Identity Based Proxy Re-encryption From BB1 IBE

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 1998, Blaze, Bleumer, and Strauss proposed a kind of cryptographic primitive called proxy re-encryption. In proxy re-encryption, a proxy can transform a ciphertext computed under Alice's public key into one that can be opened under Bob's decryption key. In 2007, Matsuo proposed the concept of four types of proxy re-encryption schemes: CBE (Certificate Based Public Key Encryption) to IBE (Identity Based Encryption) (type 1), IBE to IBE (type 2), IBE to CBE (type 3), CBE to CBE (type 4). In this paper, we find that if we allow the PKG to use its master-key in the process of generating re-encryption key for proxy re-encryption in identity based setting, many open problems can be solved. We give the new security models for proxy re-encryption in identity based setting, especially considering PKG's involving in the re-encryption key generation process and PKG's master-key's security. We construct the new IND-ID-CPA and the first IND-ID-CCA2 secure proxy re-encryption schemes based on BB1 IBE. We also prove their security by introducing some new techniques which maybe have independent interest. At last, we compare our new schemes with existing ones, the results show that our scheme can achieve high security levels and are very efficient for re-encryption and, which are very important for practical applications.**

***Index Terms*— Cryptography, Identity based proxy re-encryption, PKG, BB1 IBE, Security proof.**

I. Introduction

The concept of proxy re-encryption(PRE) comes from the work of Blaze, Bleumer, and Strauss in 1998[2]. The goal of proxy re-encryption is to securely enable the re-encryption of ciphertexts from one key to another, without relying on trusted parties. In 2005, Ateniese et al proposed a few new PRE schemes and discussed its several potential applications such as e-mail forwarding, law enforcement, cryptographic operations on storage-limited devices, distributed secure file systems and out-sourced filtering of encrypted spam [1]. Since then, many excellent schemes have been proposed[10], [25], [20], [26], [15], [27], [11], [29]. In ACNS'07, Green et al. proposed the first identity based proxy re-encryption schemes(IDPRE) [15]. In ISC'07, Chu et al. proposed the first IND-ID-CCA2 IDPRE schemes in the standard model, they constructed their scheme 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 [29]. In Pairing'07, Matsuo proposed another few more PRE schemes in identity based setting [27]. Interestingly, they proposed the concept of four types of PRE: CBE(Certificate Based Public Key Encryption) to IBE(Identity Based Encryption)(type 1), IBE to IBE(type 2), IBE to CBE (type 3), CBE to CBE (type 4)[27], which can help the ciphertext [33], [24] circulate smoothly in the network. They constructed two PRE schemes: one is the hybrid PRE from CBE to IBE, the other is the PRE from IBE to IBE. Both of the schemes are now being standardized by P1363.3 workgroup [28]. Recently, Tang et al. extended the concept of identity based proxy re-encryption, they proposed a concept of inter-domain identity based proxy re-encryption which aimed to constructing proxy re-encryption scheme between different domains in identity based setting [31].

The second author is the corresponding author. This paper is an extended work of [34], [35] 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.

A. Main Idea and Contribution

Our contributions are mainly as following: If we follow the principal that all the work PKG can do is just generating private keys for IBE users, it is indeed difficult for constructing PRE based on BB_1 IBE. But if we allow PKG generating re-encryption keys for PRE by using its $\mathsf{master-key}$, we can easily construct PRE based on a variant of BB_1 IBE.

On the Role of PKG *in* IBPRE *and Related Primitives*. We challenge the traditional idea of PKG is only responsible to generate private keys. Traditionally when cryptographers design IBE and other related schemes, they assume the PKG can only generate the private keys to the users. The idea situation is that after PKG generating private keys for the whole users, the PKG is shut up to avoid "single-point failure" problem. But we remark that this idea situation can not work in the practical application, we can not predicate all the future users of the system when it was set up. Furthermore, in the IBE systems, there are also requirements of revocation of the identity, which will necessary involved the PKG. Thus many usable IBE systems let their PKG be online

doi:10.4304/jcp.8.6.1618-1626

24/7/365. From a practical point, for PRE in the identity based setting, involving PKG in generating re-encryption key can generically help the proxy improve its efficiency, which is very important for practical IBPRE systems, after all, re-encryption is the main operation in the PRE systems. More importantly, involving PKG in generating some "valued ephemeral" maybe bring unexpected benefits to existing identity based primitives. For example, in identity based broadcast encryption, some "valued ephemeral" given by the PKG maybe be very useful for the receivers for decryption, Note the length of this "valued ephemeral" is just constant, instead of linear with the receivers, thus improve the efficiency greatly. Also note this feature can not be shared with the normal public key broadcast encryption schemes.

B. Organization

We organize our paper as following. In Section II, we give some preliminaries which are necessary to understand our paper. We propose our new proxy re-encryption scheme based on a variant of BB_1 IBE and prove its security in SectionIII. In Section IV, we give the comparison results with previous IBPRE schemes. We give our conclusions in the last Section V.

II. Preliminaries

In the following, we sometimes use notations described in this section without notice. We denote the concatenation of a and b by $a||b$, denote random choice from a set S by $\stackrel{R}{\leftarrow} S$.

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, $c \stackrel{R}{\leftarrow} Z_p^*$, a random generator $g \stackrel{R}{\leftarrow} G$, and an element $R \stackrel{R}{\leftarrow} G$, we define the advantage of an algorithm $\mathcal{A}$ in solving the Decision Bilinear Diffie-Hellman(DBDH) problem as follows:

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

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)-DBDH assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the DBDH problem in G under a security parameter k.

C. Identity Based Encryption

An Identity Based Encryption(IBE) system consists of the following algorithms.

1) **SetUp**$_{\mathsf{IBE}}$(k). Given a security parameter k, PKG generate a pair (parms, mk), where parms denotes the public parameters and mk is the master − key.
2) **KeyGen**$_{\mathsf{IBE}}$(mk, parms, **ID**). Given the master − key mk and an identity ID with parms, generate a secret key sk_{ID} for ID.
3) **Enc**$_{\mathsf{IBE}}$(**ID**, parms, M). Given a message M and the identity ID with parms, compute the encryption of M, C_{ID} for ID.
4) **Dec**$_{\mathsf{IBE}}$(sk, parms, C_{ID}). Given the secret key sk, decrypt the ciphertext C_{ID}.

III. IBPRE Based on a Variant of BB_1 IBE

A. Our Definition for IBPRE

In this section, we give our definition and security model for identity based PRE scheme, which is based on [15], [31].

Definition 2: 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 $\perp$.

Remark 1: This definition is different from the Definition of IBPRE in the work of [27]. We insist this is a more natural and general Definition for PRE from IBE to IBE. This definition is consistent with the work of [15], [31].

B. Our Security Models for IBPRE

In PRE from IBE to IBE, there is no necessary to consider the malicious PKG attack, so we omit PKG in our security model when considering delegator security and delegatee security.

Delegator Security.

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

Definition 3: **(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 $\mathsf{Keygen}_{\mathsf{CBE}}$, ID_j were produced by $\mathsf{Keygen}_{\mathsf{IBE}}$, 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 4: **(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 3.

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 5: **(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 3.

C. Our Proposed IND-Pr-sID-CPA Secure IBPRE Scheme Based on a Variant of BB_1 IBE

- The underlying IBE scheme: We give a variant of BB_1-IBE scheme as follows:
  Let G be a bilinear group of prime order p (the security parameter determines the size of G). Let $e : G \times G \rightarrow G_1$ be the bilinear map. For now, we assume public keys (ID) is element in Z_p^*. We later extend the construction to public keys over $\{0,1\}^*$ by first hashing ID using a collision resistant hash $H : \{0,1\}^* \rightarrow Z_p$. We also assume messages to be encrypted are elements in G. The IBE system works as follows:
  1) $\mathbf{SetUp_{IBE}(k)}$. Given a security parameter k, select a random generator $g \in G$ and random elements $g_2 = g^{t_1}, h = g^{t_2} \in G$. Pick a random $\alpha \in Z_p^*$. Set $g_1 = g^\alpha$,$mk = g_2^\alpha$, and $params =$

[1]DGA means Delegator
[2]DGE means Delegatee.

(g, g_1, g_2, h). Let mk be the master-secret key and let $params$ be the public parameters.

2) $\mathbf{KeyGen_{IBE}(mk, params, ID)}$. Given $mk = g_2^{\alpha}$ and ID with $params$, the PKG picks random $s_0, s_1 \in Z_p^*$, choose a hash function $\widetilde{H} : \mathcal{Z}_p^* \times \{0,1\}^* \rightarrow \mathcal{Z}_p^*$ and computes $u_0 = \widetilde{H}(s_0, ID)$, $u_1 = \widetilde{H}(s_1, ID)$. Set $sk_{ID} = (d_0, d_1, d_0') = (g_2^{\alpha}(g_1^{ID}h)^{u_0}, g^{u_0}, (g_2^{\alpha}(g_1^{ID}h)^{u_1}))$. The PKG preserves (s_0, s_1).

3) $\mathbf{Enc_{IBE}(ID, params, M)}$. To encrypt a message $M \in G_1$ under the public key $ID \in Z_p^*$, pick a random $r \in Z_p^*$ and compute $C_{ID} = (g^r, (g_1^{ID}h)^r, Me(g_1, g_2)^r)$.

4) $\mathbf{Dec_{IBE}(sk_{ID}, params, C_{ID})}$. Given ciphertext $C_{ID} = (C_1, C_2, C_3)$ and the secret key $sk_{ID} = (d_0, d_1)$ with $prams$, compute $M = \frac{C_3 e(d_1, C_2)}{e(d_0, C_1)}$.

- The delegation scheme:

1) $\mathbf{KeyGen_{PRO}(sk_R, params, ID, ID')}$. The PKG computes $u_1' = \widetilde{H}(s_1, ID')$ and randomly selects $k_1, k_2, k_3 \in Z_p^*$ and sets $rk_{ID \rightarrow ID'} = (rk_1, rk_2, rk_3, rk_4) = (\frac{\alpha ID' + t_2 + k_1}{k_3(\alpha ID + t_2)} + k_2, g^{u_1' k_3}, g^{u_1' k_2 k_3}, g^{u_1' k_1})$ and sends them to the proxy via secure channel. We must note that the PKG computes a different (k_1, k_2, k_3) for every different user pair (ID, ID').

2) $\mathbf{Check(params, C_{ID}, ID)}$. Given the delegator's identity ID and $C_{ID} = (C_1, C_2, C_3)$ with $params$, compute $v_0 = e(C_1, g_1^{ID}h)$ and $v_1 = e(C_2, g)$. If $v_0 = v_1$ then output 1. Otherwise output 0.

3) $\mathbf{ReEnc(rk_{ID \rightarrow ID'}, params, C_{ID}, ID')}$. Given the identities ID, ID', $rk_{ID \rightarrow ID'} = (rk_1, rk_2, rk_3, rk_4) = (\frac{\alpha ID' + t_2 + k_1}{k_3(\alpha ID + t_2)} + k_2, g^{u_1' k_3}, g^{u_1' k_2 k_3}, g^{u_1' k_1})$ with $params$, the proxy re-encrypt the ciphertext C_{ID} into $C_{ID'}$ as follows. First it runs "Check", if output 0, then return "Reject". Else computes $C_{2ID'} = (C_1', C_2', C_3', C_4', C_5', C_6', C_7') = (C_1, C_2, C_3, C_2^{\frac{\alpha ID' + t_2 + k_1}{k'(\alpha ID + t_2)} + k_2}, rk_2, rk_3, rk_4)$.

4) $\mathbf{Dec1_{IBE}(sk_{ID'}, params, C_{2ID'})}$. Given a re-encrypted ciphertext $C_{2ID'} = (C_1', C_2', C_3', C_4', C_5', C_6', C_7')$ and the secret key $sk_{ID} = (d_0, d_1, d_0')$ with $params$, computes

$$M = \frac{C_3' e(C_5', C_4')}{e(C_2', C_6') e(C_1', C_7') e(d_0', C_1')}$$

$$= \frac{C_3' e(rk_2, C_4')}{e(C_2', rk_3) e(C_1', rk_4) e(d_0', C_1')}$$

5) $\mathbf{Dec2_{IBE}(sk_{ID'}, params, C_{1ID'})}$. Given a normal ciphertext $C_{ID'} = (C_1, C_2, C_3)$ and the secret key $sk_{ID'} = (d_0, d_1, d_0')$ with $prams$, compute $M = \frac{C_3 e(d_1, C_2)}{e(d_0, C_1)}$.

We can verify its correctness as following

$$\frac{C_3' e(rk_2, C_4')}{e(C_2', rk_3) e(C_1', rk_4) e(d_0', C_1')}$$
$$= \frac{Me(g_1, g_2)^r e(g^{k_3 u_1'}, (g_1^{ID}h)^{r(\frac{\alpha ID' + t_2 + k_1}{k_3(\alpha ID + t_2)} + k_2)})}{e((g_1^{ID}h)^r, g^{u_1' k_2 k_3}) e(g^r, g^{k_1 u_1'}) e(g_2^{\alpha}(g_1^{ID'}h)^{u_1'}, g^r)}$$
$$= \frac{Me(g_1, g_2)^r e(g^{k_3 u_1'}, (g_1^{ID}h)^{k_2 r}) e(g^{k_3 u_1'}, (g_1^{ID'}h)^{\frac{r}{k_3}}) e(g^{k_3 u_1'}, g^{\frac{k_1 r}{k_3}})}{e((g_1^{ID}h)^r, g^{u_1' k_2 k_3}) e(g^r, g^{k_1 u_1'}) e(g_2^{\alpha}(g_1^{ID'}h)^{u_1'}, g^r)}$$
$$= \frac{Me(g_1, g_2)^r}{e(g_2^{\alpha}, g^r)} = M$$

Remark 2: In our scheme, we must note that the PKG computes a different (k_1, k_2, k_3) for every different pair (ID, ID'). Otherwise, if the adversary knows $\frac{\alpha ID' + t_2 + k_1}{k_3(\alpha ID + t_2)} + k_2$ for five different pairs (ID, ID') but the same $k_1, k_2, k_3, \alpha, t_2$, he can compute (α, t_2), which is not secure at all.

D. Security Analysis

Theorem 1: Suppose the DBDH assumption holds, then our scheme proposed in Section III-C is DGA-IBE-IND-sID-CPA secure for the proxy and the delegatee's colluding.

Proof: Suppose $\mathcal{A}$ can attack our scheme, we construct an algorithm $\mathcal{B}$ solves the DBDH problem in G. On input $(g, g^a, g^{a^2}, g^b, g^c, T)$, algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g, g)^{abc}$ and 0 otherwise. Let $g_1 = g^a, g_2 = g^b, g_3 = g^c$. Algorithm $\mathcal{B}$ works by interacting with $\mathcal{A}$ in a selective identity game as follows:

1) **Initialization**. The selective identity game begins with $\mathcal{A}$ first outputting an identity ID^* that it intends to attack.

2) **Setup**.To generate the system's parameters, algorithm $\mathcal{B}$ picks $\alpha' \in Z_p$ at random and defines $h = g_1^{-ID^*} g^{\alpha'} \in G$. It gives $\mathcal{A}$ the parameters $params = (g, g_1, g_2, h)$. Note that the corresponding $master - key$, which is unknown to $\mathcal{B}$, is $g_2^a = g^{ab} \in G^*$.

3) **Phase 1**

- *"$\mathcal{A}$ issues up to private key queries on ID_i".* $\mathcal{B}$ selects randomly $r_i, r_i' \in {Z_p}^*$ and $k' \in Z_p$, sets $sk_{ID_i} = (d_0, d_1, d_0') = (g_2^{\frac{-\alpha'}{ID_i - ID^*}} (g_1^{(ID_i - ID^*)} g^a)^{r_i}, g_2^{\frac{-1}{ID_i - ID^*}} g^{r_i}, g_2^{\frac{-\alpha'}{ID_i - ID^*}} (g_1^{(ID_i - ID^*)} g^a)^{r_i'})$. We claim sk_{ID_i} is a valid random private key for ID_i. To see this, let $\widetilde{r_i} = r_i - \frac{b}{ID - ID^*}$ and $\widetilde{r_i'} = r_i' - \frac{b}{ID - ID^*}$. Then we have that
$d_0 = g_2^{\frac{-\alpha'}{ID_i - ID^*}} (g_1^{(ID_i - ID^*)} g^{\alpha'})^{r_i} = g_2^a (g_1^{(ID_i - ID^*)} g^{\alpha'})^{r_i - \frac{b}{ID - ID*}} = g_2^a (g_1^{ID_i} h)^{\widetilde{r_i}}$.
$d_1 = g_2^{\frac{-1}{ID_i - ID^*}} g^{r_i} = g^{\widetilde{r_i}}$.
$d_0' = g_2^{\frac{-\alpha'}{ID_i - ID^*}} (g_1^{(ID_i - ID^*)} g^{\alpha'})^{r_i'} = g_2^a (g_1^{(ID_i - ID^*)} g^{\alpha'})^{r_i' - \frac{b}{ID - ID*}} = g_2^a (g_1^{ID_i} h)^{\widetilde{r_i'}}$.

- *"$\mathcal{A}$ issues up to rekey generation queries on (ID, ID')".*
The challenge $\mathcal{B}$ chooses a randomly $x \in Z_p^*$,

sets $rk_{ID\to ID'} = x$ and returns it to $\mathcal{A}$. He computes $w = \frac{(g^{H_1(ID)}h)^x}{(g^{H_1(ID)}h)}$ and sends it to the proxy. We observe that

$$rk_1 = \frac{\alpha ID' + t_2 + k_1}{k_3(\alpha ID + t_2)} + k_2$$

but from the simulation, $\alpha = a$ and $t_2 = \alpha' - aID^*$, so we can get

$$rk_1 = \frac{aID' + \alpha' - aID^* + k_1}{k_3(aID + \alpha' - aID^*)} + k_2$$

Let $rk_1 = x$, we can get

$$\begin{aligned} k_1 &= k_3(aID + \alpha' - aID^*)(x - k_2) \\ &\quad -(aID' + \alpha' - aID^*) \\ &= [k_3(x - k_2)a(ID - ID^*) \\ &\quad -a(ID' - ID^*)] + k_3\alpha'(x - k_2) - \alpha' \end{aligned}$$

So the challenge $\mathcal{B}$ simulates as follows. He chooses a randomly $k_2, k_3 \in Z_p^*$, sets

$$x = \frac{ID' - ID^*}{k_3(ID - ID^*)} + k_2,$$
$$k_1 = \alpha'(\frac{ID' - ID^*}{ID - ID^*}) - \alpha'$$

searches in `User-key-list` for item (ID', α', r, r')(we assume $sk_{ID'} = (d_0, d_1, d'_0) = (g_2^{\frac{-\alpha'}{ID'-ID^*}}(g_1^{(ID'-ID^*)}g^a)^r, g_2^{\frac{-1}{ID'-ID^*}}g^r, g_2^{\frac{-\alpha'}{ID'-ID^*}}(g_1^{(ID'-ID^*)}g^a)^{r'})$ and computes

$$\begin{aligned} rk_1 &= \frac{ID' - ID^*}{k_3(ID - ID^*)} + k_2, \\ rk_2 &= g_2^{\frac{-k_3}{ID'-ID^*}} g^{k_3 r'} \\ rk_3 &= g_2^{\frac{-k_2 k_3}{ID'-ID^*}} g^{k_2 k_3 r'}, \\ rk_4 &= g_2^{\frac{\alpha'(\frac{ID'-ID^*}{ID-ID^*})-\alpha'}{ID'-ID^*}} g^{(\alpha'(\frac{ID'-ID^*}{ID-ID^*})-\alpha')r'} \end{aligned}$$

returns them to $\mathcal{A}$. We can see

$$\frac{C'_3 e(rk_2, C'_4)}{e(C'_2, rk_3)e(C'_1, rk_4)e(d'_0, C'_1)}$$

can be reduced to

$$\frac{Me(g_1, g_2)^r}{e(g_2^\alpha, g^r)} = M$$

Thus our simulation is indistinguishable from the real algorithm running. Thus our simulation is indistinguishable from the real algorithm running.

- *"$\mathcal{A}$ issues up to re-encryption queries on (C_{ID}, ID, ID')"*. The challenge $\mathcal{B}$ runs $ReEnc(rk_{ID\to ID'}, C_{ID}, ID, ID')$ and returns the results.

4) **Challenge** When $\mathcal{A}$ decides that Phase1 is over, it outputs two messages $M_0, M_1 \in G$. Algorithm $\mathcal{B}$ picks a random bit b and responds with the ciphertext $C = (g^c, (g^{\alpha'})^c, M_b \cdot T)$. Hence if $T = e(g,g)^{abc} = e(g_1, g_2)^c$, then C is a valid encryption of M_b under ID^*. Otherwise, C is independent of b in the adversary's view.
5) **Phase2** $\mathcal{A}$ issues queries as he does in Phase 1 except natural constraints.
6) **Guess** Finally, $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$. 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 advantage for breaking the scheme is same as $\mathcal{B}$'s advantage for solving DBDH problem. ■

Theorem 2: Suppose the DBDH assumption holds, then our scheme proposed in Section III-C is DGE-IBE-IND-sID-CPA secure for the delegator and proxy'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^*)"*, for $\mathcal{B}$ does not know the private key corresponding to ID^*. ■

Theorem 3: Suppose the DBDH assumption holds, then our scheme proposed in Section III-C is PKG-OW secure for the delegator, delegatee and proxy's colluding.

Proof: We just give the intuition for this theorem. The master-key is g_2^α, and delegator's private key is $sk_{ID} = (g_2^\alpha(g_1^{ID}h)^{u_0}, g^{u_0}, (g_2^\alpha(g_1^{ID}h)^{u_1}))$, the delegatee's private key is $sk_{ID'} = (g_2^\alpha(g_1^{ID'}h)^{u_0}, g^{u_0}, (g_2^\alpha(g_1^{ID'}h)^{u_1}))$, the proxy re-encryption key is $rk_{ID\to ID'} = (\frac{\alpha ID'+t_2+k_1}{k_3(\alpha ID+t_2)} + k_2, g^{u'_1 k_3}, g^{u'_1 k_2 k_3}, g^{u'_1 k_1})$. Because the re-encryption key $rk_{ID\to ID'}$ is uniformly distributed in $(Z_p^*, \mathbb{G}, \mathbb{G}, \mathbb{G})$, and the original BB_1 IBE is secure, we can conclude that g_2^α can not be disclosed by the proxy, delegatee and delegator's colluding. ■

E. Toward Chosen Ciphertext Security

As we all know, just considering IND-sID-CPA security is not enough for many applications. We consider construct IND-Pr-ID-CCA secure IBPRE based on a variant of BB_1 IBE. There are two ways to construct IND-Pr-ID-CCA secure IBPRE. One way is considering CHK transformation to hierarchal variant of BB_1 IBE to get IND-Pr-sID-CCA secure IBPRE or get IND-Pr-IDKEM-CCA secure IBPRE. The other way is considering variant of BB_1 IBE in the random oracle model. From a practical viewpoint, we construct an IND-Pr-ID-CCA secure IBPRE based on a variant of BB_1 IBE in the random oracle model.

F. Our Proposed IND-Pr-ID-CCA Secure IBPRE Scheme Based on a Variant of BB_1 IBE

Let G be a bilinear group of prime order p(the security parameter determines the size of G). Let $e : G \times G \to G_1$ be the bilinear map. Identities are represented using distinct arbitrary bit strings in $\{0, 1\}^l$. The messages (or session keys) are bit strings in $\{0,1\}^l$ of some fixed length l. We require the availability of five hash functions viewed as random oracles:

- A hash function $H_1 : \{0,1\}^* \to Z_q^*$;
- A hash function $H_2 : G_1 \times \{0,1\}^l \to G$;
- A hash function $H_3 : G_1 \to \{0,1\}^l$;
- A hash function $H_4 : \{0,1\}^* \times G \times G \times G \times \{0,1\}^l \to G$;

1) **SetUp.** To generate IBE system parameters, first select three integers $\alpha, \beta, \gamma \in Z_p$ at random. Set $g_1 = g^{\alpha}$, $g_2 = g^{t_1}$ and $h = g^{t_2}$ in G, and compute $v_0 = e(g,g)^{\alpha\beta}$. The public system parameters $params$ and the $masterkey$ are given by: $params = (g, g_1, g_3, v_0)$, $masterkey = (\alpha, \beta, \gamma)$. Strictly speaking, the generator need not be kept secret, but since it will be used exclusively by the authority, it can be retained in $masterkey$ rather than published in $params$.
2) **Extract.** To generate a private key d_{ID} for an identity $ID \in \{0,1\}^*$, using the $masterkey$, the PKG picks random $s_0, s_1 \in Z_p^*$, choose a hash function $\widetilde{H} : \mathcal{Z}_p^* \times \{0,1\}^* \to \mathcal{Z}_p^*$ and computes $u_0 = \widetilde{H}(s_0, ID)$, $u_1 = \widetilde{H}(s_1, ID)$. It outputs: $d_{ID} = (d_0, d_1) = (g_2^{\alpha}(g_1^{H_2(ID)}h)^{u_0}, g^{u_0}, g_2^{\alpha}(g_1^{H_2(ID)}h)^{u_1})$. The PKG preserves (s_0, s_1).
3) **Encrypt.** To encrypt a message $M \in \{0,1\}^l$ for a recipient $\{0,1\}^*$, the sender chooses a randomly $\delta \in G$ and computes $s = H_2(\delta, M)$, $k = v_0^s$, $C_1 = g^s$, $C_2 = h^s g_1^{H_1(ID)s}$, $C_3 = \delta \cdot k$, $C_4 = M \oplus H_3(\delta)$, $C_5 = H_4(ID \parallel C_1 \parallel C_2 \parallel C_3 \parallel C_4)^s$, and then outputs $C = (C_1, C_2, C_3, C_4, C_5)$.
4) **ReKeyGen.** The PKG computes $u_1' = \widetilde{H}(s_1, ID')$ and randomly selects $k_1, k_2, k_3 \in Z_p^*$, sets $rk_{ID \to ID'} = (\frac{\alpha H_1(ID') + t_2 + k_1}{k_3(\alpha H_1(ID) + t_2)} + k_2, g^{u_1' k_3}, g^{u_1' k_2 k_3}, g^{u_1' k_1})$ and sends it to the proxy via secure channel. We must note that the PKG computes a different (k_1, k_2, k_3) for every different user pair (ID, ID').
5) **ReEnc.** Given the identities (ID, ID'), $rk_{ID \to ID'} = (rk_1, rk_2, rk_3, rk_4) = (\frac{\alpha H_1(ID') + t_2 + k_1}{k_3(\alpha H_1(ID) + t_2)} + k_2, g^{u_1' k_3}, g^{u_1' k_2 k_3}, g^{u_1' k_1})$, $C_{ID} = (C_1, C_2, C_3, C_4, C_5)$ with $params$, the proxy re-encrypts the ciphertext C_{ID} into $C_{ID'}$ as follows.
   a) First it computes $v_0 = e(C_5, g)$ and $v_1 = e(H_4(ID \parallel C_1 \parallel C_2 \parallel C_3 \parallel C_4), C_1)$. If $v_0 \neq v_1$, the ciphertext is rejected.
   b) Else computes $C_{ID'} = (C_1', C_2', C_3', C_4', C_5', C_6', C_7', C_8') = (C_1, C_2, C_3, C_2^{rk_1}, rk_2, rk_3, rk_4, C_4)$.
6) **Decrypt.**
   a) To decrypt a normal ciphertext $C = (C_1, C_2, C_3, C_4, C_5)$ using the private key $d_{ID} = (d_0, d_1, d_0')$, it computes $v_0 = e(C_5, g)$ and $v_1 = e(H_4(ID \parallel C_1 \parallel C_2 \parallel C_3 \parallel C_4), C_1)$. If $v_0 \neq v_1$, the ciphertext is rejected. The recipient computes $k = \frac{e(C_1, d_0)}{e(C_2, d_1)}$. It then computes $\delta = \frac{C_3}{k}$, $M = H_4(\delta) \oplus C_4$. It computes $s' = H_2(\delta, M)$ and verifies that $C_1 = g^{s'}$, $C_2 = h^{s'} g_1^{H_1(ID)s'}$, if either checks fails, returns $\perp$, otherwise returns M.
   b) To decrypt a re-encrypted ciphertext $C_{ID'} = (C_1', C_2', C_3', C_4', C_5', C_6', C_7', C_8')$ using the private key $d_{ID} = (d_0, d_1, d_0')$, the recipient computes $k = \frac{C_3' e(C_5', C_4')}{e(C_2', C_6') e(C_1', C_7') e(d_0', C_1')} = \frac{C_3' e(rk_2, C_4')}{e(C_2', rk_3) e(C_1', rk_4) e(d_0', C_1')}$. It then computes $\delta = \frac{C_3}{k}$, $M = H_3(\delta) \oplus C_8'$. It computes $s' = H(\delta, M)$ and verifies that $C_1 = g^{s'}$, $C_2 = h^{s'} g_1^{H_1(ID)s'}$, if either check fails, returns $\perp$, otherwise returns M.

G. Security Analysis

Theorem 4: Suppose the DBDH assumption holds, then our scheme proposed in Section III-F is DGA-IBE-IND-ID-CCA secure for the proxy and delegatee's colluding.

Proof: Let $\mathcal{A}$ be a p.p.t. algorithm that has non-negligible advantage in attacking the scheme proposed in Section III-F. We use $\mathcal{A}$ in order to construct a second algorithm $\mathcal{B}$ which has non-negligible advantage at solving the DBDH problem in G. Algorithm $\mathcal{B}$ accepts as input a properly-distributed tuple (g, g^a, g^b, g^c, R) and outputs 1 if $R = e(g,g)^{abc}$. We now describe the algorithm $\mathcal{B}$, which interacts with algorithm $\mathcal{A}$ as following.

$\mathcal{B}$ simulates the random oracles H_1, H_2, H_3, H_4 as follows.

1) $H_1 : \{0,1\}^* \to Z_q^*$. On receipt of a new query for $ID \neq ID^*$, return $t \leftarrow_R Z_q^*$ and record (ID, t); On receipt of a new query for ID^*, select randomly $T \in Z_q^*$, return T and record (ID^*, T).
2) $H_2 : G_1 \times \{0,1\}^l :\to Z_q^*$. On a new query (δ, M), returns $s \leftarrow_R G$ and record (δ, M, s).
3) $H_3 : G_1 :\to \{0,1\}^l$. On receipt of a new query δ, select $p \leftarrow \{0,1\}^l$ and return p. Record the tuple (δ, p).
4) $H_4 : \{0,1\}^* \times G \times G \times G \times \{0,1\}^l :\to G$. On receipt of a new query $(ID \parallel C_1 \parallel C_2 \parallel C_3 \parallel C_4)$, select $z \in Z_q^*$ and return $g^z \in G$, record $(ID \parallel C_1 \parallel C_2 \parallel C_3 \parallel C_4, z, g^z)$.

Our simulation proceeds as follows:

1) **Setup.** $\mathcal{B}$ generates the scheme's master parameter as following. First it lets $g_1 = g^a$, $g_2 = g^b$, $g_3 = g^c$, algorithm $\mathcal{B}$ picks $\alpha \in Z_p$ at random and defines $h = g_1^{-T} g^{\alpha'} \in G$ $\mathcal{B}$ lets $params = (G_1, H_1, H_2, H_3, H_4, g, g_1, g_2, g_3, h)$ and gives $params$ to $\mathcal{A}$.
2) **Find/Guess.** During the Find stage, there are no restrictions on which queries $\mathcal{A}$ may issue. The scheme permits only a single consecutive re-encryption, therefore, during the GUESS stage, $\mathcal{A}$ is restricted from issuing the following queries:
   a) $(extract, ID^*)$ where ID^* is the challenge identity.

b) $(decrypt, ID^*, c^*)$ where c^* is the challenge ciphertext.
c) Any pair of queries $(rkextract, ID^*, ID_i)$, $(decrypt, ID_i, c_i)$ where c_i=Reencrypt$(rk_{ID^* \to ID_i}, c^*)$.

In the Guess stage, let ID^* be the target identity, and parse the challenge ciphertext c^* as $(C_1^*, C_2^*, C_3^*, C_4^*, C_5^*)$. In both phases, $\mathcal{B}$ responds to $\mathcal{A}$'s queries as follows.

- On $(extract, ID)$, where(in the Guess)stage $ID \neq ID^*$, $\mathcal{B}$ selects randomly $r_i \in Z_p^*$, sets $sk_{ID_i} = (d_0, d_1) = (g_2^{\frac{-\alpha'}{H_1(ID_i)-T}} (g_1^{(H_1(ID_i)-T)} g^{\alpha'})^{r_i}, g_2^{\frac{-1}{H_1(ID_i)-T}} g^{r_i})$. We claim sk_{ID_i} is a valid random private key for ID_i. To see this, let $\widetilde{r_i} = r_i - \frac{b}{H_1(ID_i)-T}$. Then we have that
$d_0 = g_2^{\frac{-\alpha'}{H_1(ID_i)-T}} (g_1^{(H_1(ID_i)-T)} g^{\alpha'})^{r_i} = g_2^a (g_1^{(H_1(ID_i)-T)} g^{\alpha'})^{r_i - \frac{b}{H_1(ID_i)-T}} = g_2^a (g_1^{H_1(ID_i)} h)^{\widetilde{r_i}}$.
$d_1 = g_2^{\frac{-1}{H(ID_i)-T}} g^{r_i} = g^{\widetilde{r_i}}$.
$d_0' = g_2^{\frac{-1}{H(ID_i)-T}} g^{r_i} = g^{\widetilde{r_i}}$.
- On $(rkextract, ID, ID')$, do the same as $\mathcal{A}$ handling re-encryption key query in Phase 13 in the above theorem.
- On $(decrypt, ID, c)$ where (in the Guess stage) $(ID, c) \neq (ID^*, c^*)$, check whether c is a level-1 (non re-encrypted) or level-2 (re-encrypted) ciphertext. In the Guess stage, parse c^* as $(C_1^*, C_2^*, C_3^*, C_4^*, C_5^*)$.
For a level-1 ciphertext, $\mathcal{B}$ parses c as $(C_1, C_2, C_3, C_4, C_5)$ and:
  a) Looks up the value $(ID \parallel C_1 \parallel C_2 \parallel C_3 \parallel C_4)$ in the H_4 table, to obtain the tuple $(ID \parallel C_1 \parallel C_2 \parallel C_3 \parallel C_4, z, g^z)$. If $(ID \parallel C_1 \parallel C_2 \parallel C_3 \parallel C_4)$ is not in the table, or if (in the Guess stage) $C_5 = C_5^*$, then $\mathcal{B}$ returns $\perp$ to $\mathcal{A}$.
  b) Looks up the value (δ, M, s) in the H_2 table. Checks whether there exist an item of (δ, M, s) such that $S = g^{zs}$. If not, $\mathcal{B}$ returns $\perp$ to $\mathcal{A}$.
  c) Computes $k = \frac{e(C_1, d_0)}{e(C_2, d_1)}$, checks that $\delta = \frac{C}{k}$. If not, $\mathcal{B}$ returns $\perp$ to $\mathcal{A}$.
  d) Checks that $C_4 = H_3(\delta) \oplus M$. If not, $\mathcal{B}$ returns $\perp$ to $\mathcal{A}$.
  e) Otherwise, $\mathcal{B}$ returns M to $\mathcal{A}$.

  For a level-2 ciphertext, $\mathcal{B}$ parses c as $(C_1', C_2', C_3', C_4', C_5', C_6', C_7', C_8')$ and:
  a) Computes
$$k = \frac{C_3' e(C_5', C_4')}{e(C_2', C_6') e(C_1', C_7') e(d_0', C_1')} = \frac{C_3' e(rk_2, C_4')}{e(C_2', rk_3) e(C_1', rk_4) e(d_0', C_1')}$$
  b) Checks that $\delta = \frac{C}{k}$. If not, $\mathcal{B}$ returns $\perp$ to $\mathcal{A}$.
  c) Checks that $C_2 = h^s g_1^{H_1(ID)s}$. If so, return M. Otherwise, return $\perp$.
- On $(reencrypt, C_{ID}, ID, ID')$. $\mathcal{B}$ runs $ReEnc(rk_{ID \to ID'}, C_{ID}, ID, ID')$ and returns the results.

At the end of the Find phase, $\mathcal{A}$ outputs (ID^*, M_0, M_1), with the condition that $\mathcal{A}$ has not previously issued $(extract, ID^*)$. At the end of the Guess stage, $\mathcal{A}$ outputs its guess bit i'.

3) **Choice and Challenge.** At the end of the Find phase, $\mathcal{A}$ outputs (ID^*, M_0, M_1). $\mathcal{B}$ forms the challenge ciphertext as follows:
  a) Choose $\delta \in G_1$ and $p \in \{0,1\}^n$ randomly, and insert (δ, p) in H_3 table.
  b) Insert $(\delta, M_b, ?, g_3, \delta \cdot R, M_b \oplus p)$ to H_2 table.
  c) Choose $z \in Z_p$ randomly, and insert $((g_3, g_3^{\alpha'}, \delta \cdot R, M_b \oplus p), z, g^z)$ in the H_4 table.

  $\mathcal{B}$ outputs the challenge ciphertext $(C_1^*, C_2^*, C_3^*, C_4^*, C_5^*) = (g_3, g_3^{\alpha'}, \delta \cdot R, M_b \oplus p, g_3^z)$ to $\mathcal{A}$ and begins the GUESS stage.
4) **Forgeries and Abort conditions** The adversary may forge C_5 on (C_1, C_2, C_3, C_4), but from the security of BLS short signature [7], this probability is negligible.

■

Theorem 5: Suppose the DBDH assumption holds, then our scheme proposed in Section III-F is DGE-IBE-IND-ID-CCA secure for the delegator and proxy'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^*)"*, for $\mathcal{B}$ does not know the private key corresponding to ID^*. ■

Theorem 6: Suppose the DBDH assumption holds, then our scheme proposed in Section III-F is PKG-OW secure for the delegator, proxy and delegatee's colluding.

Proof: The security proof is same as the proof for Theorem 3. ■

IV. Comparison

In this section, we give our comparison results with other identity based proxy re-encryption schemes[15], [11], [27], [29]. We compare our schemes with other schemes from two ways. First we concern about schemes' security, then we concern about schemes' efficiency.

Notations: In Table I, we denote with/without random oracle as W/O RO, assumption as Assum, security model as SecMod, colluding attackers as Colluding, underlying IBE as UnderIBE, stand model as Std, , proxy as P, DGA as delegator, DGE as delegatee. P and DGA means that proxy colludes with delegator, P or DGA means that proxy or delegator is malicious adversary but they never collude. SymEnc-Sec means the security of symmetric encryption.

TABLE I.
IBPRE SECURITY COMPARISON

Scheme	Security	W/O RO	Assum	SecMod	Colluding	UnderlyIBE	Remark
GA07A[15]	IND-Pr-ID-CPA ␣	RO	DBDH	Sec.3.1[15]	P and DGA or P and DGE	BF IBE	Weak
GA07B[15]	IND-Pr-ID-CCA ␣	RO	DBDH	Sec.3.1[15]	P and DGA or P and DGE	BF IBE	Strong
M07B [27]	IND-Pr-sID-CPA ␣	Std	DBDH	Sec.4.2[27]	P or DGA or DGE	BB_1 IBE	Weak
CT07[11]	IND-Pr-ID-CPA ␣	Std	DBDH	Sec.4.2[11]	P and DGA or P and DGE	Waters' IBE	Weak
SXC08[29]	IND-Pr-ID-CCA ␣	Std	DBDH	Sec.2.6[29]	P and DGA or P and DGE	Waters' IBE	Strong
OursCIII-C	IND-Pr-sID-CPA ␣	Std	DBDH	III-B	P and DGA or P and DGE	Variant of BB_1 IBE	Weak
OursDIII-F	IND-Pr-ID-CCA ␣	RO	DBDH	III-B	P and DGA or P and DGE	Variant of BB_1 IBE	Strong

TABLE II.
IBPRE EFFICIENCY COMPARISON

Scheme	Enc	Check	Reenc	Dec		Ciph-Len	
				1stCiph	2-ndCiph	1stCiph	2-ndCiph
GA07A[15]	$1t_e + 1t_p$	0	$1t_p$	$2t_p$	$1t_p$	$2\|G\| + 2\|G_e\|$	$1\|G\| + 1\|G_e\|$
GA07B[15]	$1t_p + 1t_e$	$2t_p$	$2t_e + 2t_p$	$1t_e + 2t_p$	$2t_e + 2t_p$	$1\|G\| + 1\|G_e\| +2\|m\| + \|id\|$	$1\|G\| + 1\|G_T\| +1\|G_e\| + \|m\|$
M07B [27]	$1t_p + 2t_e$	$2t_p$	$1t_p$	$2t_p$	$2t_p$	$2\|G_e\| + 1\|G_T\|$	$2\|G_e\| + 1\|G_T\|$
CT07[11]	$3t_e + 1t_p + 1t_s$	$1t_v$	$2t_e$	$2t_e + 10t_p + 1t_v$	$2t_e + 3t_p$	$9\|G\| + 2\|G_T\| +\|vk\| + \|s\|$	$3\|G\| + \|G_T\| +\|vk\| + \|s\|$
SXC08[29]	$3t_e + 1t_p + 1t_s$	$1t_v$	$2t_e + 1t_s$	$2t_e + 10t_p + 2t_v$	$2t_e + 3t_p + 1t_v$	$9\|G\| + 2\|G_T\| +2\|vk\| + 2\|s\|$	$3\|G\| + \|G_T\| +1\|vk\| + 1\|s\|$
OursCIII-C	$2t_e + 1t_p$	$2t_p$	$1t_e$	$4t_p$	$2t_p$	$6\|G\| + \|G_T\|$	$2\|G\| + \|G_T\|$
OursDIII-F	$3t_e + 1t_{me}$	$2t_p$	$1t_e$	$4t_p + 1t_e + 1t_{me}$	$2t_p + 1t_e + 1t_{me}$	$7\|G\| + m$	$4\|G\| + m$

From Table I, we can know that our IBPRE scheme based on a variant of BB_1 IBE scheme is the most secure IBPRE. M07B scheme is the weakest IBPRE for it can only achieve IND-Pr-sID-CPA under separated proxy or delegator or delegatee attack.

In Table II, we denote encryption as Enc, re-encryption as Reenc, decryption as Dec, ciphertext as Ciph and ciphertext length as Ciph-Len. t_p, t_e and t_{me} represent the computational cost of a bilinear pairing, an exponentiation and a multi-exponentiation respectively, while t_{s} and t_{v} represent the computational cost of a one-time signature signing and verification respectively. $|\mathbb{G}|$, $|\mathbb{Z}_q|$, $|\mathbb{G}_e|$ and $|\mathbb{G}_T|$ denote the bit -length of an element in groups $\mathbb{G}$, $\mathbb{Z}_q$, $\mathbb{G}_e$ and $\mathbb{G}_T$ respectively. Here $\mathbb{G}$ and $\mathbb{Z}_q$ denote the groups used in our scheme, while $\mathbb{G}_e$ and $\mathbb{G}_T$ are the bilinear groups used in GA07, CT07, SXC08 schemes, i.e., the bilinear pairing is $e : \mathbb{G}_e \times \mathbb{G}_e \to \mathbb{G}_T$. Finally, $|vk|$ and $|s|$ denote the bit length of the one-time signature's public key and a one-time signature respectively.

From Table II, Our schemes[3], GA07[4] and M07B schemes are much more efficient than CT07 and SXC08 scheme due to their underlying IBE is Waters' IBE. And for the proxy, CT07 and SXC08 scheme are much more efficient than others for their special paradigm, our IBPRE scheme is more efficient than GA07B scheme and our other schemes, we think this is important for resisting DDos attack against the proxy.

[3]Our first level ciphertext maps second level ciphertext and second level ciphertext maps first level ciphertext in [15], [11], [29]. Sometimes in our schemes we use $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ or $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, in the former cases, $\mathbb{G}$ maps to $\mathbb{G}_e$, $\mathbb{G}_1$ maps $\mathbb{G}_T$, in the latter case, $\mathbb{G}_1$ maps to $\mathbb{G}_e$, $\mathbb{G}_T$ maps $\mathbb{G}_T$.

[4]GA07 and SXC08 are multi-hop IBPRE but we just consider their single-hop variant.

V. CONCLUSIONS AND OPEN PROBLEMS

In 2007, Matsuo proposed the concept of four types of PRE schemes: CBE to CBE, IBE to CBE, CBE to IBE and IBE to IBE [27]. In Matsuo's scheme, they allow the PKG to help the delegator and the delegatee to generate re-encryption key. We explore this feature further, if we allow PKG to generate re-encryption keys by directly using $\mathsf{master-key}$, many open problems can be solved. Considering the standardization of BB_1 IBE and its broad applications, we give new identity based proxy re-encryption schemes based on BB_1 IBE, and prove its security in our new stronger security models. Furthermore, our schemes are very efficient for the re-encryption process, which is the most heavy-load part of PRE.

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, E. Goh, T. Matsuo. Proposal for P1363.3 Proxy Re-encryption. http://grouper.ieee.org/groups/1363/IBC /submissions/NTTDataProposal-for-P1363.3-2006-09-01.pdf.

[4] D. Boneh, 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 Rando Oracles. In *CRYPTO 2004*, volume 3152 of *LNCS*, pages 443–459, 2004.

[7] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil Pairing. In *ASIACRYPTO 2001*, volume 1976 of *LNCS*, pages 514–532, 2004.

[8] M. Barbosa, L. Chen, Z. Cheng. SK−KEM: An Identity−based Kem. http://grouper.ieee.org/groups/1363/IBC/submissions/Barbosa-SK-KEM-2006-06.pdf.

[9] R. Canetti, S. Halevi and J. Katz. A forward-secure public-key encryption scheme. In *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 255–271, 2003.

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

[11] C. Chu and W. Tzeng. Identity-based proxy re-encryption without random oracles. In *ISC 2007*, volume 4779 of *LNCS*, pages 189–202, 2007.

[12] L. Chen and Z. Cheng. Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme. http://eprint.iacr.org/2005 /226.pdf, 2005.

[13] Y. Dodis. and A. Ivan Proxy cryptography revisited. In *Internet Society (ISOC): NDSS 2003*, 2003.

[14] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *CRYPTO 1999*, volume 1666 of *LNCS*, pages 535–554, 1999.

[15] M. Green and G. Ateniese. Identity-based proxy re-encryption. In *ACNS 2007*, volume 4521 of *LNCS*, pages 288–306, 2007.

[16] V. Goyal. Reducing Trust in Identity Based Cryptosystems. In *CRYPTO 2007*, volume 4622 of *LNCS*, pages 430–447, 2007.

[17] C. Gentry. Practical Identity-Based Encryption without Random Oracles. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464, 2006.

[18] E. Goh and T. Matsuo. Proposal for P1363.3 Proxy Re-encryption. http://grouper.ieee.org/groups/1363/IBC /submissions/NTTDataProposal-for-P1363.3-2006-08-14.pdf.

[19] S. Hohenberger. Advances in Signatures, Encryption, and E-Cash from Bilinear Groups. Ph.D. Thesis, MIT, May 2006.

[20] S. Hohenberger, G. N. Rothblum, a. shelat, V. Vaikuntanathan. Securely Obfuscating Re-encryption. In *TCC 2007*, volume 4392 of *LNCS*, pages 233–252, 2007.

[21] M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In *PKC 1999*, volume 1560 of LNCS, pages 112–121, 1999.

[22] 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.

[23] M. Luo, C. Zou, J. Xu. An efficient identity-based broadcast signcryption scheme. In *Journal of Software*, pages 366-373, Vol. 7, Num. 2, 2012.

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

[25] B. Libert and D. Vergnaud. Tracing malicious proxies in proxy re-encryption. In *Pairing 2008*, volume 5209 of *LNCS*, pages 332–353, 2008.

[26] T. Matsuo. Proxy re-encryption systems for identity-based encryption. In *PAIRING 2007*, volume 4575 of *LNCS*, pages 247–267, 2007.

[27] L. Martin(editor). P1363.3(TM)/D1, Draft Standard for Identity-based Public Cryptography Using Pairings, May 2008.

[28] 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.

[29] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report2003/054. 2003.

[30] 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.

[31] Q. Tang. Type-based proxy re-encryption and its construction. In *INDOCRYPT 2008*, volume 5365 of *LNCS*, pages 130–144, 2008.

[32] 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.

[33] X. A. Wang, X. Y. Yang, J. R. Hu. CCA-Secure Identity Based Proxy Re-encryption Based on a Variant of BB1 IBE. The 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC 2010), IEEE Press, (Vol.2) 509-513, 2010.

[34] Y. Ding, X. A. Wang. Identity Based Proxy Re-encryption Based on a Variant of BB1 Identity Based Encryption. The 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC 2010), IEEE Press, (Vol.2) 509-513, 2010.

[35] L. D. Zhou, M. A. Marsh, F. B. Schneider, and A. Redz. Distributed blinding for ElGamal re-encryption. TR 1924, Cornell CS Dept., 2004.

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 University of Chinese Armed Police Force. Now he is an associate professor in the same University. His main research interests includes public key cryptography and information security.

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.