parameter as input, it outputs both the master public parameters *params* and the master key *msk*, while the former are distributed to users, and the latter is kept private.
2. **KeyGen(params, msk, ID).** This algorithm is given an identity $ID \in \{0,1\}^*$ and the master secret key *msk* as input, it outputs that identity's decryption key sk_{ID}.
3. **Encrypt(params, ID, r, r', m).** This algorithm is given a set of public parameters, an identity $ID \in \{0,1\}^*$, a fixed ephemeral randomness r and a plaintext $m \in M$ as input, it outputs a second level ciphertext C_{ID}. Note this ciphertext can be probabilistic generated by using other non-fixed ephemeral randomness r', and it can be further re-encrypted by the proxy.
4. **ReKeyGen(params, r, ID_1, ID_2).** This algorithm is given the fixed ephemeral randomness r for ID_1, and identity $ID_2 \in \{0,1\}^*$ as input, the encrypter non-interactively generates the re-encryption key $rk_{ID_1 \to ID_2}$ and outputs it.
5. **Reencrypt(params, $rk_{ID_1 \to ID_2}$, C_{ID_1}).** This algorithm is given a second level ciphertext C_{ID_1} under identity ID_1, and a re-encryption key $rk_{ID_1 \to ID_2}$ as input, it outputs a first level re-encrypted ciphertext C_{ID_2}.
6. **Decrypt$_2$(params, sk_{ID}, C_{ID}).** This algorithm is given a second level ciphertext C_{ID} under identity ID with secret key sk_{ID} as input, it decrypts the ciphertext C_{ID} and outputs m or $\perp$.
7. **Decrypt$_1$(params, sk_{ID}, C_{ID}).** This algorithm is given a first level re-encrypted ciphertext C_{ID} under identity ID with secret key sk_{ID} as input, it decrypts the re-encrypted ciphertext C_{ID} and outputs m or $\perp$.

Correctness: If the expected decryption of a properly generated ciphertex is always outputted by the Decrypt algorithm, we call the IBPRE$^+$ scheme correct.

Formally, if $c_{ID_1} \leftarrow Encrypt(params, ID_1, r, m)$ then $\forall m \in \mathcal{M}, \forall ID_1, ID_2 \in \{0,1\}^*$, where $sk_{ID_1} = KeyGen(msk, ID_1), sk_{ID_2} = KeyGen(msk, ID_2), rk_{ID_1 \to ID_2} \leftarrow ReKeyGen(param,$
$r, ID_1, ID_2)$ the following always holds:

- $Decrypt(params, sk_{ID_1}, c_{ID_1}) = m$
- $Decrypt(params, sk_{ID_2}, Reencrypt(params, rk_{ID_1 \to ID_2}, c_{ID_1})) = m$

Remark 1. *In the* Encrypt *algorithm, fixed ephemeral randomness r is critical for the re-encryption key generation. r can be reused for encryption of different plaintexts. In some cases, other non-fixed ephemeral randomness r' can be used for encryption, but this r' can not be reused for encryption of different plaintexts. The encryptor can achieve message-level fine-grained delegation and the weak non-transferable property.*

2.1.4. IND-sID-CPA Security for Second Level Ciphertext of IBPRE$^+$

IND-sID-CPA security for the second level ciphertext is defined as following:

1. Setup. The challenger runs $\mathsf{Setup}(1^k)$ and gets $(params, msk)$, sends $params$ to $\mathcal{A}$. Here we define extract oracle $O_{extract}$ as the key generation oracle, $O_{rkextract}$ as the re-encryption key extract oracle, $O_{reencrypt}$ as the re-encrypt oracle.
2. Find phase. The following queries are made by $\mathcal{A}$. At the beginning of this phase $\mathcal{A}$ will select $ID^* \in \{0,1\}^*$ as the target identity, it also selects randomly $(m_0, m_1) \in \mathcal{M}^2$.
   (a) For $\mathcal{A}$'s queries to extract oracle $O_{extract}$ with $(extract, ID)$, return $sk_{ID} = KeyGen(params, msk, ID)$ to $\mathcal{A}$.
   (b) For $\mathcal{A}$'s queries to re-encryption key extract oracle $O_{rkextract}$ with $(rkextract, ID_1, ID_2)$, where $ID_1 \neq ID_2$, return $rk_{ID_1 \to ID_2} = ReKeygen$ $(params, r, ID_2)$ which is indistinguishable with the real correct re-encryption key to $\mathcal{A}$, where r is a randomly chosen randomess for

encryption. Note here only the encrypter can generate the correct re-encryption key, and any other can not generate this, thus the oracle returns a simulated indistinguishable re-encryption key for $\mathcal{A}$. And this does not help $\mathcal{A}$ to distinguish the simulated environment from the real environment, for in the real environment the re-encryption with incorrect re-encrypt key also cause the delegatee's unsuccessful decrypt.

(c) For $\mathcal{A}$'s queries to re-encrypt oracle $O_{reencrypt}$ with $(reencrypt, ID_1, ID_2, C)$, derive a re-encryption key $rk_{ID_1 \to ID_2}$ as above, and return $C' = Reencrypt(params, rk_{ID_1 \to ID_2}, ID_1, ID_2, C)$ to $\mathcal{A}$.

Note that ID^* such that trivial decryption is possible using keys extracted during this phase is not permitted by $\mathcal{A}$ to choose (e.g. translate from ID^* to some identity for which $\mathcal{A}$ holds a decryption key by using extracted re-encryption keys).

3. Choice and Challenge. When $(choice, ID^*, m_0, m_1)$ is presented by $\mathcal{A}$, the challenger chooses $i \leftarrow_R \{0,1\}$, computes $C^* = Encrypt(params, ID^*, m_i)$ and gives C^* to $\mathcal{A}$.

4. Guess stage. As in the find stage $\mathcal{A}$ continues to make queries. Let $\mathcal{C}$ $= (C^*, ID^*)$. Let $\mathcal{C}'$ be the set of all possible values derived via calls to Reencrypt oracle, for all rk given to $\mathcal{A}$, e.g. on successful execution of re-encrypt query $(reencrypt, ID^*, ID', C^*)$, let C' be the result and add the pair (C', ID') to the set $\mathcal{C}'$. Derivative of (C^*, ID^*) is defined as $\mathcal{C} \cup \mathcal{C}')$.

   (a) any queries $(extract, ID)$ to extract oracle $O_{extract}$ or $(rkextract, ID_1, ID_2)$ to re-encryption key extract oracle $O_{rkextract}$ that would permit trivial decryption of any ciphertext in (C, C') is not permitted to be issued by $\mathcal{A}$.

   (b) any query of the form $(reencrypt, ID_1, ID_2, C)$ to re-encrypt oracle $O_{reencrypt}$ where $\mathcal{A}$ possesses the keys to trivially decrypt ciphertexts under ID_2 and $(C, ID_1) \in (\mathcal{C} \cap \mathcal{C}')$ is not not permitted to be issued by $\mathcal{A}$.

At the conclusion of this stage, $\mathcal{A}$ outputs i', where $i' \in \{0, 1\}$.

If $i' = i$ then $\mathcal{A}$ wins the game. Let $Adv_{\mathcal{A}} = \mid Pr(i' = i) - 1/2 \mid$. we say that the IBPRE$^+$ scheme $\mathcal{S}$ is IND-sID-CPA secure for the second level ciphertext, if for all probabilistic polynomial time algorithms $\mathcal{A}$, $Adv_{\mathcal{A}}$ is negligible.

2.1.5. IND-sID-CPA Security for First Level Ciphertext of IBPRE$^+$

IND-sID-CPA Security for the first level ciphertext is defined as the following:

1. Setup. The challenger runs $\mathsf{Setup}(1^k)$ and gets $(params, msk)$, sends $params$ to $\mathcal{A}$. Here we define extract oracle $O_{extract}$ as the key generation oracle, $O_{rkextract}$ as the re-encryption key extract oracle, $O_{reencrypt}$ as the re-encrypt oracle.
2. Find phase. The following queries are made by $\mathcal{A}$. At the beginning of this phase $(ID^{\star}, ID^{*}) \in \{0, 1\}^*$ as the target identity pair will be selected by $\mathcal{A}$, it also selects randomly $(m_0, m_1) \in \mathcal{M}^2$.
   (a) Return sk_{ID} =KeyGen(params, msk, ID) to $\mathcal{A}$, for $\mathcal{A}$'s queries to extract oracle $O_{extract}$ with $(extract, ID)$.
   (b) This oracle handles as the above game 2.1.4, for $\mathcal{A}$'s queries to re-encryption key extract oracle $O_{rkextract}$ with $(rkextract, ID_1, ID_2)$.

   Note here that all the extracted re-encryption keys including ID^* to some identity for which $\mathcal{A}$ holds a decryption key is permitted to be given to $\mathcal{A}$. Also note here that the re-encrypt oracle is useless, he can do all the re-encryption and transform the second level ciphertext to the first level ciphertext since $\mathcal{A}$ knows all the re-encryption key.
3. Choice and Challenge. When $(choice, ID^{\star}, ID^{*}, m_0, m_1)$ is presented by $\mathcal{A}$, choose $i \leftarrow_R \{0, 1\}$, compute $C^{\star} = Encrypt(params, ID^{*}, m_i)$ and $C^{*} = Reencrypt$
   $(params, rk_{ID^{*} \to ID^{\star}}, ID^{\star}, ID^{*}, C^{\star})$ give $C^{\star}$ to $\mathcal{A}$.
4. Guess stage. $\mathcal{A}$ continues to make queries as in the find stage, with the following restrictions.

(a) Any queries $(extract, ID^{\star})$ or $(extract, ID^{*})$ to extract oracle $O_{extract}$ is not permitted to be issued by $\mathcal{A}$.

$\mathcal{A}$ outputs i', where $i' \in \{0,1\}$ at the conclusion of this stage.

If $i' = i$ then $\mathcal{A}$ wins the game. Let $Adv_{\mathcal{A}}$=$\mid Pr(i' = i) - 1/2 \mid$. If $Adv_{\mathcal{A}}$ is negligible for all probabilistic polynomial time algorithms $\mathcal{A}$, we say that the IBPRE^{+} scheme is IND-ID-CPA secure for the first level ciphertext.

Remark 2. *In this security notion, we give the target identity pair $(ID^{*}, ID^{\star})$ for our re-encryption does not randomize the second level ciphertext. From the re-encrypted first level ciphertext, anyone can trivially derive its second level ciphertext. So we restricted this trivial attack in our security model game.*

2.1.6. Master Secret Security for IBPRE^{+}

$$\begin{aligned} Pr[sk_{ID^{\star}} \leftarrow O_{extract}(ID^{\star}), \\ sk_{ID_x} \leftarrow O_{extract}(ID_x)\}, \\ \{R_{ID^{\star}\rightarrow ID_x} \leftarrow O_{rkextract}(ID^{\star}, r, ID_x)\}, \\ \{R_{ID_x\rightarrow ID^{\star}} \leftarrow O_{rkextract}(ID_x, r', ID^{\star})\}, \\ \gamma \leftarrow \mathcal{A}(ID^{\star}, \{ID_x, sk_{ID_x}\}, \\ \{R_{ID^{\star}\rightarrow ID_x}\}, \{R_{ID_x\rightarrow ID^{\star}}\}) : \gamma = sk_{ID^{\star}}] \end{aligned}$$

The definition on master secret security of PRE[20] by Libert and Vergnaud is extended by us to IBPRE^{+}, which requires that no coalition of dishonest delegatees be able to pool their re-encryption keys in order to expose the private key of their common delegator. The above probability should be negligible as a function of the security parameter. λ[1]

[1] Notations: $(ID^{\star}$, $sk_{ID^{\star}})$ denotes the target user's identity and private key, $(ID_x$, $sk_{ID_x})$ denotes the colluding user's identity and private key.

2.2. Mathematical Tool and Assumption

In this subsection, we give the mathematical tool and assumption which are necessary to understand our schemes.

2.2.1. Leveled Multilinear Map

Cryptographic multilinear maps are introduced by Boneh and Silverberg [7] in 2003, which recently received great attention from cryptographic community since Garg, Gentry, and Halevi [27] gave the plausible construction in 2013. We define generic leveled multilinear maps following the definition of Garg, Gentry, and Halevi [27].

Definition 1. *(Leveled Multilinear Maps). Assume a group generator $\mathcal{G}$ exists, which takes as input a security parameter λ and a positive integer k as input. Let $\bar{\mathbb{G}} = (\mathbb{G}_1, \cdots, \mathbb{G}_k)$ be a sequence of groups with large prime order $p \geq 2^{\lambda}$. In addition, canonical generators of $\mathbb{G}_i$ are $g_{i1}, g_{i2}, \cdots, g_{ik}$ respectively. A set of bilinear maps $\{e_{i,j} : \mathbb{G}_i \times \mathbb{G}_j \to \mathbb{G}_{i+j} | i, j \geq 1; i + j \leq k\}$ that have the following properties exists:*

- *(Bilinearity) The map $e_{i,j}$ satisfies the following relation: $\forall a, b \in Z_p$,*

  $$e_{i,j}(g_{ik}^a, g_{js}^b) = g_{(i+j|t)}^{ab}$$

  where k, s, t have no explicit algebraic relationship, just for denoting the different generators of different leveled groups.

- *(Non-degenerate) We have that $e_{i,j}(g_{ik}, g_{js}) = g_{i+j|t}$ for each valid i, j where k, s, t have no explicit algebraic relationship, just for denoting the different generators of different leveled groups.*

If the group operations in $\bar{G}$ as well as all bilinear maps are efficiently computable, we say that $\bar{G}$ is a multilinear group. We often omit the subscripts of $e_{i,j}$ and just write e.

Remark 3. *Although there are now many works on the insecurity of the proposed levelled multilinear map [36, 37], we think it is still valuable to construct* *schemes based on multilinear map to demonstrate the novelty of some new concepts, and finally guide us to some construction without multilinear map.*

2.2.2. 3-linear Maps

In our scheme, we only need to use 3-leveled multilinear maps, we denote them as 3-linear maps. The structure of our 3-linear map groups can be seen in Fig 4. Concretely they are the following: let (G_1, G_2, G_3) be 3-linear groups of prime order p, and let g be a generator of $\mathbb{G}_1$. In addition, let $e_{a,b} : \mathbb{G}_a \times \mathbb{G}_b \rightarrow \mathbb{G}_{a+b}(a + b \leq 3)$ denote the 3-linear map. Given a security parameter 1^k as input, select a random generator g_{11} and $h_{11}, g_{12} \in G_1$. Pick $\alpha \in Z_p^*$ and set $g_{13} = g_{11}^{\alpha}$. Let $e_{11}(g_{12}, g_{13}) = g_{21}, e_{21}(g_{21}, g_{11}) = g_{31}$.

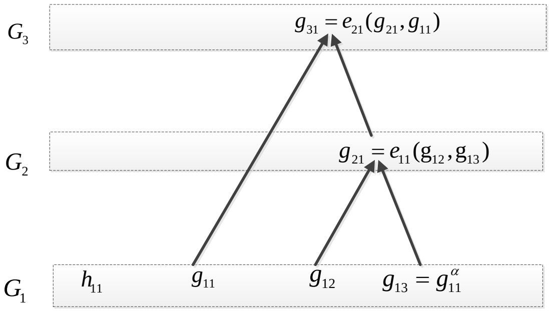
G_3
$g_{31} = e_{21}(g_{21}, g_{11})$
G_2
$g_{21} = e_{11}(g_{12}, g_{13})$
G_1
h_{11}
g_{11}
g_{12}
$g_{13} = g_{11}^{\alpha}$

Figure 4: The structure of 3-linear groups

2.2.3. D3DH Assumption

We give an assumption named Decisional 3-linear Diffie-Hellman(D3DH) hard problem just like DBDH hard problem as following:

Definition 2. *It is difficult to distinguish* $(g_{11}, g_{11}^a, g_{11}^b, g_{11}^c, g_{11}^d, e(g_{11}, g_{11}, g_{11})^{abcd})$ *from* $(g_{11}, g_{11}^a, g_{11}^b, g_{11}^c, g_{11}^d, T)$ *where* T *is randomly chosen from* $\mathbb{G}_3$ *for any algorithms running in polynomial time in 3-linear map groups. Note here we denotes* e *as the general 3-linear map which omits the footnote on describing the level of map for easily understanding.*

It is easy to derive the hardness of D3DH problem which is a natural extension of DBDH hard problem. In 3-linear map groups, anyone can compute from

$g_{11}^a, g_{11}^b, g_{11}^c, g_{11}^d$ to get $e(g_{11}, g_{11}, g_{11})^{abc}$ or $e(g_{11}, g_{11}, g_{11})^{abd}$ or $e(g_{11}, g_{11}, g_{11})^{bcd}$ by using 3-linear map, but it is difficult to get $e(g_{11}, g_{11}, g_{11})^{abcd}$. This is just like in bilinear map groups, anyone can compute from g^a, g^b, g^c to get $e(g,g)^{ab}$ or $e(g,g)^{bc}$ or $e(g,g)^{ac}$, but it is difficult to get $e(g,g)^{abc}$.

3. Our Proposed IBE and IBPRE$^+$ Schemes with Fixed Randomness Based on 3-linear Map

In this section, we first review the BB1 IBE scheme, and then give a new IBE scheme and a new IBE scheme with fixed randomness based on 3-linear map, finally we give new IBPRE$^+$ scheme with fixed randomness based on 3-linear map.

3.1. Review of the BB1 IBE Scheme

1. $\mathsf{SetUp}(1^k)$. Let G, G_T be a bilinear group of prime order p, and the bilinear map be $e : G \times G \rightarrow G_T$. A security parameter 1^k is given as input, this algorithm select random generators g and $h, g_2 \in G$. Pick $\alpha \in Z_p^*$ and set $g_1 = g^\alpha$.
$$MK = \alpha, Pub = (g, g_1, g_2, h)$$
Let Pub be the public parameters, and MK be the master secret key.
2. $\mathsf{KeyGen}(MK, Pub, ID)$. Given public parameters Pub, master secret key $MK = \alpha$ and an identity ID as input, the PKG picks $u \in Z_p^*$ and outputs an IBE secret key
$$SK = (sk_1, sk_2) = (g_2^\alpha (g_1^{ID} h)^u, g^u)$$
3. $\mathsf{Encrypt}(ID, Pub, M)$. Given plaintext $M \in G_T$, an identity ID and public parameter Pub as input, select $w \in Z_p^*$ and output an IBE ciphertext C
$$C = (C_1, C_2, C_3) = (g^\omega, (g_1^{ID} h)^\omega, Me(g_1, g_2)^\omega)$$
4. $\mathsf{Decrypt}(SK, Pub, C)$. Given public parameters Pub, an IBE ciphertext C_I and an IBE secret key SK as input, output a plaintext M.
$$M = \frac{C_3 e(sk_2, C_2)}{e(sk_1, C_1)}$$

3.2. New IBE Scheme Based on 3-linear Map

1. $\mathsf{SetUp}(1^k)$. Let (G_1, G_2, G_3) be 3-linear groups of prime order p, and let g be a generator of $\mathbb{G}_1$. In addition, denote the 3-linear map as $e_{a,b} : \mathbb{G}_a \times \mathbb{G}_b \to \mathbb{G}_{a+b}(a+b \leq 3)$. Taken a security parameter 1^k as input, select random generators g_{11} and $h_{11}, g_{12} \in G_1$. Pick $\alpha \in Z_p^*$ and set $g_{13} = g_{11}^{\alpha}$. Let $e_{11}(g_{12}, g_{13}) = g_{21}, e_{21}(g_{21}, g_{11}) = g_{31}$.

$$MK = \alpha, Pub = (g_{11}, g_{12}, g_{13}, h_{11}, g_{21}, g_{31})$$

Let Pub be the public parameters and MK be a master secret key.

2. $\mathsf{KeyGen}(MK, Pub, ID)$. Given public parameters Pub, an identity ID, and master secret key $MK = \alpha$ as input, the PKG picks $u \in Z_p^*$ and outputs an IBE secret key as

$$SK = (sk_1, sk_2) = (g_{12}^{\alpha}(g_{13}^{ID}h_{11})^u, g_{11}^u)$$

3. $\mathsf{Encrypt}(ID, Pub, M)$. Given plaintext $M \in G_T$, an identity ID, public parameter Pub as input, select $w \in Z_p^*$ and output an IBE ciphertext C

$$\begin{aligned} &C = (C_1, C_2, C_3, C_4) \\ &= (g_{11}^{\omega}, (g_{13}^{ID}h_{11})^{\omega}, Mg_{31}^{\omega t}, g_{11}^t) \end{aligned}$$

4. $\mathsf{Decrypt}(SK, Pub, C)$. Given public parameters Pub, an IBE ciphertext C_I and an IBE secret key SK as input, output a plaintext M.

$$\begin{aligned} &M = \frac{C_3}{A}, A = e_{21}(\frac{e(sk_2, C_2)}{e(sk_1, C_1)}, C_4) \\ &= e_{21}(e_{11}(g_{12}, g_{13})^{\omega}, g_{11}^t) = e_{21}(g_{21}^{\omega}, g_{11}^t) \\ &= g_{31}^{\omega t} \end{aligned}$$

3.3. New IBE Scheme with Fixed Randomness Based on 3-linear Map

1. $\mathsf{SetUp}(1^k)$. Let (G_1, G_2, G_3) be 3-linear groups of prime order p, and let $\mathbb{G}_1$'s a generator be g. In addition, let $e_{a,b} : \mathbb{G}_a \times \mathbb{G}_b \to \mathbb{G}_{a+b}(a+b \leq 3)$ denotes the 3-linear map. Given a security parameter 1^k as input, select

random generators g_{11} and $h_{11}, g_{12} \in G_1$. Pick $\alpha \in Z_p^*$ and set $g_{13} = g_{11}^{\alpha}$. Let $e_{11}(g_{12}, g_{13}) = g_{21}, e_{21}(g_{21}, g_{11}) = g_{31}$.

$$MK = \alpha, Pub = (g_{11}, g_{12}, g_{13}, h_{11}, g_{21}, g_{31})$$

Let MK be a master secret key, and Pub be the public parameters.

2. $\mathsf{KeyGen}(MK, Pub, ID)$. Given an identity ID, master secret key $MK = \alpha$ and public parameters Pub as input, the PKG picks $u \in Z_p^*$ and outputs an IBE secret key as

$$SK = (sk_1, sk_2) = (g_{12}^{\alpha}(g_{13}^{ID} h_{11})^u, g_{11}^u)$$

3. $\mathsf{Encrypt}(ID, Pub, M)$. Given plaintext $M \in G_T$, an identity ID and public parameter Pub as input, select a fixed random number $r \in Z_p^*$ and a random number $w \in Z_p^*$ and output an IBE ciphertext C

$$\begin{aligned} C &= (C_1, C_2, C_3, C_4) \\ &= (g_{11}^{r\omega}, (g_{13}^{ID} h_{11})^{r\omega}, M g_{31}^{r\omega t}, g_{11}^{t}) \end{aligned}$$

4. $\mathsf{Decrypt}(SK, Pub, C)$. Given an IBE ciphertext C, an IBE secret key SK and public parameters Pub as input, output a plaintext M.

$$\begin{aligned} M &= \frac{C_3}{A}, A = e_{21}(\frac{e(sk_2, C_2)}{e(sk_1, C_1)}, C_4) \\ &= e_{21}(e_{11}(g_{12}, g_{13})^{r\omega}, g_{11}^{t}) \\ &= e_{21}(g_{21}^{r\omega}, g_{11}^{t}) = g_{31}^{r\omega t} \end{aligned}$$

3.4. New IBPRE$^+$ Scheme with Fixed Randomness Scheme Based on 3-linear Map

1. $\mathsf{SetUp}(1^k)$. Let (G_1, G_2, G_3) be 3-linear groups of prime order p, and let g be a generator of $\mathbb{G}_1$. In addition, let the 3-linear map be $e_{a,b} : \mathbb{G}_a \times \mathbb{G}_b \to \mathbb{G}_{a+b} (a + b \leq 3)$. Given a security parameter 1^k as input, select random generators g_{11} and $h_{11}, g_{12} \in G_1$. Pick $\alpha \in Z_p^*$ and set $g_{13} = g_{11}^{\alpha}$. Let $e_{11}(g_{12}, g_{13}) = g_{21}, e_{21}(g_{21}, g_{11}) = g_{31}$.

$$MK = \alpha, Pub = (g_{11}, g_{12}, g_{13}, h_{11}, g_{21}, g_{31})$$

Let Pub be the public parameters and MK be a master secret key.

2. KeyGen(MK, Pub, ID_1). Given public parameters Pub, master secret key $MK = \alpha$ and an identity ID_1 as input, the PKG picks $u \in Z_p^*$ and output an IBE secret key

$$SK_{ID_1} = (sk_1, sk_2) = (g_{12}^{\alpha}(g_{13}^{ID_1} h_{11})^u, g_{11}^u)$$

3. Encrypt(ID_1, Pub, M). Given plaintext $M \in G_T$, an identity ID_1 and public parameter Pub as input, select a fixed random number $r \in Z_p^*$ and a random number $w \in Z_p^*$ and output an IBE ciphertext C

$$C = (C_1, C_2, C_3, C_4, C_5) = (g_{11}^{r\omega}, (g_{13}^{ID_1} h_{11})^{r\omega}, M g_{31}^{r\omega t}, g_{11}^t, g_{12}^{\omega t})$$

We can see the encrypter can decrypt the ciphertext by using g_{11}^r and computing $e_{21}(e_{11}(C_5, g_{13}), g_{11}^r) = e_{21}(g_{21}^{\omega t}, g_{11}^r) = g_{31}^{r\omega t}$.

4. ReKeyGen(Pub, r, ID_1, ID_2). On input public parameter Pub, the encrypter's fixed randomness r for ID_1, the delegator's identity ID_1, delegatee's identity ID_2, the encrypter generates the re-encryption key as following:

$$rk_{ID_1 \to ID_2} = (rk_1, rk_2, rk_3) = (g_{11}^{-r} H(X)^y, g_{13}^y, IBE_{ID_2}(X))$$

where $H : \{0,1\}^* \to G_1$ is a map to point hash function.

5. Reencrypt$(Pub, C, rk_{ID_1 \to ID_2}, ID_1, ID_2)$. On input the re-encryption key and the delegator's second level ciphertext, the proxy does the following:

$$\begin{aligned} C' &= (C'_1, C'_2, C'_3, C'_4) = (C_3 e_{21}(e_{11}(C_5, rk_1), g_{13}), rk_2, C_5, IBE_{ID_2}(X)) \\ &= (Me(H(X)^y, g_{12}^{\omega t}, g_{13}), g_{13}^y, g_{12}^{\omega t}, IBE_{ID_2}(X)) \end{aligned}$$

6. Decrypt2(SK_{ID_1}, Pub, C). Given public parameters Pub, an IBE secret key SK and an IBE ciphertext C as input, output a plaintext M.

$$\begin{aligned} A2 &= e_{21}(\frac{e(sk_2, C_2)}{e(sk_1, C_1)}, C_4) = e_{21}(e_{11}(g_{12}, g_{13})^{r\omega}, g_{11}^t) = e_{21}(g_{21}^{r\omega}, g_{11}^t) = g_{31}^{r\omega t} \\ M &= \frac{C_3}{A2} \end{aligned}$$

7. Decrypt1(SK_{ID_2}, Pub, C'). ID_2 decrypt $C'_4 = IBE_{ID_2}(X)$ to get $H(x)$, and compute

$$A1 = e(C'_3, H(X), C'_2) = e(g_{13}^y, H(X), g_{12}^{\omega t}), M = C'_1/A1$$

4. Security Analysis

We first give three lemmas to prove the three schemes proposed in the above section are IND-CPA secure, then we finally prove our IBPRE$^+$ scheme is also IND-CPA secure.

Lemma 1. *If there exists an adversary $\mathcal{A}$ which can break the IND-CPA property of the IBE encryption scheme in subsection 3.1, then we can construct an algorithm $\mathcal{B}$ which can solve the DBDH hard problem.*

Proof. Assume algorithm $\mathcal{B}$ is given the input (g, g^a, g^b, g^c, T), if $T = e(g, g)^{abc}$, then $\mathcal{B}$ outputs 1, otherwise it outputs 0. We say $\mathcal{B}$ can solve the DBDH hard problem, if the difference between $\mathcal{B}$ outputs 1 and outputs 0 is non-negligible. We show how $\mathcal{B}$ simulates the IBE environment for adversary $\mathcal{A}$ and then uses $\mathcal{A}$'s attack ability for IBE to solve the DBDH problem. $\mathcal{B}$ runs the IND-sID-CPA game with $\mathcal{A}$ as the following:

1. Initialization. First $\mathcal{A}$ outputs a target identity ID^* which he wants to attack.
2. Setup. $\mathcal{B}$ first sets $h = g_1^{-ID^*} g^{\alpha'} \in \mathbb{G}$ where α' is chosen randomly from Z_p^*, let the public parameters are $(g, g_1 = g^a, g_2 = g^b, g_3 = g^c, h = g_1^{-ID^*} g^{\alpha'})$, note here the master key $MK = g_2^a = g^{ab}$ is unknown to $\mathcal{B}$.
3. Phase 1. $\mathcal{A}$ makes private key queries to $\mathcal{B}$, the only restriction is that the queried identities being not the ID^*. Assume the queried identity is ID, then $\mathcal{B}$ returns the private key as

$$g_2^{\frac{-\alpha'}{ID-ID^*}} (g_1^{ID-ID^*} g^{\alpha'})^{r_j} = g_2^a (g_1^{ID-ID^*} g^{\alpha'})^{r_j - \frac{b}{ID-ID^*}} = g_2^a (g_1^{ID} h)^u$$
$$g^{r_j - \frac{b}{ID-ID^*}} = g^{r_j} g_2^{-1/(ID-ID^*)} = g^u$$

where r_j is chosen randomly from Z_p^*, $u = r_j - \frac{b}{ID-ID^*}$. It is easily to know the returned simulated private key is indistinguishable from the real private key.

4. Challenge. After phase 1 is over, adversary $\mathcal{A}$ outputs two messages $M_0, M_1 \in \mathbb{G}$ and sends them to $\mathcal{B}$, $\mathcal{B}$ chooses $b \in \{0,1\}$ randomly and computes
$$C = (g_3, (g_1^{ID^* - ID^*} g^{\alpha'})^c = g^{c\alpha'}, M_b \cdot T)$$
If $T = e(g,g)^{abc}$, then the above C is a valid challenge ciphertext, otherwise it is an invalid challenge ciphertext.
5. Phase 2. Same as the simulation in Phase 1 with the restriction the queried identities can not be ID^*.
6. Guess. Finally $\mathcal{A}$ outputs a guess b'. Algorithm $\mathcal{B}$ concludes its own game by outputting a guess as follows. If $b = b'$ then $\mathcal{B}$ outputs 1 meaning $T = e(g,g)^{abc}$, otherwise it outputs 0 meaning $T \neq e(g,g)^{abc}$.

When $T = e(g,g)^{abc}$ then $\mathcal{A}$'s view is same as the real attack game. On the other hand, when $T \neq e(g,g)^{abc}$ then $\mathcal{A}$ can only randomly guess b, and thus $Pr[b = b'] = 1/2$, then the security of the scheme can be reduced to the security of D3DH hard problem.

Lemma 2. *If there exists an adversary $\mathcal{A}$ which can break the IND-CPA property of the IBE encryption scheme in subsection 3.2, then we can construct an algorithm $\mathcal{B}$ which can solve the Decisional 3-linear Diffie-Hellman (D3DH) hard problem.*

Proof. We can easily observe that the IBE encryption scheme in subsection 3.2 is similar as the IBE encryption scheme in subsection 3.1, with only the difference the first scheme uses 3-linear map while the latter scheme using the bilinear map (pairing). Thus we first give an assumption named Decisional 3-linear Diffie-Hellman hard(D3DH) problem just like DBDH problem as following: it is difficult to distinguish $(g_{11}, g_{11}^a, g_{11}^b, g_{11}^c, g_{11}^d, e(g_{11}, g_{11}, g_{11})^{abcd})$ from $(g_{11}, g_{11}^a, g_{11}^b, g_{11}^c, g_{11}^d, T)$ where T is randomly chosen from G. Note here we denotes e as the general 3-linear map which omits the footnote on describing the level of map for easily understanding.

Assume algorithm $\mathcal{B}$ is given the input $(g_{11}, g_{11}^a, g_{11}^b, g_{11}^c, g_{11}^d, T)$, if $T = e(g_{11}, g_{11})^{abcd}$, then $\mathcal{B}$ outputs 1, otherwise it outputs 0. We say $\mathcal{B}$ can solve the D3DH hard problem, if the difference between $\mathcal{B}$ outputs 1 and outputs 0 is non-negligible. We show how $\mathcal{B}$ simulate the IBE environment for adversary $\mathcal{A}$ and then use $\mathcal{A}$'s attack ability for IBE to solve the D3DH problem. $\mathcal{B}$ runs the IND-sID-CPA game with $\mathcal{A}$ as the following:

1. Initialization. First $\mathcal{A}$ outputs a target identity ID^* which he wants to attack.
2. Setup. $\mathcal{B}$ first sets $h = g_{12}^{-ID^*} g_{11}^{\alpha'} \in \mathbb{G}$ where α' is chosen randomly from Z_p^*, let the public parameters are $(g_{11} = g_{11}, g_{12} = g_{11}^b, g_{13} = g_{11}^a, h_{11} = g_{12}^{-ID^*} g_{11}^{\alpha'}, g_{21} = e_{11}(g_{12}, g_{13}) = e(g_{11}, g_{11})^{ab}, g_{31} = e_{21}(g_{21}, g_{11}) = e(g_{11}, g_{11}, g_{11})^{ab})$, note here the master key $MK = g_{12}^a = g_{11}^{ab}$ is unknown to $\mathcal{B}$.
3. Phase 1. $\mathcal{A}$ makes private key queries to $\mathcal{B}$, the only restriction is that the queried identities being not the ID^*. Assume the queried identity is ID, then $\mathcal{B}$ returns the private key as

   $$g_{12}^{\frac{-\alpha'}{ID-ID^*}} (g_{13}^{ID-ID^*} g_{11}^{\alpha'})^{r_j} = g_{12}^a (g_{13}^{ID-ID^*} g_{11}^{\alpha'})^{r_j - \frac{b}{ID-ID^*}} = g_{12}^a (g_{13}^{ID} h_{11})^u$$
   $$g_{11}^{r_j - \frac{b}{ID-ID^*}} = g_{11}^{r_j} g_{12}^{-1/(ID-ID^*)} = g^u$$

   where r_j is chosen randomly from Z_p^*, $u = r_j - \frac{b}{ID-ID^*}$. It is easily to know the returned simulated private key is indistinguishable from the real private key.
4. Challenge. After phase 1 is over, adversary $\mathcal{A}$ outputs two messages $M_0, M_1 \in \mathbb{G}$ and sends them to $\mathcal{B}$, $\mathcal{B}$ chooses $b \in \{0, 1\}$ randomly and computes

   $$C = (g_{11}^c, (g_{12}^{ID^*-ID^*} g_{11}^{\alpha'})^c = g_{11}^{c\alpha'}, M_b \cdot T, g_{11}^d)$$

   If $T = e(g_{11}, g_{11}, g_{11})^{abcd}$, then the above C is a valid challenge ciphertext, otherwise it is an invalid challenge ciphertext.
5. Phase 2. Same as the simulation in Phase 1 with the restriction the queried identities can not be ID^*.

6. Guess. Finally $\mathcal{A}$ outputs a guess b'. Algorithm $\mathcal{B}$ concludes its own game by outputting a guess as follows. If $b = b'$ then $\mathcal{B}$ outputs 1 meaning $T = e(g, g)^{abc}$, otherwise it outputs 0 meaning $T \neq e(g, g)^{abc}$.

When $T = e(g_{11}, g_{11}, g_{11})^{abcd}$ then $\mathcal{A}$'s view is same as the real attack game. On the other hand, when $T \neq e(g_{11}, g_{11})^{abc}$ then $\mathcal{A}$ can only randomly guess b, and thus $Pr[b = b'] = 1/2$, then the security of the scheme can be reduced to the security of D3DH hard problem.

Lemma 3. *If there exists an adversary $\mathcal{A}$ which can break the IND-CPA property of the IBE encryption scheme in subsection* **??**, *then we can construct an algorithm $\mathcal{B}$ which can solve the Decisional 3-linear Diffie-Hellman (D3DH) hard problem.*

PROOF. We can easily observe that the IBE encryption scheme in subsection **??** is similar as the IBE encryption scheme in subsection 3.2, with only the difference that the former scheme uses a fixed randomness while the later scheme is not using that. For the fixed randomness is only used in the encryption process, thus the security proof is almost the same as the above lemma except on how to deal with the challenge of the ciphertext.

We show how $\mathcal{B}$ simulates the IBE environment for adversary $\mathcal{A}$ and then uses $\mathcal{A}$'s attack ability for IBE to solve the D3DH problem. $\mathcal{B}$ runs the IND-sID-CPA game with $\mathcal{A}$ as the following:

1. Initialization. Same as the above lemma.
2. Setup. Same as the above lemma.
3. Phase 1. Same as the above lemma.
4. Challenge. After phase 1 is over, adversary $\mathcal{A}$ outputs two messages $M_0, M_1 \in \mathbb{G}$ and sends them to $\mathcal{B}$, $\mathcal{B}$ chooses $b \in \{0, 1\}$ randomly and computes

$$C = (g_{11}^{rc}, (g_{12}^{ID^*-ID^*} g_{11}^{\alpha'})^{rc} = g_{11}^{rc\alpha'}, M_b \cdot T, g_{11}^{d})$$

where r is a randomly chosen fixed randomness from Z_p^*. If $T = e(g_{11}, g_{11}, g_{11})^{abcd}$, then the above C is a valid challenge ciphertext, otherwise it is an invalid challenge ciphertext. Note here r is used for every encryption process for ID^*, and this does not affect the security for r which is embedded in the exponent.

5. Phase 2. Same as the above lemma.
6. Guess. Same as the above lemma.

Thus as the above lemma, the security of the scheme can be reduced to the security of D3DH hard problem.

Theorem 1. *If there exists an adversary $\mathcal{A}$ which can break the IND-CPA property of the second level ciphertexts of our $IBPRE^+$ scheme in subsection 3.4, then we can construct an algorithm $\mathcal{B}$ which can solve the Decisional 3-linear Diffie-Hellman (D3DH) hard problem.*

Proof. Assume algorithm $\mathcal{B}$ is given the input $(g_{11}, g_{11}^a, g_{11}^b, g_{11}^c, g_{11}^d, T)$, if $T = e(g_{11}, g_{11})^{abcd}$, then $\mathcal{B}$ outputs 1, otherwise it outputs 0. We say $\mathcal{B}$ can solve the D3DH hard problem, if the difference between $\mathcal{B}$ outputs 1 and outputs 0 is non-negligible. We show how $\mathcal{B}$ simulate the $IBPRE^+$ environment for adversary $\mathcal{A}$ and then use $\mathcal{A}$'s attack ability for the second level ciphertexts of $IBPRE^+$ to solve the D3DH problem. $\mathcal{B}$ runs the IND-sID-CPA game with $\mathcal{A}$ as the following:

1. Initialization. First $\mathcal{A}$ outputs a target identity ID^* which he wants to attack.
2. Setup. $\mathcal{B}$ first sets $h = g_{12}^{-ID^*} g_{11}^{\alpha'} \in \mathbb{G}$ where α' is chosen randomly from Z_p^*, let the public parameters are $(g_{11} = g_{11}, g_{12} = g_{11}^b, g_{13} = g_{11}^a, h_{11} = g_{12}^{-ID^*} g_{11}^{\alpha'}, g_{21} = e_{11}(g_{12}, g_{13}) = e(g_{11}, g_{11})^{ab}, g_{31} = e_{21}(g_{21}, g_{11}) = e(g_{11}, g_{11}, g_{11})^{ab})$, note here the master key $MK = g_{12}^a = g_{11}^{ab}$ is unknown to $\mathcal{B}$.
3. Phase 1.
   - $\mathcal{A}$ makes private key queries to $\mathcal{B}$, the only restriction is that the queried identities being not the ID^*. Assume the queried identity is

ID, then $\mathcal{B}$ returns the private key as

$$g_{12}^{\frac{-\alpha'}{ID-ID^*}}(g_{13}^{ID-ID^*}g_{11}^{\alpha'})^{r_j} = g_{12}^{a}(g_{13}^{ID-ID^*}g_{11}^{\alpha'})^{r_j-\frac{b}{ID-ID^*}} = g_{12}^{a}(g_{13}^{ID}h_{11})^{u}$$
$$g_{11}^{r_j-\frac{b}{ID-ID^*}} = g_{11}^{r_j}g_{12}^{-1/(ID-ID^*)} = g^{u}$$

where r_j is chosen randomly from Z_p^*, $u = r_j - \frac{b}{ID-ID^*}$. It is easily to know the returned simulated private key is indistinguishable from the real private key.

- Case 1: the re-encryption key query on $ID \to ID'$ where $ID, ID' \neq ID^*$. For any other encrypter's ciphertexts C_{ID} for ID, $\mathcal{B}$ does not know the randomness in the exponent, thus $\mathcal{B}$ returns

  $$\begin{aligned} rk_{ID_1 \to ID_2} &= (rk_1, rk_2, rk_3) \\ &= (g_{11}^{-r_1}H(X_1)^{y_1}, g_{13}^{y_1}, IBE_{ID_2}(X_1)) \end{aligned}$$

  where r_1, y_1 randomly chosen from Z_p^*, and X_1 is randomly chosen from $\{0,1\}^*$, $H : \{0,1\}^* \to G_1$. This re-encryption key is distributed same as the real re-encryption key, but it can not re-encrypt any other encrypter's ciphertexts correctly.

  Note here one might wonder that $\mathcal{A}$ can distinguish the simulation with the real implementation as following: $\mathcal{A}$ first encrypts message m to get the ciphertexts C_{ID} for ID, and then queries the re-encryption key on $ID \to ID'$ and implements the re-encryption process himself, and then query the private key of ID', and thus decrypt the re-encrypted ciphertext $C_{ID'}$ and find the message is not m, then $\mathcal{A}$ realize himself in the simulated environment. We remark that this is not true, for in the real environment, the correct re-encrypted key also can only be generated by the encrypter himself. Thus the simulated environment is indistinguishable with the real environment for this case.
- Case 2: the re-encryption key query on $ID \to ID'$ where ID' is ID^*. In this case, $\mathcal{A}$ can not know the private key of the

   delegatee ID^*, and other discussion is the same with the above case. Thus $\mathcal{B}$ can simulate the re-encryption key as the above case.

   - Case 3: the re-encryption key query on $ID \to ID'$ where ID is ID^*. In this case, for the ciphertexts C_{ID^*} for ID^* created by $\mathcal{B}$ by using the fixed randomness r, $\mathcal{B}$ knows the fixed randomness and thus he can simulate the correct re-encryption key

     $$\begin{aligned} & rk_{ID_1 \to ID_2} = (rk_1, rk_2, rk_3) \\ & = (g_{11}^{-r} H(X_2)^{y_2}, g_{13}^{y_2}, IBE_{ID_2}(X_2)) \end{aligned}$$

     where y_2 randomly chosen from Z_p^*, and X_2 is randomly chosen from $\{0,1\}^*$, $H : \{0,1\}^* \to G_1$. This re-encryption key is distributed same as the real re-encryption key, and it can re-encrypt the ciphertexts correctly. For the ciphertexts C_{ID^*} for ID^* not created by $\mathcal{B}$ or created by $\mathcal{B}$ but not using the fixed randomness r, the simulation is same as Case 1.

4. Challenge. After phase 1 is over, adversary $\mathcal{A}$ outputs two messages $M_0, M_1 \in \mathbb{G}$ and sends them to $\mathcal{B}$, $\mathcal{B}$ chooses $b \in \{0,1\}$ randomly and computes

   $$C = (g_{11}^{rc}, (g_{12}^{ID^*-ID^*} g_{11}^{\alpha'})^{rc} = g_{11}^{rc\alpha'}, M_b \cdot T, g_{11}^{d})$$

   where r is a randomly chosen fixed randomness from Z_p^*. If $T = e(g_{11}, g_{11}, g_{11})^{abcd}$, then the above C is a valid challenge ciphertext, otherwise it is an invalid challenge ciphertext. Note here r is used for every encryption process, and this does not affect the security for r which is embedded in the exponent.

5. Phase 2. Same as Phase 1.

6. Guess. Finally $\mathcal{A}$ outputs a guess b'. Algorithm $\mathcal{B}$ concludes its own game by outputting a guess as follows. If $b = b'$ then $\mathcal{B}$ outputs 1 meaning $T = e(g_{11}, g_{11}, g_{11})^{abcd}$, otherwise it outputs 0 meaning $T \neq e(g_{11}, g_{11}, g_{11})^{abcd}$.

When $T = e(g_{11}, g_{11}, g_{11})^{abcd}$ then $\mathcal{A}$'s view is same as the real attack game. On the other hand, when $T \neq e(g_{11}, g_{11}, g_{11})^{abcd}$ then $\mathcal{A}$ can only randomly guess

b, and thus $Pr[b = b'] = 1/2$, then the security of the scheme can be reduced to the security of D3DH hard problem.

Theorem 2. *If there exists an adversary $\mathcal{A}$ which can break the IND-CPA property of the first level ciphertexts of our $IBPRE^+$ scheme in subsection 3.4, then we can construct an algorithm $\mathcal{B}$ which can solve the Decisional 3-linear Diffie-Hellman (D3DH) hard problem.*

PROOF. The security proof for this lemma is almost same as the above lemma except the handling on the challenge re-encrypted ciphertext

1. Initialization. Same as the above lemma.
2. Setup. Same as the above lemma.
3. Phase 1. Same as the above lemma.
4. Challenge. After phase 1 is over, adversary $\mathcal{A}$ outputs two messages $M_0, M_1 \in \mathbb{G}$ and sends them to $\mathcal{B}$, $\mathcal{B}$ chooses $b \in \{0,1\}$ randomly and computes

   $$C = (M_b e(H(X)^y, g_{11}^{d'}, g_{13}), g_{13}^y, g_{11}^{d'}, IBE_{ID^*}(X))$$

   where y, d' is randomly chosen from Z_p^* and X is randomly chosen from $\{0,1\}^*$,

   $$IBE_{ID^*}(X) = (g_{11}^{rc}, (g_{12}^{ID^*-ID^*} g_{11}^{\alpha'})^{rc} = g_{11}^{rc\alpha'}, M_b \cdot T, g_{11}^{d})$$

   where r is a randomly chosen fixed randomness from Z_p^*. If $T = e(g_{11}, g_{11}, g_{11})^{abcd}$, then the above C is a valid challenge ciphertext, otherwise it is an invalid challenge ciphertext. Note here r is used for every encryption process, and this does not affect the security for r which is embedded in the exponent.
5. Phase 2. Same as Phase 1.
6. Guess. Same as the above lemma.

Thus as the above lemma, the security of the scheme can be reduced to the security of D3DH hard problem.

Theorem 3. *Our $IBPRE^+$ scheme in subsection 3.4 is master secret secure and weak non-transferable.*

Proof. From the re-encryption key $rk_{ID_1 \to ID_2} = (g_{11}^{-r} H(X)^y, g_{13}^y, IBE_{ID_2}(X))$, we can easily see that it is independent with ID_1's private key, thus even if the delegatee and the proxy collude, they can not derive any information on the private key of the delegator, so our scheme can achieve master secret secure. Furthermore, from $rk_{ID_1 \to ID_2}$, sk_{ID_2}, ID_2 can easily produce $rk_{ID_1 \to ID_3}$ for fixed randomness r, but it can not produce $rk_{ID_1 \to ID_3}$ for other ciphertexts not using randomness r, thus our scheme is weak non-transferable.

5. Properties and Performance Analysis

5.1. Properties Analysis

Based on [2], our scheme has the following properties:

1. Unidirectional: the data sender S generates the re-encryption keys in our scheme, the re-encryption key from A → B can not be used to compute re-encryption key from B → A, so our scheme is unidirectional.
2. Non-interactive: using Bob's public key, Alice generates the re-encryption key; no trusted third party or interaction of Bob is required, so our scheme is non-interactive.
3. Non-transitive: Any information about the sender's private key cannot be inferred from the re-encryption key by the proxy, thus the proxy cannot re-delegate decryption rights. From $rk_{a \to b}$ and $rk_{b \to c}$, the proxy can not derive $rk_{a \to c}$, so our scheme is non-transitive.
4. Message level based delegation: in our scheme, the encrypter can easily control which message will be delegated by the proxy. For example, for $rk_{ID_1 \to ID_2} = (g_{11}^{-r} H(X)^y, g_{13}^y, IBE_{ID_2}(X))$, the message is encrypted with randomness r if the encrypter wants to share this message with the delegatee, otherwise the message is encrypted with other randomness. In this way message level based delegation can be achieved.

5. Weak non-transferability: A set of delegatees and the proxy cannot collude to re-delegate decryption rights for the delegator. For example, although they can produce $rk_{a \to c}$ for fixed randomness r from $rk_{a \to b}$, sk_b, pk_c, but they can not produce $rk_{a \to c}$ for other ciphertexts generated by not using randomness r. Thus the non-transferability is partially solved.
6. ReKeyGen not involving PKG: The generation of re-encryption key does not need the PKG involving. In our scheme, the re-encryption key is generated by the encrypter by using the fixed ephemeral randomness and the delegatee's identity. Involving PKG in the re-encryption key generation is not a good choice for many applications for PKG is only online in the system initialization phase.
7. ReKeyGen involving Encrypter: The generation of re-encryption key does need the Encrypter involving. In many cases, the encrypter decides which message to be encrypted and thus it should have more control on the messages compared with the decryptor. In our scheme, the re-encryption key is generated by the encrypter by using the fixed ephemeral randomness and the delegatee's identity, and thus it has more power for controlling the delegation of the message.

We compare our scheme's properties with [31] which is a typical IBPRE scheme, Table 1 shows comparison results, where we can see that our scheme has many advantages compared to [31].

5.2. Performance Analysis

In this subsection, the performance of IBPRE$^+$ scheme is analysed from the following two aspects: the communication cost and the computation cost.

Let $t_{3linear}$ represent the time of one bilinear map operation in 3 linear group $(e, G_1, G_2, G_3, Z_p^*)$, t_{exp1}, t_{exp2} and t_{exp3} represents the exponential operation of the group G_1, G_2, G_3, the elements length of group G_1 is $|G_1|$ bits, the elements length of group G_2 is $|G_2|$ bits, the elements length of group G_3 is $|G_3|$ bits, the elements length of group Z_p^* is $|Z_p^*|$ bits.

Table 1: Feature comparison

Schemes	Our Scheme	[31]
Unidirectional	Yes	Yes
Non-transitive	Yes	Yes
Multi-hop	Yes	Yes
Non-transferable	Yes(Partially)	Yes
Message-level based delegation	Yes	No
ReKeyGen Involving PKG	No	Yes
ReKeyGen Involving Encrypter	Yes	No

Table 2: Communication cost

Scheme	Our Scheme	[31]
Public Parameter	$4\|G_1\|+\|G_2\|+\|G_3\|$	$5\|H_1\|+2\|H_2\|+\|Z_{p'}^*\|$
Private Key	$2\|G_1\|$	$2\|H_1\|$
Re-encryption Key	$6\|G_1\|+\|G_3\|$	$2\|H_1\|$
Original Ciphertext	$4\|G_1\|+\|G_3\|$	$3\|H_1\|+\|H_2\|$
Re-encrypted Ciphertext	$6\|G_1\|+2\|G_3\|$	$2\|H_1\|+\|H_2\|$

Let $T_{bilinear}$ represents the time of one bilinear map operation in bilinear group $(e, H_1, H_2, Z_{p'}^*)$, T_{exp1}, T_{exp2} represents the exponential operation of the group H_1, H_2, the elements length of group H_1 is $|H_1|$ bits, the elements length of group H_2 is $|H_2|$ bits, the elements length of group H_3 is $|H_3|$ bits, the elements length of group $Z_{p'}^*$ is $|Z_{p'}^*|$ bits.

Table 2 shows the comparison results about communication complexity between the scheme of [31] and our scheme, Table 3 shows the comparison results about computation cost between the scheme of [31] and our scheme.

Please note here that a very rough comparison on the number of group elements or the operation of group elements is done; actually our scheme is a theoretical construction due to the current research status of multilinear map. However, we stress here that our scheme is the first identity based proxy re-encryption scheme which can support message-level based fine-grained delegation for the data owner and can easily achieve weak non-transferable property. It is a novel cryptographic primitive which may find other interesting applications. Furthermore, we think it is very probable to find new construction of IBPRE$^+$ without multilinear map, which we leave as future work.

We do not implement our IBPRE$^+$ scheme in this paper for the research on multilinear map including 3-linear map is very active and unstable. Many candidate constructions have been broken, but until now many cryptographic researchers still are optimistic on the final construction of 3-linear map and even multilinear map [8].

6. IBPRE$^+$ for Secure Social Cloud Data Sharing

Here, we demonstrate the application of our scheme in the social cloud storage access control system. As shown in Fig. 5, the main actors of our system are the data owner, many data users, a System Management Server (SMS) and a number of cloud storage servers (Cloud Storage Server, CSS). For a particular user, if she is the owner of a certain data, we call her as the Data Owner (DO), the rest of the data users may share the data, then they are called Data

Table 3: Computation cost

Schemes	Our Scheme	[31]
KeyGen	$4t_{exp1}$	$3T_{exp1}$
Encrypt	$4t_{exp1} + t_{exp3}$	$T_{bilinear} + 3T_{exp1} + T_{exp2}$
ReKeyGen	$5t_{exp1}$	$3T_{exp1}$
Reencrypt	$2t_{3linear}$	$2T_{bilinear} + T_{exp2}$
Decrypt1	$3t_{3linear}$	$2T_{bilinear} + T_{exp2}$
Decrypt2	$t_{3linear}$	$2T_{bilinear} + T_{exp2}$

Sharer (DS). The data owner encrypts her data contents like his social photos' encapsulation key (the social photos are directly encrypted by ciphers suitable for JPEG or video encryption using this key) and then outsource them to the cloud storage servers. Later she wants to share the social photos with other friends. The System Management Server mainly stores some public information for the users to grant access control, such as the system's parameters, the users' public key information, re-encryption keys and so on. The Cloud storage server effectively and safely store users' sensitive data, ensuring the robustness and integrity of the stored data. As a service, the Quality of Service is also an important basis for the user to choose the providers of cloud storage service, therefore, the robustness and the confidentiality of data should be ensured. In this paper, it is assumed that the cloud storage server is semi-trusted, and it will respond and give the correct answer for the user's legitimate request; at the same time, it would be interested in the encrypted data content and attempt to gain the knowledge of the underline plaintexts.

Concretely, system initialization, key generation, data storage, data sharing and data recovery consist the algorithms of our IBPRE$^+$ for secure social cloud data sharing framework:

1. System initialization. First a security parameter is selected by the PKG. The PKG generates some public parameters on inputting this security

parameter. The public parameters are then outsourced to the system management server and made to be publicly to anyone.

2. Key generation. By using the system parameters, user's identity and master secret key, the PKG generates the private key of the system users. Then by using a secure channel, the private key is sent to the users by the PKG.
3. Data storage. When outsourcing her private social photos to the cloud, data owner Alice first selects cipher suitable for photo encryption and then encrypts the social photos with this cipher. Then by using our IBPRE$^+$ scheme with some fixed randomness, she encrypts the cipher's key for photos A1, A2, $\cdots$, An, she also encrypts the cipher's key for photos B1, B2, $\cdots$, Bn with some other fixed randomness. Finally all the ciphertexts are outsourced to the cloud storage server. Of course the outsource data's integrity will be ensured by other cryptographic techniques like provable data position. Note here when Alice does not want to share her personal photo C with Bob or Charlie, she can simply encrypt the cipher's key with other randomness. In this way, Alice can completely control which photo will be shared with Bob, which photo will be shared with Charlie, which photo will be not shared with Bob or Charlie either.
4. Data sharing with Bob. With her close friend Bob when Alice wants to share her personal photo A1, she generates the re-encryption keys for Bob. The key is generated by using public parameters, Bob's identity and the fixed randomness for photo A1 and sent to the cloud. Alice's outsourced encrypted photo A1 is first retrieved by the cloud storage server, then it implements the re-encryption algorithm and send the re-encrypted ciphertext to Bob.
5. Data sharing with Charlie. When sharing her personal photo B1 with another close friend Charlie, data owner Alice first generates the re-encryption key for Charlie. This key is generated by using public parameters, Charlie's identity and the fixed randomness for photo B and sent to the cloud. Then Alice's outsourced encrypted photo B1 is first retrieved by the cloud

storage servers, and the re-encryption algorithm is implemented, then the re-encrypted ciphertext is sent to Charlie.

6. Data recovery. By using his own private key, after getting the re-encrypted ciphertexts data sharer Bob decrypts encrypted photo A1, and he will get the cipher key for social photo A1. Then he requires the cloud also send him the encrypted social photo A1, he can decrypt them by using the retrieved cipher key to get the social photo. By implementing the similar process, data sharer Charlie can retrieve photo B1.

We describe our framework in the following algorithm 1:

By using the traditional identity based proxy re-encryption, Alice also can share her private social photos with Bob. But she cannot achieve the message-level fine-grained access control on her photos. Such as, if she wants to share with Bob only the photo A but not photo B, IBPRE cannot easily achieve this property, but IBPRE$^+$ can achieve this easily by controlling the randomness used in the encryption process.

Furthermore, by using IBPRE, Bob and cloud can easily collude to re-assign re-encryption ability to the proxy for sharing photos with Charlie. But IBPRE$^+$ can prevent this for even if Bob and the cloud collude, they can not derive new re-encryption keys from Alice to Charlie. Someone may argue that, as Bob can share Alice's private photos, he of course has the ability to share these photos with Charlie. This is true, but note that this sharing process is offline and Bob can be easily caught for high bandwidth or direct communication between Bob and Charlie. While sharing through proxy re-encryption, Bob needs only collude with the cloud to generate new re-encryption keys, which is much smaller than the social photos, and can be caught only with very little probability.

7. Conclusion

In this paper, we further extend the concept of PRE$^+$ to the identity based setting. We propose a new primitive IBPRE$^+$ and give a concrete construction. IBPRE$^+$ can be seen as the dual of the traditional IBPRE scheme. We prove the

Algorithm 1: Algorithm of IBPRE$^+$ for Secure Social Cloud Data Sharing

```
**System initialization:** $PKG(1^k) \rightarrow Pub$, $Pub \rightarrow SMS$, let $Pub$ be public;
**Key generation:**
for $i = 1$ to $t$ do
    PKG runs $KeyGen(ID_i, MK, Pub) \rightarrow SK_{ID_i}$, distribute $SK_{ID_i}$ to $ID_i$;
**Data storage:**
Alice first encrypts the social photos with ciphers suitable for JPEG encryption; then she encrypts the cipher's key with our IBPRE$^+$ scheme with some fixed randomness for photos A1, A2, $\cdots$, An;
for $i = 0$ to $n$ do
    calculate $Cipher_K(Ai) \rightarrow DEM$;
    $Encrypt(Pub, r, K) \rightarrow KEM$ where $r$ is the fixed randomness;
for $i = 0$ to $n$ do
    calculate $Cipher_{K'}(Bi) \rightarrow DEM$;
    $Encrypt(Pub, r', K') \rightarrow KEM$ where $r'$ is the fixed randomness;
**Data sharing photo A1:**
Alice she first generates the re-encryption keys for Bob;
$ReKeyGen(Pub, r, Alice, Bob) \rightarrow rk_{A \rightarrow B}$;
Cloud Server implements the re-encryption algorithm;
$Reencrypt(Pub, KEM, rk_{A \rightarrow B}, Alice, Bob) \rightarrow C'$, $C' \rightarrow Bob$;
**Data sharing photo B1:**
Alice she first generates the re-encryption keys for Charlie;
$ReKeyGen(Pub, r, Alice, Charlie) \rightarrow rk_{A \rightarrow C}$;
Cloud Server implements the re-encryption algorithm;
$Reencrypt(Pub, KEM, rk_{A \rightarrow C}, Alice, Charlie) \rightarrow C''$, $C'' \rightarrow Charlie$;
**Data recovery:**
Bob decrypt encrypted photo A1 by using his own private key;
$Decrypt1(SK_{Bob}, Pub, C') \rightarrow K$, $DeCipher_K(DEM) = A1$.
Charlie decrypt encrypted photo B1 by using his own private key;
$Decrypt1(SK_{Charlie}, Pub, C'') \rightarrow K'$, $DeCipher_{K'}(DEM) = B1$.
```

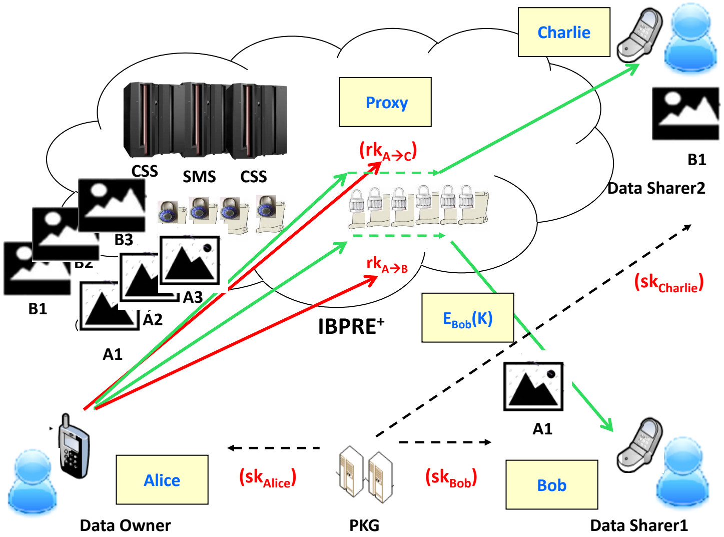

Figure 5: IBPRE$^+$ for secure cloud data sharing

security of the construction by using standard cryptographic techniques. Many interesting directions can be explored, such as giving more efficient construction of IBPRE$^+$ scheme, finding more application of IBPRE$^+$, etc.

Acknowledgements

This work is supported by National Cryptography Development Fund of China Under Grants No. MMJJ20170112, National Natural Science Foundation of China (Grant Nos. 61772550, 61572521, U1636114, 61402531), National Key Research and Development Program of China Under Grants No. 2017YFB0802000, Natural Science Basic Research Plan in Shaanxi Province of china (Grant Nos. 2018JM6028) and Guangxi Key Laboratory of Cryptography and Information Security (No. GCIS201610).

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *NDSS 2005*, San Diego, California, USA, February 3–4, 2005. The Internet Society.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Transactions on Information and System Security, vol. 9, no. 1, pages 1–30. 2006.

[3] M. Blaze, G. Bleumer and M. Strauss. Divertible protocols and atomic proxy cryptography. In Kaisa Nyberg, editor, *EUROCRYPT'98*, volume 1403 of *LNCS*, pages 127–144, Espoo, Finland, May 31 – June 4, 1998. Springer, Berlin, Germany.

[4] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229, 2001.

[5] D. Boneh and X.Boyen. Efficient selective-id secure identity based encryption without random oracles. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238, 2004.

[6] D. Boneh and X.Boyen. Secure identity based encryption without random oracles. In *CRYPTO 2004*, volume 3152 of *LNCS*, pages 443–459, 2004.

[7] D. Boneh and A. Silverberg. Applications of multilinear forms to cryptography. Contemporary Mathematics, 324: 71–90, 2003

[8] D. Boneh, D. Glass, D. Krashen, K. Lauter, S. Sharif, A. Silverberg, M. Tibouchi and M. Zhandry Multiparty Non-Interactive Key Exchange and More From Isogenies on Elliptic Curves. Cryptology ePrint Archive, Report 2018/665, 2018.

[9] Y. Chiu, C. Lei, and C. Huang. Secure multicast using proxy encryption. In Sihan Qing, Wenbo Mao, Javier López, and Guilin Wang, editors, *ICICS 05*, volume 3783 of *LNCS*, pages 280–290, Beijing, China, December 10–13, 2005. Springer, Berlin, Germany.

[10] J. Shao, P. Liu, G. Wei, and Y. Ling. Anonymous proxy re-encryption. Security and Communication Networks, vol. 5, no. 5, pp. 439-449, 2012.

[11] M. Green and G. Ateniese, Identity-Based Proxy Re-encryption. In *Applied Cryptography and Network Security'07,*LNCS 4521, pp. 288–306.Springer–Verlag,2007.

[12] Q. Tang, P. Hartel and W Jonker. Inter-domain Identity-based Proxy Re-encryption. Accepted by Inscrypt'08. http://eprints.eemcs.utwente.nl/12259/01/.

[13] Q. Tang. Type-based Proxy Re-encryption and its Construction. http://eprints.eemcs.utwente.nl/13024/01/.

[14] J. Weng, R. H. Deng, C. Chu, X. Ding, and J. Lai. Conditional proxy re-encryption secure against chosen-ciphertext attack. In *ACM ASIACCS 2009*, Pages 322–332, 2009.

[15] J. Weng, Y. Yang, Q. Tang, R. Deng, and F. Bao. Efficient conditional proxy re-encryption with chosen-ciphertext security. In *ISC 2009*, volume 5735 of *LNCS*, pages 151–166, 2009.

[16] K. Gai, M. Qiu, Z. Ming, H. Zhao, L. Qiu. Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks. IEEE Transactions on Smart Grid, 2017, 8(5):2431-2439

[17] K. Gai, M. Qiu, M. Chen, H. Zhao. SA-EAST: security-aware efficient data transmission for ITS in mobile heterogeneous cloud computing ACM Transaction on Embed Computer Sysstem, 16(2):60, 2016.

[18] K. Gai, M. Qiu. An Optimal Fully Homomorphic Encryption Scheme. International Conference on Big Data Security on Cloud. IEEE, 2017:101-106.

[19] K. Gai, M. Qiu, Y. Li, X. Y. Liu. Advanced Fully Homomorphic Encryption Scheme Over Real Numbers. International Conference on Cyber Security and Cloud Computing. IEEE, 2017: 64-69.

[20] B. Libert and D. Vergnaud. Unidirectional chosen ciphertext secure proxy re-encryption. In *PKC 2008*, volume 4939 of *LNCS*, pages 360–379, 2008.

[21] Y. Li, K. Gai, Z. Ming, H. Zhao, M. Qiu. Intercrossed Access Controls for Secure Financial Services on Multimedia Big Data in Cloud Systems. ACM Transactions on Multimedia Computing, Communications and Applications (TOMM), Volume 12 Issue 4s, Article No. 67, 2016.

[22] K. Liang, M. H. Au, J. K. Liu, X. Qi, W. Susilo, X. P. Tran, D. S.Wong, and G. Yang. A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667-1680, 2014.

[23] 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 Miroslaw Kutylowski and Jaideep Vaidya, editors, *ESORICS 2014, Part I*, volume 8712 of *LNCS*, pages 257–272, Wroclaw, Poland, September 7–11, 2014. Springer, Berlin, Germany.

[24] A. Ivan and Y. Dodis. Proxy cryptography revisited. In *NDSS 2003*, San Diego, California, USA, February 5–7, 2003. The Internet Society.

[25] Y. Wang, J. Du, X. Cheng, Z. Liu, and K. Lin. Degradation and encryption for outsourced png images in cloud storage. International Journal of Grid and Utility Computing, vol. 7, no. 1, pp. 22-28, 2016.

[26] S. Zhu and X. Yang. Protecting data in cloud environment with attribute-based encryption. International Journal of Grid and Utility Computing, Vol. 6, No. 2, pp. 91-97, 2015.

[27] S. Garg, C. Gentry and S. Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, EUROCRYPT 2013, volume 7881 of Lecture Notes in Computer Science, pages 1-17. Springer, 2013

[28] S. Guo and H. Xu. A secure delegation scheme of large polynomial computation in multi-party cloud. International Journal of Grid and Utility Computing, Vol. 6, No. 2, pp.1-7, 2015.

[29] C. Dutu, E. Apostol, C. Leordeanu, and V. Cristea. A solution for the management of multimedia sessions in hybrid clouds. International Journal of Space-Based and Situated Computing, Vol. 4, No. 2, pp. 77-87, 2014.

[30] M. Thabet, M. Boufaida, and F. Kordon. An approach for developing an interoperability mechanism between cloud providers. International Journal of Space-Based and Situated Computing, Vol. 4, No. 2, pp. 88-99, 2014.

[31] L. Wang, L. Wang, M. Mambo, and E. Okamoto. Identity-based proxy cryptosystems with revocability and hierarchical confidentialities. In *ICICS 10*, volume 6476 of *LNCS*, pages 383–400, Barcelona, Spain, December 15–17, 2010. Springer, Berlin, Germany.

[32] X. Wang, Y. Ge, and X. Yang. PRE^{+}: Dual of proxy re-encryption and its application. Cryptology ePrint Archive, Report 2013/872, 2013.

[33] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang. Aconditional proxy broadcast re-encryption scheme supporting timed-release. ISPEC 2013, LNCS 7863, Springer, Heidelberg, pp. 132-146, 2013.

[34] S. Park, K. Lee, and D. H. Lee. New constructions of revocable identity based encryption from multilinear maps. IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1564-1577, 2015.

[35] C. Gentry, S. Gorbunov, S. Halevi. Graph-Induced Multilinear Maps from Lattices. http://eprint.iacr.org/2014/645, 2014.

[36] Y. Hu and H. Jia. Crytanalysis of GGH Map. http://eprint.iacr.org/2015/301, 2015.

[37] J. Cheon, K. Han, C. Lee, H. Ryu and D. Stehle. Crytanalysis of the Multilinear Map over the Integers. http://eprint.iacr.org/2014/906, 2014.

[38] J. Kim, S. Kim and J. Seo. Multilinear Map via Scale-Invariant FHE: Enhancing Security and Efficiency. http://eprint.iacr.org/2015/992, 2015.

[39] X. Wang, F. Xhafa, J. Ma, L. Barolli, Y. Ge. PRE$^+$: dual of proxy re-encryption for secure cloud data sharing service. International Journal of Web and Grid Services, Vol.14, No.1, pp. 44-69, 2018.

[40] X. Wang, F. Xhafa, Z. Zheng, J. Nie. Identity Based Proxy Re-encryption Scheme(IBPRE$^+$) for Secure Cloud Data Sharing. International Conference on Intelligent Networking and Collaborative Systems, pp.44-48, 2016.

[41] X. Wang, J. Ma, F. Xhafa, M. Zhang, X. Luo. Cost-efficitive Secure E-health Cloud System Using Identity Based Cryptographic Techniques. Future Generation Computer Systems. http://dx.doi.org/10.1016/j.future.2016.08.008, 2016.

[42] X. Wang, X. Huang, X. Yang, L. Liu, X. Wu. Further observation on proxy re-encryption with keyword search. Journal of Systems and Software, doi:10.1016/j.jss.2011.09.035, 2011.

[43] X. Wang, J. Ma, X. Yang. A new proxy re-encryption scheme for protecting critical information systems. Journal of Ambient Intelligence and Humanized Computing Vol 6, No. 6, pp. 699-711, 2015.

[44] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. IEEE Transaction on Parallel Distributed System. Vol 24, No. 1, pp. 131-143, 2013

[45] S. Yu, C. Wang, K. Ren, W. Lou. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010: 534-542