Identity Based Proxy Re-encryption Based on BB2 and SK IBE with the Help of PKG

Jindan Zhang[1], Xu An Wang[2] and Xiaoyuan Yang[2]
[1]Department of Electronic Information
Xianyang Vocational Technical College, 712000, P. R. China
[2]Key Laboratory of Information and Network Security
Engineering University of Chinese Armed Police Force, 710086, P. R. China
wangxahq@yahoo.com.cn

***Abstract*— In proxy re-encryption, a proxy can transform a ciphertext computed under A's public key into one that can be opened under B's decryption key. In this paper, we focus on the the research of proxy re-encryption in the identity based setting. In particular, we are interested in constructing PRE schemes basically based on standardized IBE schemes, such as BB2 IBE, SK IBE. We construct the first IBPRE scheme based on BB2 IBE, the first IBPRE scheme based on SK IBE with the help of PKG. Concretely, we allow PKG to generate the re-encryption keys between the Delegator and Delegatee by using its master-key. We also prove their security in the corresponding security models, by introducing some novel techniques which maybe have independent interest. At a first look, involving PKG in generating re-encryption keys seems unreasonable, which will greatly increase PKG's workload. But we challenge this traditional view. Firstly, in an IBE system, typically small self-organizations like corporation etc, the demand on proxy re-encryption between any two users is not very often. Thus PKG's workload will be greatly lower than our original anticipation. Secondly, these schemes can easily achieve *master secret secure* property, while the previous PRE schemes can not easily achieve, and even *non-transferable* property, while all the previous PRE schemes can not achieve. These properties are very important for the wide adaptation of IBPRE and PRE.**

***Index Terms*— Cryptography, Identity based proxy re-encryption, PKG, BB_2 IBE, SK IBE, Security proof.**

I. Introduction

Blaze, Bleumer, and Strauss introduced the concept of proxy re-encryption (PRE) in 1998 [2]. Proxy re-encryption enables a semi-trusted proxy transforming a ciphertext under one person to another person, without the proxy knowing the secret keys of the persons and the underlying plaintext. According to the direction of transformation, PRE schemes can be classified into bidirectional schemes and unidirectional schemes. Also according to the times the transformation can apply on the ciphertext, PRE schemes can be classified into single-hop schemes and multi-hop schemes. PRE has been demonstrated to be very useful in e-mail forwarding, law enforcement, cryptographic operations on storage-limited devices, distributed secure file systems and outsourced filtering of encrypted spam, interoperable DRM architecture, multicast etc.

Until now, many variants of PRE have been proposed, such as CCA-secure PRE, PRE in the identity based setting, PRE in the attribute based setting, PRE in the broadcast setting, conditional PRE or type-based PRE, key private PRE, PRE with keyword search etc. But in this paper, we concentrated on one of them: PRE in the identity based setting.

A. Related Work

The first identity based proxy re-encryption schemes(IBPRE) was proposed by Green et al. in ACNS'07. In ISC'07, Chu et al. proposed the first IND-ID-CCA2 IBPRE schemes in the standard model based on Water's IBE. But unfortunately Shao *et al.* found a flaw in their scheme and they fixed this flaw by proposing an improved scheme [16]. In Pairing'07, Matsuo proposed new PRE schemes in the identity based setting [14], one is the hybrid PRE from CBE to IBE, the other is the PRE from IBE to IBE, which can help the ciphertext circulate smoothly in the network. But the latter scheme was recently pointed out to be insecure [21]. In Inscrypt'08, concerning on constructing proxy re-encryption between different domains in identity based setting, Tang et al. proposed the new concept of inter-domain identity based proxy re-encryption [18]. They follow Green's paradigm but based on Boneh-Frankin IBE. Later, Ibraimi et al. construct a type and identity based proxy re-encryption, which aimed at combing type and identity properties in one proxy re-encryption system [11]. Based on identity-based mediated encryption, recently Lai et al. [12] gave new constructions on IBPRE Wang et al. proposed the first multi-use CCA-secure unidirectional IBPRE scheme [21].

B. Our Motivation and Contribution

We extend Matsuo's research on PRE in identity based setting [14]. A fact we must note is the standardization and general acceptance of IBE technology in these years.

The second author is the corresponding author. This paper is an extended work of [20], [22] and supported by the National Natural Science Foundation of China under contract no. 61103230, 61103231, 61272492, 61202492, Natural Science Foundation of Shaanxi Province and Natural Science Foundation of Engineering University of Chinese Armed Police Force.

doi:10.4304/jcp.8.5.1230-1239

IBE is a public-key technology in which the recipient's public key is an arbitrary string that represents the recipient's identity. The sender encrypts the message directly by using this identity. The recipient is given the corresponding private key from a secure server called a private-key generator (PKG) to decrypt the ciphertext. Although the concept of IBE has been proposed in 1984, but the first practical IBE only realized in 2001 by Boneh and Franklin [3]. Later numerous interesting IBE and related schemes have been proposed and implemented [23], [24]. And the interest on IBE quickly spreads from the academical society to the industry and even to every normal person. More and more standardization organization show great interest on standardize IBE schemes, such as P1363 workgroup, IETF and NIST. RFC 5091 (www. ietf.org/rfc/rfc5091.txt) defines two IBE schemes, and the IEEE P1363.3 Standard for Identity-Based Cryptographic Techniques using Pairings (http://grouper.ieee.org/groups/1363/IBC/) concentrates on IBE and related schemes. In 2008, NIST holds a workshop on the IBE technology. All these standardization body show interest on standardizing four IBE schemes: BF IBE [3], BB_1 IBE [4], BB_2 IBE [4], and SK IBE [17]. Thus when we consider extending Matsuo's research on PRE in identity based setting, we first try to construct PRE schemes based on these standardizing IBE schemes, which will give more choice and guidance to the security engineers. We remark although there are many PRE schemes in the identity based setting, but none of them is constructed from this viewpoint.

Our contributions are mainly as following: by allowing PKG generating re-encryption keys for PRE by using its master − key, we construct PRE based on SK IBE and PRE based on BB_2 IBE.

C. Organization

We organize our paper as following. In Section II, we give some preliminaries which are necessary to understand our paper. In Section III, we propose our new proxy re-encryption scheme based on BB_2 IBE and prove its security. In Section IV, we propose our new proxy re-encryption scheme based on SK IBE and prove its security. In Section V, we discuss about issues PKG's workload in our scheme. We give our conclusions in the last Section VI.

II. Preliminaries

A. Bilinear groups

Let G and G_1 be multiplicative cyclic groups of prime order p, and g be generator of G. We say that G_1 has an admissible bilinear map $e : G \times G \to G_1$. if the following conditions hold.

1) $e(g^a, g^b) = e(g, g)^{ab}$ for all a, b.
2) $e(g, g) \neq 1$.
3) There is an efficient algorithm to compute $e(g^a, g^b)$ for all a, b and g.

B. Assumptions

Definition 1: For randomly chosen integers a, b, $c \xleftarrow{R} Z_p^*$, a random generator $g \xleftarrow{R} G$, and an element $R \xleftarrow{R} G$, we define the advantage of an algorithm $\mathcal{A}$ in solving the modified Decision Bilinear Diffie-Hellman(mDBDH) problem as follows:

$$Adv_G^{dbdh}(\mathcal{A}) = |Pr[\mathcal{A}(g, g^a, g^{a^2}, g^b, g^c, e(g,g)^{abc}) = 0] \\ -Pr[\mathcal{A}(g, g^a, g^{a^2}, g^b, g^c, R) = 0]|$$

where the probability is over the random choice of generator $g \in G$, the randomly chosen integers a, b, c, the random choice of $R \in G$, and the random bits used by A. We say that the (k, t, ϵ)-mDBDH assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the mDBDH problem in G under a security parameter k.

Definition 2: For randomly chosen integers $x \xleftarrow{R} Z_p^*$, a random generator $g_1, g_2 \xleftarrow{R} G$, we define the advantage of an algorithm $\mathcal{A}$ in solving the q_1-BDHI problem as follows:

$$Adv_G^{q_1-BDHI}(\mathcal{A}) = |Pr[e(g_1, g_2)^{\frac{1}{x}} \leftarrow \\ \mathcal{A}(g_1, xg_2, x^2g_2, x^3g_2, \cdots, x^{q_1}g_2)]|$$

where the probability is over the random choice of generator $g_1, g_2 \in G$, the randomly chosen integers x, and the random bits used by A. We say that the (k, t, ϵ)-q_1-BDHI assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the q_1-BDHI problem in G under a security parameter k.

C. Our Definition for IBPRE

In this section, we give our definition and security model for identity based PRE scheme, which is based on [9], [18].

Definition 3: An identity based PRE scheme is tuple of algorithms (Setup, KeyGen, Encrypt, Decrypt, RKGen, Reencrypt):

- Setup(1^k). On input a security parameter, the algorithm outputs both the master public parameters which are distributed to users, and the master secret key (msk) which is kept private.
- KeyGen(params, msk, ID). On input an identity $ID \in \{0,1\}^*$ and the master secret key, outputs a decryption key sk_{ID} corresponding to that identity.
- Encrypt(params, ID, m). On input a set of public parameters, an identity $ID \in \{0,1\}^*$ and a plaintext $m \in M$, output c_{ID}, the encryption of m under the specified identity.
- RKGen(params, msk, sk_{ID_1}, sk_{ID_2}, ID_1, ID_2). On input secret keys msk, sk_{ID_1}, sk_{ID_2}, and identities $ID \in \{0,1\}^*$, PKG, the delegator and the delegatee interactively generat the re-encryption key $rk_{ID_1 \to ID_2}$, the algorithm output it.
- Reencrypt(params, $rk_{ID_1 \to ID_2}$, c_{ID_1}). On input a ciphertext c_{ID_1} under identity ID_1, and a re-encryption key $rk_{ID_1 \to ID_2}$, outputs a re-encrypted ciphertext c_{ID_2}.

- Decrypt(params, sk_{ID}, c_{ID}). Decrypts the ciphertext c_{ID} using the secret key sk_{ID}, and outputs m or $\perp$.

D. Our Security Models for IBPRE

PKG **Security.**

In PRE from IBE and IBE, PKG's master key can not leverage even if the delegator, the delegatee and proxy collude.

Definition 4: **(PKG-OW)** A PRE scheme from IBE to IBE is one way secure for PKG if the probability

$$\begin{aligned} Pr[\{(ID_x, sk_{ID_x}) \leftarrow KeyGen(\cdot)\},\\ \{(ID_h, sk_{ID_h}) \leftarrow KeyGen(\cdot)\},\\ \{R_{hx} \leftarrow RKGen(msk, sk_{ID_h}, sk_{ID_x}, \cdot)\},\\ \{R_{xh} \leftarrow RKGen(msk, sk_{ID_x}, sk_{ID_h}, \cdot)\},\\ \{R_{hh} \leftarrow RKGen(msk, sk_{ID_h}, sk_{ID_h}, \cdot)\},\\ \{R_{xx} \leftarrow RKGen(msk, sk_{ID_x}, sk_{ID_x}, \cdot)\},\\ mk' \leftarrow A^{O_{renc}}(\{sk_{ID_x}\}, \{sk_{ID_h}\}, \{R_{xh}\},\\ \{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\}, \{parms\}) : mk = mk'] \end{aligned}$$

is negligibly close to 0 for any PPT adversary A. The notations in this game are same as Definition 5.

Delegator Security.

In PRE from IBE to IBE, we consider the case that proxy and delegatee are corrupted.

Definition 5: **(DGA-IBE-IND-ID-CPA)** A PRE scheme from IBE to IBE is DGA[1]-IBE-IND-ID-CPA secure if the probability

$$\begin{aligned} Pr[\{(ID^\star, sk_{ID^\star}) \leftarrow KeyGen(\cdot)\}\\ \{(ID_x, sk_{ID_x}) \leftarrow KeyGen(\cdot)\},\\ \{(ID_h, sk_{ID_h}) \leftarrow KeyGen(\cdot)\},\\ \{R_{hx} \leftarrow RKGen(msk, sk_{ID_h}, sk_{ID_x}, \cdot)\},\\ \{R_{xh} \leftarrow RKGen(msk, sk_{ID_x}, sk_{ID_h}, \cdot)\},\\ \{R_{hh} \leftarrow RKGen(msk, sk_{ID_h}, sk_{ID_h}, \cdot)\},\\ \{R_{xx} \leftarrow RKGen(msk, sk_{ID_x}, sk_{ID_x}, \cdot)\},\\ \{R_{\star h} \leftarrow RKGen(msk, sk_{ID^\star}, sk_{ID_h}, \cdot)\},\\ \{R_{\star x} \leftarrow RKGen(msk, sk_{ID^\star}, sk_{ID_x}, \cdot)\},\\ (m_0, m_1, St) \leftarrow A^{O_{renc}}(ID^\star, \{sk_{ID_x}\},\\ \{R_{xh}\}, \{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\}, \{R_{\star h}\}, \{R_{\star x}\}),\\ d^\star \xleftarrow{R} \{0,1\}, C^\star = Encrypt(m_{d^\star}, ID^\star),\\ d' \leftarrow A^{\emptyset_{renc}}(C^\star, St) : d' = d^\star] \end{aligned}$$

is negligibly close to $1/2$ for any PPT adversary A. In our notation, St is a state information maintained by $\mathcal{A}$ while $(ID^\star, sk_{ID^\star})$ is the target user's pubic and private key pair generated by the challenger which also chooses other keys for corrupt and honest parties. For other honest parties, keys are subscripted by h and we subscript corrupt keys by x. Oracles $\mathcal{O}_{renc}$ proceeds as follows:

- **Re-encryption** $\mathcal{O}_{renc}$**:** on input (pk_i, ID_j, C_{pk_i}), where C_{pk_i} is the ciphertext under the public key pk_i , pk_i were produced by $\text{Keygen}_{\text{CBE}}$, ID_j were produced by $\text{Keygen}_{\text{IBE}}$, this oracle responds with 'invalid' if C_{pk_i} is not properly shaped w.r.t. pk_i. Otherwise the re-encrypted first level ciphertext $C_{ID} = ReEnc(KeyGen_{PRO}(sk_i, ID_j, mk, parms), ID_j, parms, C_{pk_i})$ is returned to $\mathcal{A}$.

Delegatee Security.

In PRE from IBE to IBE, we consider the case that proxy and delegator are corrupted.

Definition 6: **(DGE-IBE-IND-ID-CPA)** A PRE scheme from IBE to IBE is DGE[2]-IBE-IND-ID-CPA secure if the probability

$$\begin{aligned} Pr[\{(ID^\star, sk_{ID^\star}) \leftarrow KeyGen(\cdot)\}\\ \{(ID_x, sk_{ID_x}) \leftarrow KeyGen(\cdot)\},\\ \{(ID_h, sk_{ID_h}) \leftarrow KeyGen(\cdot)\},\\ \{R_{hx} \leftarrow RKGen(msk, sk_{ID_h}, sk_{ID_x}, \cdot)\},\\ \{R_{xh} \leftarrow RKGen(msk, sk_{ID_x}, sk_{ID_h}, \cdot)\},\\ \{R_{hh} \leftarrow RKGen(msk, sk_{ID_h}, sk_{ID_h}, \cdot)\},\\ \{R_{xx} \leftarrow RKGen(msk, sk_{ID_x}, sk_{ID_x}, \cdot)\},\\ \{R_{h\star} \leftarrow RKGen(msk, sk_{ID_h}, sk_{ID^\star}, \cdot)\},\\ \{R_{x\star} \leftarrow RKGen(msk, sk_{ID_x}, sk_{ID^\star}, \cdot)\},\\ (m_0, m_1, St) \leftarrow A^{O_{renc}}(ID^\star, \{sk_{ID_x}\}, \{R_{xh}\},\\ \{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\}, \{R_{h\star}\}, \{R_{x\star}\}),\\ d^\star \xleftarrow{R} \{0,1\}, C^\star = Encrypt(m_{d^\star}, ID^\star),\\ d' \leftarrow A^{\emptyset_{renc}}(C^\star, St) : d' = d^\star] \end{aligned}$$

is negligibly close to $1/2$ for any PPT adversary A. The notations in this game are same as Definition 5.

III. IBPRE Based on BB_2 IBE

A. Review of the BB_2 Identity Based Encryption

Let $\mathbb{G}$ be a bilinear group of prime order p and g be a generator of $\mathbb{G}$. For now, we assume that the public keys (ID) are elements in Z_p^*. We show later that arbitrary identities in $\{0,1\}^*$ can be used by first hashing ID using a collision resistant hash $H : \{0,1\}^* \rightarrow Z_p^*$. We also assume that the messages to be encrypted are elements in $\mathbb{G}_1$. The IBE system works as follows:

1) **Setup:** To generate IBE parameters, select random elements $(x, y) \in Z_p^*$ and define $X = g^x$ and $Y = g^y$. The public parameters parms and the secret master − key are given by parms $= (g, g^x, g^y)$, master − key $= (x, y)$
2) **KeyGen**(master − key, **ID**)**:** To create a private key for the public key $\text{ID} \in Z_p^*$:
   a) pick a random $r \in Z_p$ and compute $K = g^{\frac{1}{(ID+x+ry)}} \in \mathbb{G}$,
   b) output the private key $d_{ID} = (r, K)$. In the unlikely event that $x + ry + ID = 0 \mod p$, try again with a new random value for r.

[1]DGA means Delegator

[2]DGE means Delegatee.

3) **Encrypt(parms, ID, M):** To encrypt a message $M \in G_1$ under public key $ID \in Z_p^*$, pick a random $s \in Z_p^*$ and output the ciphertext $C = (g^{s \cdot ID}X^s, Y^s, e(g,g)^s \cdot M)$. Note that $e(g,g)$ can be precomputed once and for all so that encryption does not require any pairing computations.
4) **Decrypt(d_{ID}, C):** To decrypt a ciphertext $C = (A, B, C)$ using the private key $d_{ID} = (r, K)$, output $C/e(AB^r, K)$. Indeed, for a valid ciphertext we have

$$\frac{C}{e(AB^r, K)} = \frac{C}{e(g^{s(ID+x+ry)}, g^{1/(ID+x+ry)})}$$

$$= \frac{C}{e(g,g)^s} = M$$

Remark 1: This scheme is an efficient identity based encryption and proved to be IND-sID-CPA secure in the standard model. In Eurocrypt'06, Gentry proposed a practical identity based encryption based on this scheme which can achieve IND-ID-CCA2 with tight security proof [10]. Thus this scheme plays an important role in the field of identity based encryption.

B. Our PRE Scheme Based on BB_2 Identity Based Encryption

1) **ReKeyGen$_{ID \to ID'}$:** PKG chooses a collision resistent hash function $H : \{0,1\}^{3|p|} \to Z_p^*$ and a random seed $t \in Z_p^*$, and computes $k = H(ID, ID', t)$. He computes $rk_{ID \to ID'} = (rk_1, rk_2, rk_3) = (r, \frac{ID'+x+r'y}{ID+x+ry} + k \mod p, g^{\frac{k}{(ID'+x+r'y)}})$ and sends them to the proxy as the re-encryption key. We note that PKG chooses a different k for every different user pair (ID, ID').
2) **Encrypt(parms, ID, M):** Same as the Encrypt algorithm in III-A.
3) **ReEnc** $(rk_{ID \to ID'}, \mathsf{parms}, \widetilde{C_{ID}}, ID')$**:**. On input the ciphertext $\widetilde{C_{ID}} = (\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3}) = (g^{s \cdot ID}X^s, Y^s, e(g,g)^s \cdot M)$, the proxy computes $\widehat{C_{ID'}} = (\widehat{C_1}, \widehat{C_2}) = (\widetilde{C_1}\widetilde{C_2}^{rk_1}, \widetilde{C_3}e((\widetilde{C_1}\widetilde{C_2}^{rk_1})^{rk_2}, rk_3))$, and sends it to the delegatee.
4) **Decrypt$_1$($\widehat{C_{ID'}}, d_{ID'}$):** On input a re-encrypted ciphertext $\widehat{C_{ID'}} = (\widehat{C_1}, \widehat{C_2})$, the delegatee decrypts like this: $M = \frac{\widehat{C_2}}{e(\widehat{C_1}, {d_{ID'}}^2)} = \frac{\widehat{C_2}}{e(\widehat{C_1}, K')}$ and returns M.
5) **Decrypt$_2$(d_{ID}, C):** On input a normal ciphertext, the delegatee do the same as the Decrypt algorithm in III-A.
6) **Check:**. On input a ciphertext $\widetilde{C_{ID}} = (\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3})$, the proxy computes $v_1 = e(\widetilde{C_1}, Y)$ and $v_2 = e(\widetilde{C_2}, g^{ID}X)$, if $v_1 = v_2$, then return "Valid", else return "Invalid".

First we verify our scheme's correctness as following.

$$\begin{aligned}
\frac{\widehat{C_2}}{e(\widehat{C_1}, K')} &= \frac{\widetilde{C_3}e(\widetilde{C_1}\widetilde{C_2}^{rk_1}, rk_3)}{e((\widetilde{C_1}\widetilde{C_2}^{rk_1})^{rk_2}, g^{\frac{1}{ID'+x+r'y'}})} \\
&= \frac{e(g,g)^s \cdot M \cdot e(g^{s \cdot ID}X^sY^{sr}, g^{\frac{k}{(ID'+x+r'y)}})}{e((g^{s \cdot ID}X^sY^{sr})^{\frac{ID'+x+r'y}{ID+x+ry}+k}, g^{\frac{1}{ID'+x+r'y'}})} \\
&= \frac{e(g,g)^s \cdot M \cdot e(g^{s(ID+x+ry)}, g^{\frac{k}{(ID'+x+r'y)}})}{e(g^{s(ID'+x+r'y)}, g^{\frac{1}{ID'+x+r'y'}})e(g^{sk(ID+x+ry)}, g^{\frac{1}{ID'+x+r'y'}})} \\
&= M
\end{aligned}$$

Remark 2: In our scheme, we let $rk_1 = r$ which is a part of delegator's secret key. We remark that let r be public should still preserve BB_2 IBE scheme's IND-sID-CPA security.

C. Security Analysis

Theorem 1: Suppose Decision q-BDHI assumption holds in $\mathbb{G}$, then our scheme is DGA-IBE-IND-sID-CPA secure for the proxy and delegatee's colluding.

Proof: Suppose $\mathcal{A}$ has advantage in attacking our PRE system. We build an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ to solve the Decision $q - BDHI$ problem in $\mathbb{G}$. Algorithm $\mathcal{B}$ is given as input a random $(q+2)$-tuple $(g, g^\alpha, g^{(\alpha^2)}, ..., g^{(\alpha^q)}, T) \in (\mathbb{G}^*)^{q+1} \times \mathbb{G}_1$ that is either sampled from P_{BDHI} (where $T = e(g,g)^{\frac{1}{\alpha}}$) or from R (where T is uniform and independent in $\mathbb{G}_1$). Algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g,g)^{1/\alpha}$ and 0 otherwise. Algorithm $\mathcal{B}$ works by interacting with $\mathcal{A}$ in a selective identity game as follows:

Preparation. Algorithm $\mathcal{B}$ builds a generator $h \in \mathbb{G}^*$ for which it knows $q-1$ pairs of the form $(w_i, h^{1/(\alpha+w_i)})$ for random $w_1, ..., w_{q-1} \in Z_p^*$. This is done as follows:

1) Pick random $w_1, ..., w_{q-1} \in Z_p^*$ and let $f(z)$ be the polynomial $f(z) = \prod_{i=1}^{q-1}(z + w_i)$. Expand the terms of f to get $f(z) = \sum_{i=0}^{q-1} c_i x_i$. The constant term c_0 is non-zero.
2) Compute $h = \prod_{i=0}^{q-1}(g^{(\alpha^i)})^{c_i} = g^{f(\alpha)}$ and $u = \prod_{i=1}^{q}(g^{(\alpha^i)})^{c_{i-1}} = g^{\alpha f(\alpha)}$. Note that $u = h^\alpha$.
3) Check that $h \in G^*$. Indeed if we had $h = 1$ in $\mathbb{G}$ this would mean that $w_j = -\alpha$ for some j easily identifiable w_j, at which point $\mathcal{B}$ would be able to solve the challenge directly. We thus assume that all $w_j \neq -\alpha$.
4) Observe that for any $i = 1, ..., q-1$, it is easy for $\mathcal{B}$ to construct the pair $(w_i, h^{1/(\alpha+w_i)})$. To see this, write $f_i(z) = f(z)/(z + w_i) = \sum_{i=0}^{q-2} d_i Z_i$. Then $h^{1/(\alpha+w_i)} = g^{f_i(\alpha)} = \prod_{i=0}^{q-2}(g^{(\alpha^i)})^{d_i}$.
5) Next $\mathcal{B}$ computes

$$\begin{aligned}
T_h &= T^{c_0 f(\alpha)} \cdot T_0 \\
T_0 &= \prod_{i=0}^{q-1}\prod_{j=0}^{q-2} e(g^{(\alpha^i)}, g^{(\alpha^j)})^{c_i c_{j+1}}
\end{aligned}$$

Observe that if $T = e(g,g)^{1/\alpha}$ then $T_h = e(g^{f(\alpha)/\alpha}, g^{f(\alpha)}) = e(h,h)^{1/\alpha}$. On the contrary, if T is uniform in G_1, then so is T_h.

We will be using the values h, u, T_h and the pairs $(w_i, h^{1/(\alpha+w_i)})$ for $i = 1, ..., q-1$ throughout the simulation.

1) **Initialization.** The selective identity game begins with $\mathcal{A}$ first outputting an identity $ID^\star \in Z_p^*$ that it intends to attack.
2) **Setup.** To generate the system parameters,algorithm $\mathcal{B}$ does the following:
   a) Pick random $a, b \in Z_p^*$ under the constraint that $ab = ID^\star$.
   b) Compute $X = u^{-a}h^{-ab} = h^{-a(\alpha+b)}$ and $Y = u = h^\alpha$.
   c) Publish $\mathsf{parms} = (h, X, Y)$ as the public parameters. Note that X, Y are independent of $ID^\star$ in the adversary's view.
   d) We implicitly define $x = -a(\alpha+b)$ and $y = \alpha$ so that $X = h^x$ and $Y = h^y$. Algorithm $\mathcal{B}$ does not know the value of x or y, but does know the value of $x + ay = -ab = -ID^\star$.
3) **Phase 1**.
   - *"$\mathcal{A}$ issues up to $q_s < q$ private key queries".* Consider the i-th query for the private key corresponding to public key $ID_i \neq ID^\star$. We need to respond with a private key $(r, h^{\frac{1}{(ID_i+x+ry)}})$ for a uniformly distributed $r \in Z_p$. Algorithm $\mathcal{B}$ responds to the query as follows:
     a) Let $(w_i, h^{1/(\alpha+w_i)})$ be the $i-$th pair constructed during the preparation step. Define $h_i = h^{1/(\alpha+w_i)}$.
     b) $\mathcal{B}$ first constructs an $r \in Z_p$ satisfying $(r-a)(\alpha+w_i) = ID_i + x + ry$. Plugging in the values of x and y the equation becomes
     $$(r-a)(\alpha+w_i) = ID_i - a(\alpha+b) + r\alpha$$
     We see that the unknown α cancels from the equation and we get $r = a + \frac{ID_i - ab}{w_i} \in Z_p$ which B can evaluate.
     c) Now $(r, h_i^{1/(r-a)})$ is a valid private key for ID for two reasons. First,
     $$\begin{aligned} & h_i^{1/(r-a)} = (h^{1/(\alpha+w)})^{1/(r-a)} \\ = \; & h^{1/(r-a)(\alpha+w_i)} = h^{1/(ID_i+x+ry)} \end{aligned}$$
     as required. Second, r is uniformly distributed among all elements in Z_p for which $ID_i + x + ry \neq 0$ and $r \neq a$. This is true since w is uniform in $Z_p/\{0, -\alpha\}$ and is currently independent of $\mathcal{A}$'s view. Algorithm $\mathcal{B}$ gives $\mathcal{A}$ the private key $(r, h_i^{1/(r-\alpha)})$. For completeness, we note that $\mathcal{B}$ can construct the private key for ID_i with $r = a$ as $(r, h^{1/ID_i - ID^\star})$. Hence,the r in the private key given to $\mathcal{A}$ can be made uniform among all $r \in Z_p$ for which $ID + x + ry \neq 0$ as required.

     We point out that this procedure will fail to produce the private key for $ID_i = ID^\star$ since in that case we get $r = a$ and $ID + x + ry = 0$. Hence, B can generate private keys for all public keys except for $ID^\star$.
   - *"$\mathcal{A}$ issues up to re-encryption key queries on (ID_i, ID_j)".*
     The challenger $\mathcal{B}$ chooses a randomly $x \in Z_p^*$ and sets $rk_2 = \frac{ID_j+x+r_jy}{ID_i+x+r_iy} + k = x$, he computes re-encryption key as follows:
     $$\begin{aligned} rk_1 &= r_i, rk_2 = x \\ rk_3 &= g^{\frac{k}{ID_j+x+r_jy}} = g^{\frac{x - \frac{ID_j+x+r_jy}{ID_i+x+r_iy}}{ID_j+x+r_jy}} \\ &= g^{\frac{x}{ID_j+x+r_jy}} \cdot g^{-\frac{1}{ID_i+x+r_iy}} = h_j^{\frac{x}{r_j-a}} \cdot h_i^{\frac{1}{r_i-a}} \end{aligned}$$
     thus our simulation is a perfect simulation. Because x is uniformly in Z_p^*, the adversary (including delegator and proxy colluding or delegatee and proxy colluding) can not get any useful information from it.
   - *"$\mathcal{A}$ issues up to rekey generation queries on $(ID^\star, ID)$".*
     Do the same as the above.
   - *"$\mathcal{A}$ issues up to re-encryption queries on (C_{ID_i}, ID_i, ID_j)".*
     The challenge $\mathcal{B}$ runs $\mathsf{ReEnc}(rk_{ID_i \to ID_j}, C_{ID_i}, ID_j)$ and returns the results.
4) **Challenge.** $\mathcal{A}$ outputs two messages $M_0, M_1 \in G$. Algorithm $\mathcal{B}$ picks a random bit $b \in \{0, 1\}$ and a random $l \in Z_p^*$. It responds with the ciphertext $C^\star = (h^{-al}, h^l, T_h^l \cdot M_b)$. Define $s = l/\alpha$. On the one hand, if $T = e(h, h)^{1/\alpha}$ we have
   $$\begin{aligned} h^{-al} &= h^{a\alpha(l/\alpha)} = h^{(x+ab)(l/\alpha) = h^{sID^\star} \cdot X^s} \\ h^l &= Y^{l/\alpha} = Y^s \\ T_h^l &= e(h, h)^{l/\alpha} = e(h, h)^s \end{aligned}$$
   It follows that $C^\star$ is a valid encryption of M_b under $ID^\star$, with the uniformly distributed randomization value $s = l/\alpha$. On the other hand, when T is uniform in G_1 ,then, in the adversary's view $C^\star$ is independent of the bit b.
5) **Phase 2.** $\mathcal{A}$ issues more private key queries, for a total of at most $q_s < q$. Algorithm $\mathcal{B}$ responds as before. $\mathcal{A}$ issues more other queries like in Phase 1 except natural constraints and Algorithm $\mathcal{B}$ responds as before.
6) **Guess.** Finally, $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$. If $b = b'$ then $\mathcal{B}$ outputs 1 meaning $T = e(g, g)^{1/\alpha}$. Otherwise,it outputs 0 meaning $T \neq e(g, g)^{1/\alpha}$.

When $T = e(g, g)^{1/\alpha}$ then $\mathcal{A}$'s advantage for breaking the scheme is same as $\mathcal{B}$'s advantage for solving q-BDHI problem. ■

Theorem 2: Suppose the q-BDHI assumption holds, then our scheme is DGE-IBE-IND-sID-CPA secure for the proxy and delegator's colluding.

Proof: The security proof is same as the above theorem except that it does not allow *"$\mathcal{A}$ issues up to rekey generation queries on $(ID, ID^\star)$"*, for $\mathcal{B}$ does not know the private key corresponding to $ID^\star$. ■

Theorem 3: Suppose the q-BDHI assumption holds, then our scheme is KGC-OW secure for the proxy, delegatee and delegator's colluding.

Proof: We just give the intuition for this theorem. The master-key is (x, y), and delegator's private key is $(r_i, g^{\frac{1}{ID_i+x+r_iy}})$, the delegatee's private key is $(r_j, g^{\frac{1}{ID_j+x+r_jy}})$, the proxy re-encryption key is $(r_i, \frac{ID_j+x+r_jy}{ID_i+x+r_iy}+k \mod p, g^{\frac{k}{ID'+x+r'y}})$. Although $rk_1 = r_i$, this does not give adversary any more help for $g^{\frac{1}{ID_i+x+r_iy}}$ or x, y. Because the re-encryption key is uniformly distributed in Z_p^*, and the original BB_2 IBE is secure, we can conclude that (x, y) can not be disclosed by the proxy, delegatee and delegator's colluding. ■

IV. IBPRE Based on SK IBE

A. Review of the SK Identity Based Encryption

SK-IBE is specified by four polynomial time algorithms:

1) **Setup.** Given a security parameter k, the parameter generator follows the steps.
   a) Generate three cyclic groups G_1, G_2 and G_T of prime order q, an isomorphism φ from G_2 to G_1, and a bilinear pairing map $e : G_1 \times G_2 \to G_T$. Pick a random generator $P_2 \in G^*$ and set $P_1 = \varphi(P_2)$.
   b) Pick a random $s \in Z_q^*$ and compute $P_{pub} = sP_1$.
   c) Pick four cryptographic hash functions $H_1 : \{0,1\}^* \to Z_q^*, H_2 : G_T \to \{0,1\}^n, H_3 : \{0,1\}^n \times \{0,1\}^n \to Z_q^*$ and $H_4 : \{0,1\}^n \to \{0,1\}^n$ for some integer $n > 0$.

   The message space is $M = \{0,1\}^n$. The ciphertext space is $C = G_1^* \times \{0,1\}^n \times \{0,1\}^n$. The master public key is $M_{pk} = (q, G_1, G_2, G_T, \varphi, e, n, P_1, P_2, P_{pub}, H_1, H_2, H_3, H_4)$, and the master secret key is $M_{sk} = s$.
2) **Extract.** Given an identifier string $ID_A \in \{0,1\}^*$ of identity A, M_{pk} and M_{sk}, the algorithm returns $d_A = \frac{1}{s+H_1(ID_A)}P_2$.
3) **Encrypt.** Given a plaintext $m \in M$, ID_A and M_{pk}, the following steps are performed.
   a) Pick a random $\sigma \in \{0,1\}^n$ and compute $r = H_3(\sigma, m)$.
   b) Compute $Q_A = H_1(ID_A)P_1 + P_{pub}$, $g^r = e(P_1, P_2)^r$.
   c) Set the ciphertext to $C = (rQ_A, \sigma \oplus H_2(g^r), m \oplus H_4(\sigma))$.
4) **Decrypt.** Given a ciphertext $C = (U, V, W) \in \mathcal{C}, ID_A, d_A$ and M_{pk}, follows the steps:
   a) Compute $g' = e(U, d_A)$ and $\sigma' = V \oplus H_2(g')$.
   b) Compute $m' = W \oplus H_4(\sigma)$ and $r' = H_3(\sigma', m')$.
   c) if $U \neq r'(H_1(ID_A)P_1 + P_{pub})$, output $\perp$, else return m' as the plaintext.

B. Our Proposed PRE Based On SK Identity Based Encryption

Our proposed PRE scheme based on SK identity based encryption are as following:

1) **Setup.** Same as the above scheme IV-A.
2) **Extract.** Same as the above scheme IV-A.
3) **RKGen:** The PKG chooses a collision resistent hash function $H_5 : \{0,1\}^{3|p|} \to Z_p^*$ and random seeds $s_2, s_1 \in Z_p^*$, it computes $k_2 = H_5(ID, ID', s_2)$, $k_1 = H_5(ID, ID', s_1)k_2$. He computes $rk_{ID \to ID'} = (rk_1, rk_2, rk_3) = (\frac{s+H_1(ID')+k_1}{(s+H_1(ID))} \mod p, \frac{k_2}{(H_1(ID)+s)} \mod p, \frac{k_1}{k_2(s+H_1(ID'))}P_2)$.
4) **Encrypt.** Same as the above scheme IV-A.
5) **Reencrypt:**. On input the ciphertext $\widehat{C_{ID}} = (\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3}) = (rQ_{ID}, \sigma \oplus H_2(g^r), m \oplus H_4(\sigma))$, the proxy computes $\widehat{C_{ID'}} = (\widehat{C'_1}, \widehat{C'_2}, \widehat{C'_3}, \widehat{C'_4}, \widehat{C'_5}) = (rk_1\widetilde{C_1}, e(rk_2\widetilde{C_1}, rk_3), \widetilde{C_2}, \widetilde{C_3}, \widetilde{C_1})$, and sends it to the delegatee.
6) **Decrypt$_1$.** Given a first level ciphertext - re-encrypted ciphertext $\widehat{C_{ID'}} = (\widehat{C'_1}, \widehat{C'_2}, \widehat{C'_3}, \widehat{C'_4}, \widehat{C'_5})$, follows the steps:
   a) Compute $g' = \frac{e(\widehat{C'_1}, d_{ID'})}{\widehat{C'_2}}$ and $\sigma' = \widehat{C'_3} \oplus H_2(g')$.
   b) Compute $m' = \widehat{C'_4} \oplus H_4(\sigma')$ and $r' = H_3(\sigma', m')$.
7) **Decrypt$_2$.** Given a second level ciphertext - normal ciphertext, do the same as the algorithm Decrypt in the above scheme IV-A.
8) **Verify.** If $\widehat{C'_5} \neq r'(H_1(ID)P_1 + P_{pub})$, output $\perp$, else return m' as the plaintext.

First we verify our scheme's correctness as following.

$$
\begin{aligned}
g' &= \frac{e(\widehat{C'_1}, d_{ID'})}{\widehat{C'_2}} = \frac{e(rk_1\widetilde{C_1}, d_{ID'})}{e(rk_2\widetilde{C_1}, rk_3)} \\
&= \frac{e(\frac{s+H_1(ID')+k_1}{s+H_1(ID)} \cdot rQ_{ID}, \frac{1}{s+H_1(ID')}P_2)}{e(\frac{k_2}{(H_1(ID)+s)} \cdot rQ_{ID}, \frac{k_1}{k_2(s+H_1(ID'))}P_2)} \\
&= \frac{e(rP_1, P_2)e(rk_1P_1, \frac{1}{s+H_1(ID')}P_2)}{e(rP_1, \frac{k_1}{s+H_1(ID')}P_2)} = e(P_1, P_2)^r = g^r \\
\sigma' &= C'_3 \oplus H_2(g') = \sigma \oplus H_2(g^r) \oplus H_2(g^r) = \sigma
\end{aligned}
$$

$$
\begin{aligned}
m' &= \widehat{C'_4} \oplus H_4(\sigma') \\
&= m \oplus H_4(\sigma) \oplus H_4(\sigma') = m \oplus H_4(\sigma) \oplus H_4(\sigma) = m, \\
r' &= H_3(\sigma', m') = H_3(\sigma, m) = r \\
\widehat{C'_5} &= \widetilde{C_1} = rQ_{ID} = r(H_1(ID)P_1 + P_{pub}) \\
&= r'(H_1(ID)P_1 + P_{pub})
\end{aligned}
$$

Remark 3: In our scheme, we must note that the PKG needs to compute different (k_1, k_2) for every different user pair (ID, ID'). Otherwise, if the adversary know $(\frac{s+H_1(ID')+k_1}{(s+H_1(ID))} \mod p, \frac{k_2}{(H_1(ID)+s)} \mod p)$ for two different pair (ID, ID') but the same (k_1, k_2), he can compute s, which is not secure at all.

Remark 4: In our scheme, we require $k_1 = H_5(ID, ID', s_1)k_2$. The reason of k_2 is a factor of k_1 is just for security proof.

C. Security Analysis

Interestingly, our PRE based on SK IBE scheme even can achieve IND-Pr-ID-CCA2 secure while all the above PRE scheme can only achieve IND-Pr-sID-CPA secure.

Theorem 4: Suppose q-BDHI assumption holds in $\mathbb{G}$, then our scheme is DGA-IBE-IND-ID-CCA2 secure for the proxy and delegatee's colluding.

Proof: The proof combines the following three lemmas.

Lemma 1: Suppose that H is a random oracle and that there exists an IND-ID-CCA adversary $\mathcal{A}$ against PRE-SK-IBE with advantage $\varepsilon(k)$ which makes at most q_1 distinct queries to H (note that H can be queried directly by $\mathcal{A}$ or indirectly by an extraction query,a decryption query or the challenge operation).Then there exists an IND-CCA adversary $\mathcal{B}$ which runs in time $O(time(\mathcal{A}) + q_D \cdot (T + \Gamma_1))$ against the following PRE-BasicPub^{hy} scheme with advantage at least $\varepsilon(k)/q_1$ where T is the time of computing pairing and Γ_1 is the time of a multiplication operation 1 in $\mathbb{G}_1$.

PRE-BasicPub^{hy} is specified by six algorithms: KeyGen, RKGen, Encrypt, Reencrypt, Decrypt$_1$, Decrypt$_2$.

1) **KeyGen:** Given a security parameter k, the parameter generator follows the steps.
   a) Identical with step 1 in Setup algorithm of PRE-SK-IBE.
   b) The PKG pick a random $s \in Z_q^*$ and compute $P_{pub} = sP$. Randomly choose different elements $h_i \in Z_q^*$ and compute $\frac{1}{h_i+s}P$ for $0 \leq i \leq q_1$. Randomly choose different elements $h_0' \in Z_q^*$ and compute $\frac{1}{h_0'+s}P$.
   c) Pick three cryptographic hash functions: $H_2 : G_T \to \{0,1\}^n$, $H_3 : \{0,1\}^n \times \{0,1\}^n \to Z_q^*$ and $H_4 : \{0,1\}^n \to \{0,1\}^n$ for some integer $n > 0$.

   The message space is $M = \{0,1\}^n$. The ciphertext space is $C = G_1^* \times \{0,1\}^n \times \{0,1\}^n$. The public key for delegator is $K_{pubA} = (q, G_1, G_2, G_T, \varphi, e, n, P_1, P_2, P_{pub}, h_0, (h_1, \frac{1}{h_1+s}P_2), \cdots, (h_i, \frac{1}{h_i+s}P_2), \cdots, (h_{q_1-1}, \frac{1}{h_{q_1-1}+s}P_2), H_2, H_3, H_4)$ and the private key is $d_A = \frac{1}{h_0+s}P$. Note that $e(h_0P_1 + P_{pub}, d_A) = e(P_1, P_2)$. The public key for delegatee is $K_{pubB} = (q, G_1, G_2, G_T, \varphi, e, n, P_1, P_2, P_{pub}, h_0', (h_1, \frac{1}{h_1+s}P_2), \cdots, (h_i, \frac{1}{h_i+s}P_2), \cdots, (h_{q_1-1}, \frac{1}{h_{q_1-1}+s}P_2), H_2, H_3, H_4)$ and the private key is $d_B = \frac{1}{h_0'+s}P$. Note that $e(h_0'P_1 + P_{pub}, d_B) = e(P_1, P_2)$.
2) **RKGen:** The PKG chooses a collision resistent hash function $H_5 : \{0,1\}^{3|p|} \to Z_p^*$ and random seeds $t_1, t_2 \in Z_p^*$, and computes $k = H_5(h_0, h_0', t_1)$. He computes $rk_{A\to B} = (rk_1, rk_2, rk_3) = (\frac{s+h_0'+k_1}{s+h_0} \bmod p, \frac{k_2}{s+h_0} \bmod p, \frac{k_1}{k_2(s+h_0')}P_2)$. He sends $rk_{A\to B}$ to the proxy as the re-encryption key via authenticated channel.
3) **Encrypt:** Given a plaintext $m \in M$ and the public key K_{pubA} and K_{pubB},
   a) Pick a random $\sigma \in \{0,1\}^n$ and compute $r = H(\sigma, m)$,and $g^r = e(P_1, P_2)^r$.
   b) For the delegator, set the ciphertext to be $C = (r(h_0P_1 + P_{pub}), \sigma \oplus H_2(g^r), m \oplus H(\sigma))$.
   c) For the delegatee, set the ciphertext to be $C = (r(h_0'P_1 + P_{pub}), \sigma \oplus H_2(g^r), m \oplus H(\sigma))$.
4) **Reencrypt:**. On input the ciphertext $C_A = (C_1, C_2, C_3) = (rQ_{ID}, \sigma \oplus H_2(g^r), m \oplus H_4(\sigma))$, the proxy computes $C_B = (C_1', C_2', C_3', C_4', C_5') = (rk_1C_1, e(rk_2C_1, rk_3), C_2, C_3, C_1)$, and sends it to the delegatee.
5) **Decrypt$_1$:** For the delegator, given a ciphertext $C_A = (U, V, W)$, K_{pubA}, and the private key d_A
   a) Compute $g' = e(U, d_A)$ and $\sigma' = V \oplus H(g')$,
   b) Compute $m' = W \oplus H_4(\sigma')$ and $r' = H_3(\sigma', m')$,
   c) If $U \neq r'(h_0P_1 + P_{pub})$,reject the ciphertext, else return m' as the plaintext.
6) **Decrypt$_2$:** For the delegatee, given a ciphertext $C_B = (C_1', C_2', C_3', C_4', C_5')$:
   a) Compute $g' = \frac{e(C_1', d_B)}{C_2'}$ and $\sigma' = C_3' \oplus H_2(g')$.
   b) Compute $m' = C_4' \oplus H_4(\sigma)$ and $r' = H_3(\sigma', m')$.
   c) If $C_5' \neq r'(h_0P_1 + P_{pub})$, output $\perp$, else return m' as the plaintext.

Proof: The proof for this lemma is similar as Lemma 1 in Section 3.2 in [7]. ■

Lemma 2: Let H_3, H_4 be random oracles. Let $\mathcal{A}$ be an IND-CCA adversary against PRE-BasicPub^{hy} defined in Lemma 1 with advantage $\epsilon(k)$. Suppose $\mathcal{A}$ has running time $t(k)$, makes at most q_D decryption queries, and makes q_3 and q_4 queries to H_3 and H_4 respectively. Then there exists an IND-CPA adversary $\mathcal{B}$ against the following PRE-BasicPub scheme with advantage $\epsilon_1(k)$ and running time $t_1(k)$ where

$$\begin{aligned} \epsilon_1(k) &\geq \frac{1}{2(q_3+q_4)}[(\epsilon(k)+1)(1-\frac{2}{q})^{q_D} - 1] \\ t_1(k) &\leq t(k) + O((q_3+q_4)\cdot(n + logq)). \end{aligned}$$

PRE-BasicPub is specified by six algorithms: KeyGen, RKGen, Encrypt, Reencrypt, Decrypt$_1$, Decrypt$_2$.

1) **KeyGen:** Given a security parameter k, the parameter generator follows the steps.
   a) Identical with step 1 in algorithm KeyGen of PRE-BasicPub^{hy}.
   b) Identical with step 2 in algorithm KeyGen of PRE-BasicPub^{hy}.
   c) Pick a cryptographic hash function $H_2 : G_T \to \{0,1\}^n$ for some integer $n > 0$.

   The message space is $M = \{0,1\}^n$. The ciphertext space is $C = G_1^* \times \{0,1\}^n \times \{0,1\}^n$. The public key for delegator is $K_{pubA} =$

$(q, G_1, G_2, G_T, \varphi, e, n, P_1, P_2, P_{pub}, h_0, (h_1, \frac{1}{h_1+s}P_2), \cdots, (h_i, \frac{1}{h_i+s}P_2), \cdots, (h_{q_1-1}, \frac{1}{h_{q_1-1}+s}P_2), H_2, H_3, H_4)$ and the private key is $d_A = \frac{1}{h_0+s}P$. Note that $e(h_0P_1+P_{pub}, d_A) = e(P_1, P_2)$. The public key for delegatee is $K_{pubB} = (q, G_1, G_2, G_T, \varphi, e, n, P_1, P_2, P_{pub}, h_0', (h_1, \frac{1}{h_1+s}P_2), \cdots, (h_i, \frac{1}{h_i+s}P_2), \cdots, (h_{q_1-1}, \frac{1}{h_{q_1-1}+s}P_2), H_2, H_3, H_4)$ and the private key is $d_B = \frac{1}{h_0'+s}P$. Note that $e(h_0'P_1 + P_{pub}, d_B) = e(P_1, P_2)$.

2) **ReKeyGen:** Identical with RKGen of PRE-BasicPub^{hy} except no s generation.
3) **Encrypt:** Given a plaintext $m \in M$ and the public key K_{pub}, choose a random $r \in Z_q^*$ and compute ciphertext $C = (rP_1, r(h_0P_1 + P_{pub}), m \oplus H_2(g^r))$ where $g^r = e(P_1, P_2)^r$.
4) **Reencrypt:** Identical with Reencrypt of PRE-BasicPub^{hy}.
5) **Decrypt$_1$:** Given a ciphertext $C = (U_1, U_2, V)$, K_{pub}, and the private key d_A, compute $g' = e(U_2, d_A)$ and plaintext $m = V \oplus H_2(g')$.
6) **Decrypt$_2$:**Identical with Decrypt$_2$ of PRE-BasicPub^{hy} except no step 3(no checking step).

Proof: The proof for this lemma is similar as lemma 2 in Section 3.2 in [7], actually this is the Fujisaki-Okamoto transformation [8]. ■

Lemma 3: Let H_2 be a random oracle. Suppose there exists an IND-CPA adversary $\mathcal{A}$ against the PRE-BasicPub defined in Lemma 2 which has advantage $\epsilon(k)$ and queries H at most q_2 times. Then there exists an algorithm $\mathcal{B}$ to solve the $q_1 - BDHI$ problem with advantage at least $2\epsilon(k)/q_2$ and running time $O(time(\mathcal{A}) + q_1^2 \cdot T_2)$ where T_2 is the time of a multiplication operation in G_2.

Proof: Algorithm $\mathcal{B}$ is given as input a random $q_1 - BDHI$ instance (q,G_1, G_2,G_T, φ, P_1, P_2, xP_2, x^2P_2, ...,$x^{q_1}P_2$) where x is a random element from Z_q^*. Algorithm $\mathcal{B}$ finds $e(P_1, P_2)^{\frac{1}{x}}$ by interacting with $\mathcal{A}$ as follows: Algorithm $\mathcal{B}$ first simulates algorithm keygen of BasicPub, which was defined in Lemma 2, to create the public key as below.

1) Randomly choose different $h_0, ..., h_{q_1-1} \in Z$ and let $f(z)$ be the polynomial $f(z) = \prod_{i=1}^{q_1-1}(z + h_i)$. Reformulate f to get $f(z) = \prod_{i=0}^{q_1-1} c_i z_i$. The constant term c_0 is non-zero because $h_i \neq 0$ and c_i are computable from h_i.
2) Compute $Q_2 = \sum_{i=0}^{q_1-1} c_i x^i P_2 = f(x)P_2$ and $xQ_2 == \sum_{i=0}^{q_1-1} c_i x^{i+1} P_2 = xf(x)P_2$.
3) Check that $Q_2 \in G_2^*$. If $Q_2 = 1_{G_2}$, then there must exist an $h_i = -x$ which can be easily identified, and so, $\mathcal{B}$ solves the $q_1 - BDHI$ problem directly. Otherwise $\mathcal{B}$ computes $Q_1 = \varphi(Q_2)$ and continues.
4) Compute $f_i(z) = f(z)/(z+h_i) = \sum_{j=0}^{q_1-2} d_j z^j$ and $\frac{1}{x+h_i}Q_2 = f_i(x)P_2 = \sum_{j=0}^{q_1-2} d_j x^j P_2$ for $1 \leq i < q_1$.
5) Set $T' = \sum_{i=0}^{q_1-1} c_i x^{i-1} P_2$ and compute $T_0 = e(\varphi(T'), Q_2 + c_0P_2)$.
6) Now $\mathcal{B}$ passes $\mathcal{A}$ the public key $K_{pub} = (q, G_1, G_2, G_T, \varphi, e, n, Q_1, Q_2, xQ_1 - h_0Q_1, h_0, (h_2 + h_0, \frac{1}{h_2+x}Q_2), ..., (h_i + h_0, \frac{1}{h_i+x}Q_2), ..., (h_{q_1-1} + h_0, \frac{1}{h_{q_1-1}+x}Q_2), H_2)$(ie. setting $P_{pub} = xQ_1 - h_0Q_1$, $H_1(ID_A) = h_0$, $H_1(ID_B) = h_1 + h_0$), and the private key for A is $d_A = \frac{1}{x}Q_2$, which $\mathcal{B}$ does not know. The private key for B is $d_B = \frac{1}{h_1+x}Q_2$, which $\mathcal{B}$ knows. H_2 is a random oracle controlled by $\mathcal{B}$. Note that $e((h_i + h_0)Q_1 + P_{pub}, \frac{1}{h_i+x}Q_2) = e(Q_1, Q_2)$ for $i = 2, \cdots, q_1-1, e(h_0Q_1+P_{pub}, d_A) = e(Q_1, Q_2)$, $e((h_1 + h_0)Q_1 + P_{pub}, d_B) = e(Q_1, Q_2)$. Hence K_{pub} is a valid public key of A in BasicPub .

Now $\mathcal{B}$ starts to respond to queries as follows.

1) **Phase 1**
   a) **H$_2$ Query**(X_i)**.** At any time algorithm $\mathcal{A}$ can issue queries to the random oracle H_2. To respond to these queries C maintains a list of tuples called H_2^{list}. Each entry in the list is a tuple of the form (X_i, ζ_i) indexed by X_i. To respond to a query on X_i, $\mathcal{B}$ does the following operations:
      i) If on the list there is a tuple indexed by X_i, then $\mathcal{B}$ responds with ζ_i.
      ii) Otherwise, $\mathcal{B}$ randomly chooses a string $\zeta_i \in \{0,1\}^n$ and inserts a new tuple (X_i, ζ_i) to the list. It responds to $\mathcal{A}$ with ζ_i.
   b) **RKGen Query.** $\mathcal{B}$ Chooses a randomly $t \in Z_q^*$ and let $k_1 = tk_2$, chooses $a, b \in Z_q^*$, let $(\frac{s+h_0+h_1}{s+h_0} = a, \frac{k_2}{s+h_0} = b)$, so $(rk_1, rk_2) = (\frac{s+h_0+h_1+k_1}{s+h_0}, \frac{k_2}{s+h_0}) = (a + tb, b)$[3]. $\mathcal{B}$ computes rk_3 as following.
$$s = x - h_0, \frac{s + h_0 + h_1}{s + h_0} = a, \frac{k_2}{s + h_0} = b,$$
$$rk_3 = \frac{t}{s + h_1 + h_0}Q_2 = td_B$$
   c) **Reencrypt Query.** The challenge $\mathcal{B}$ runs ReEnc$(rk_{A\to B}, C_A, B)$ and returns the results.
2) **Challenge.** Algorithm $\mathcal{A}$ outputs two messages (m_0, m_1) of equal length on which it wants to be challenged. C chooses a random string $R \in \{0,1\}^n$ and a random element $r \in Z_p^*$, and defines $C_{ch} = (U, V) = (rQ_1, R)$. $\mathcal{B}$ gives C_{ch} as the challenge to $\mathcal{A}$. Observe that the decryption of C_{ch} is
$$V \oplus H_2(e(U, d_A)) = R \oplus H_2(e(rQ_1, \frac{1}{x}Q_2))$$
3) **Phase 2.** $\mathcal{A}$ issues more queries like in Phase 1 except natural constraints and Algorithm $\mathcal{B}$ responds as before.
4) **Guess.** After algorithm $\mathcal{A}$ outputs its guess, $\mathcal{B}$ picks a random tuple(X_i, ζ_i) from H_2list. $\mathcal{B}$ first computes $T = X_i^{1/r}$, and then returns $(T/T_0)^{1/c_0^2}$. Note that $e(P_1, P_2)^{1/x} = (T/T_0)^{1/c_0^2}$ if $T = e(Q_1, Q_2)^{1/x}$. Let H be the event that

[3] s is the master − key

algorithm $\mathcal{A}$ issues a query for $H_2(e(rQ_1, \frac{1}{x}Q_2))$ at some point during the simulation above. Using the same methods in [3], we can prove the following two claims:

Claim 1: $Pr[H]$ in the simulation above is equal to $Pr[H]$ in the real attack.

Claim 2: In the real attack we have $Pr[H] \geq 2\epsilon(k)$. Following from the above two claims, we have that $\mathcal{B}$ produces the correct answer with probability at least $2\epsilon(k)/q_2$.

Thus we prove Lemma 3. ■

From the above three Lemma, we prove Theorem 1. ■

Theorem 5: Suppose q-BDHI assumption holds in $\mathbb{G}$, then our scheme is DGE-IBE-IND-ID-CCA2 secure for the proxy and delegator's colluding.

Proof: Same as the above theorem except in the simulation the role of A and B exchanged. ■

Theorem 6: Suppose the q-BDHI assumption holds, then our scheme is PKG-OW secure for the proxy, delegatee and delegator's colluding.

Proof: We just give the intuition for this theorem. The master-key is s, and delegator's private key is $\frac{1}{s+H_1(ID)}$, the delegatee's private key is $\frac{1}{s+H_1(ID')}$, the re-encryption key is $(\frac{s+H_1(ID')+k_1}{s+H_1(ID)} \mod p, \frac{k_2}{s+H_1(ID)} \mod p, \frac{k_1}{k_2(s+H_1(ID'))}P_2)$. Because the re-encryption key is uniformly distributed in Z_p^*, and the original SK IBE is secure, we can conclude that s can not be disclosed by the proxy, delegatee and delegator's colluding. ■

V. Issues about PKG's Workload in Our Proposed Schemes

One core idea in our proposed schemes is that, PKG itself generates every delegation key -the re-encryption key. This idea looks first contradict with our intuition about PKG(That is, what PKG can only do is generating IBE user's secret key) and increases PKG's workload. But we think our idea is reasonable.

From a theoretical point, the idea about PKG generating re-encryption key comes from Matsuo's M2 proxy re-encryption [14]. In their scheme, $rk_{\mathsf{ID}\to\mathsf{ID}'} = g^{u'\alpha}$ is generated by exponentiating delegatee's secret key $g^{u'}$ with $\mathsf{master}-\mathsf{key}$ α. Later in Inscrypt'08, Tang et al. proposed an inter-domain identity based proxy re-encryption [18]. In their scheme, generating the re-encryption key needs PKG. We quote it as follows:

> $\mathsf{Pextract}(id, id', sk_{id}(sk_{id'}, mk_1, mk_2))$: *This algorithm takes the delegator's identifier id, the delegatee's identifier id′, the delegator's private key* sk_{id}*, and possibly also* $\{sk_{id'}, mk_1, mk_2\}$ *as input and outputs the proxy key* $rk_{id\to id'}$ *to the proxy. This algorithm will be run by the delegator and possibly with other parties, such as the delegatee and KGCs.*

Furthermore, it seems difficult for constructing PRE in identity based setting which just needs the delegator and the delegatee to generate re-encryption key.

From a practical point, Involving PKG in generating re-encryption key can make PRE in identity based setting much efficient for the proxy, which is important for practical IBE systems. In GA07 scheme proxy's workload is heavy, while in our scheme, PKG's workload is more heavy. But we think that in practical IBE system, Re-encryption key generation operations are much more less than re-encryption operations. Although SXC08 scheme is efficient for the proxy, but the delegator and delegatee's workload is heavy. Furthermore, many practical IBE systems let their PKG be online 24/7/365, which make PKG generating re-encryption key is tolerable for these systems.

VI. Conclusions and Open Problems

In this paper, we construct PRE based on BB_2 IBE and PRE based on SK IBE. Although some excellent work [5], [6], [9], [13], [14], [16] has been done in PRE in identity based setting, there are still many open problems need to be solved such as: (1) More reasonable security models for IBPRE and. We note that our security model is stronger than security model in [14] for we considering colluding between proxy and delegator or delegatee. But we must point out that our security model just consider single-hop IBPRE, security models for multi-hop IBPRE maybe be different. (2) More stronger security results for our IBPRE scheme. We note most of our schemes can only achieve IND-Pr-ID-CPA secure, which is not enough for most applications. (3) More interesting applications for IBPRE. From a theoretical point, Obfuscating PRE is the only positive results for obfuscation of natural cryptographic tasks, maybe this primitive can find other applications in theoretical cryptography. From a practical point, PRE can have applications in e-mail forwarding, law enforcement, mobile equipment with limited computation ability, access control in secure distributed file storage. But IBPRE maybe have other interesting applications such as anonymous encryption, group encryption, one to many, many to one identity based broadcast encryption (Actually, Matsuo's M07B PRE is a many to one IBPRE).

Acknowledgement

The authors would like to thank Dr. Jian Weng, Dr. Jun Shao, Dr. Licheng Wang, Dr. Fagen Li, Dr. Qiang Tang for many helpful discussions and the anonymous referees for helpful comments.

References

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

[2] M. Blaze, G. Bleumer and M. Strauss. Divertible protocols and atomic proxy cryptography. In *EUROCRYPT 1998*, volume 1403 of *LNCS*, pages 127–144, 1998.

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

[4] 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.
[5] R. Canetti and S. Hohenberger. Chosen ciphertext secure proxy re-encryption. In *ACM CCS 2007*, pages 185–194, 2007.
[6] C. Chu and W. Tzeng. Identity-based proxy re-encryption without random oracles. In *ISC 2007*, volume 4779 of *LNCS*, pages 189–202, 2007.
[7] L. Chen and Z. Cheng. Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme. http://eprint.iacr.org/2005 /226.pdf, 2005.
[8] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *CRYPTO 1999*, volume 1666 of *LNCS*, pages 535–554, 1999.
[9] M. Green and G. Ateniese. Identity-based proxy re-encryption. In *ACNS 2007*, volume 4521 of *LNCS*, pages 288–306, 2007.
[10] C. Gentry. Practical Identity-Based Encryption without Random Oracles. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464, 2006. 1999.
[11] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker. A type-and-identity-based proxy re-encryption scheme and its application in healthcare. In *SDM 2008*, volume 5159 of LNCS, pages 185–198, 2008.
[12] J. Lai, W. Zhu, R. Deng, S. Liu and W. Kou New constructions for identity-based unidirectional proxy re-encryption. In *Journal of Computer Science and Technology*, no. 25(4), pages 793–806. 2010.
[13] B. Libert and D. Vergnaud. Unidirectional chosen ciphertext secure proxy re-encryption. In *PKC 2008*, volume 4939 of *LNCS*, pages 360–379, 2008.
[14] T. Matsuo. Proxy re-encryption systems for identity-based encryption. In *PAIRING 2007*, volume 4575 of *LNCS*, pages 247–267, 2007.
[15] Y. Ming, X. Shen, Y. Peng. Provably security identity-based sanitizable signature scheme without random oracles. In *Journal of Software*, 1890-1897 Volume 6, Number 10, 2011.
[16] L. Martin(editor). P1363.3(TM)/D1, Draft Standard for Identity-based Public Cryptography Using Pairings, May 2008.
[17] J. Shao, D. Xing and Z. Cao, Identity-Based Proxy Rencryption Schemes with Multiuse, Unidirection, and CCA Security. Cryptology ePrint Archive: http://eprint.iacr.org/2008/103.pdf,2008.
[18] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report2003/054. 2003.
[19] Q. Tang, P. Hartel and W Jonker. Inter-domain identity-based proxy re-encryption. In *INSCRYPT 2008*, volume 5487 of *LNCS*, pages 332–347, 2008.
[20] H. Wang, Z. Cao, L. Wang. Multi-use and unidirectional identity-based proxy re-encryption schemes. In *Information Science*, No 180, pages 4042-4059, 2010.
[21] X. A. Wang, X. Y. Yang. Proxy Re-encryption Scheme Based on SK Identity Based Encryption. The Fifith International Conference on Information Assurance and Security (IAS2009), IEEE CS, (Vol.2) 657-660, 2009.
[22] X. A. Wang and X. Yang On the insecurity of an identity based proxy re-encryption. In *Fundamental Informaticae*, no. 98(2-3), pages 277–281. 2010.
[23] X. Y. Yang, X. A. Wang. Proxy Re-encryption Scheme Based on BB2 Identity Based Encryption. The 2nd International Conference on Computer Science and Information Technology (ICCSIT2009), IEEE Press, (Vol.1) 134-138, 2009.
[24] Q. Wu, W. Wang. New identity-based broadcast encryption with constant ciphertexts in the standard model. In *Journal of Software*, 1929-1936 Volume 6, Number 10, 2011.

Jindan Zhang was born in April. 27th, 1983. She obtained her master degree from University of Shaanxi Science and Technology. Now she is a lecturer in Xianyang Vocational Technical College. Her main research interests includes cryptography, and information hiding.

Xu An Wang was born in Feb. 23th, 1981. He obtained his master degree from Engineering University of Chinese Armed Police Force. Now he is an associate professor in the same University. His main research interests include public key cryptography.

Xiaoyuan Yang was born in Nov. 12th, 1959. He obtained his master and bachelor degree from Xidian University. Now he is a professor in the Engineering University of Chinese Armed Police Force. His main research interests include cryptography and information hiding.