Hybrid Proxy Re-encryption Between IBE And CBE

Jindan Zhang[1], Xu An Wang[2], 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 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). We observe that the proxy re-encryption from CBE to IBE scheme in Matsuo's scheme inherits the key escrow problem from IBE. Is this necessary for proxy re-encryption from CBE to IBE? We give a negative answer. If we emphasis on the PKG's involving in the re-encryption key generation, some interesting results can be obtained. We propose the concept of hybrid proxy re-encryption without key escrow, give the new security model for this primitive, construct such a scheme and prove its security. Furthermore, we construct the first proxy re-encryption scheme from from IBE to CBE, giving the security model for this new primitive and prove its security. At last, we compare our schemes with other related schemes, the results show that our schemes can have high level security with good efficiency.**

***Index Terms*— Cryptography, Hybrid proxy re-encryption, IBE, CBE, Without key escrow, Security proof.**

I. Introduction

In 1998, Blaze, Bleumer, and Strauss introduced the concept of proxy re-encryption (PRE) [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 outsourced filtering of encrypted spam [1]. Since then, many excellent schemes have been proposed [4]–[6], [9]–[11]. In ACNS'07, Green et al. proposed the first identity based proxy re-encryption schemes(IDPRE) [6]. 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 [11].

The second author is the corresponding author. This paper is an extended work of [12], [13] 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 Motivation and Contribution

In Pairing'07, Matsuo proposed another few more PRE schemes in identity based setting [10]. Interestingly, they proposed the concept of four types of PRE: CBE(Certificate Based Public Key Encryption) [1] IBE (Identity Based Encryption)(type 1), IBE to IBE (type 2), IBE to CBE (type 3), CBE to CBE (type 4) [10], which can help the ciphertext [8], [14] 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.

We think enabling the different types of ciphertext circulate smoothly in the network is very important for the cloud application and ubiquitous computation, especially considering the new encryption paradigm: functional encryption will come at age in the near future. It is not strange one day you will meet the ciphertexts constructed by attribute-based encryption, hidden-vector encryption, predicate-based encryption, identity based encryption, public key encryption and others. Finding a mechanism which can handle these ciphertext smoothly while not giving many changes to the existing information system will be an important task for the engineries. Until now although many cryptographic protocols have been proposed, but it seems that the only proper solution is hybrid proxy re-encryption for this situation, which can achieve some balance between security and easily useable.

We extend Matsuo's research on PRE in identity based setting [10]. We observe that: proxy re-encryption from CBE to IBE scheme in [10] inherits the key escrow problem from IBE. That is, PKG can decrypt every re-encrypted ciphertext for IBE users.

For example, scientist Alice with public/private key pair (sk_A, pk_A) *might want to exploit an* PRE *from* CBE *to* IBE *so that messages encrypted under her public key can be "automatically" converted into ciphertext for her assistant Bob under his identifier. Bob's company sets up an* IBE *system where Manager Malice plays the role of*

[1]Here we refer CBE to be the standard public key encryption, which is different from the CBE concept in [7].

doi:10.4304/jcp.8.7.1873-1881

PKG *for secure communication. If Alice and Bob adapt Matsuo's* PRE *from* CBE *to* IBE*, Malice can read every re-encrypted ciphertext for Bob. This is intolerable.*

To solve this problem, we propose the concept of hybrid proxy re-encryption from IBE to CBE without key escrow. We detail our main contributions as following:

1) Like the idea in certificateless public encryption, we propose the concept of hybrid proxy re-encryption from IBE to CBE without key escrow, elaborate the security model and construct such a scheme. The security model for this new primitive is complex for it introducing a new adversary PKG.
2) We construct a PRE from IBE to CBE scheme. The main novelty for our scheme is allowing PKG generating re-encryption keys by using its $\mathsf{master-key}$ in its plain form, while all previous schemes just allowing PKG generating re-encryption keys by using its $\mathsf{master-key}$ in exponential form.

B. Organization

We organize our paper as following. In Section II, we propose the concept of hybrid PRE from IBE to CBE without key escrow and its security model. In Section III, we show how to construct such a scheme based on PRE from CBE to IBE in [10]. In Section IV, we review the concept of PRE from IBE to CBE and detail its security model. In Section V, we propose the first proxy re-encryption scheme from IBE to CBE and prove its security. In Section VI, we give our comparison results. We give our conclusions in Section VII.

II. Hybrid PRE from CBE to IBE without Key Escrow

Definition 1: Hybrid PRE from CBE to IBE consists of: 1)the three algorithms making up a CBE system $\mathsf{KeyGen_{CBE}}$, $\mathsf{Enc_{CBE}}$ and $\mathsf{Dec_{CBE}}$ 2)the four algorithms making up an IBE system $\mathsf{SetUp_{IBE}}$, $\mathsf{KeyGen_{IBE}}$, $\mathsf{Enc_{IBE}}$ and $\mathsf{Dec_{IBE}}$ 3)and three algorithms for re-encryption, which are

1) **KeyGen**$_{PRO}(\mathsf{sk}, \mathbf{ID}, \mathsf{mk})$. Given a CBE secret key sk, an IBE secret key sk_{ID} for the IBE user ID, PKG's $\mathsf{master-key}$ mk, generate a re-encryption key rk which can re-encrypt CBE ciphertexts for pk into the IBE ciphertexts for ID.
2) **ReEnc**$(\mathsf{rk}, \mathsf{C_{pk}}, \mathbf{ID})$. Given the re-encryption key rk, a ciphertext $\mathsf{C_{pk}}$ encrypted under the traditional public key, and ID, re-encrypt ciphertext $\mathsf{C_{pk}}$ into $\mathsf{C_{ID}}$ that can be decrypted by the IBE user ID.
3) **Check**$(\mathsf{parms}, \mathsf{C_{pk}}, \mathsf{pk})$. Given $\mathsf{C_{pk}}$ and pk with parms, output 0 if $\mathsf{C_{pk}}$ is a malformed ciphertext. Otherwise, output 1.

Remark 1: Our definition is different from Matsuo's definition [10] about PRE from CBE to IBE. That is, we allow PKG generating re-encryption key directly by using its $\mathsf{master-key}$ mk while Matsuo's scheme only allow PKG helping the delegator and the delegatee generating re-encryption key indirectly.

Remark 2: Just like the PRE definition in Section 2.1 in [9], sometimes we can further distinguish the $\mathsf{Enc_{CBE}}$ and $\mathsf{Dec_{CBE}}$, $\mathsf{Enc_{IBE}}$ and $\mathsf{Dec_{IBE}}$ algorithms as two level algorithms. For example, we can distinguish $\mathsf{Enc_{IBE}}$ as $\mathsf{Enc1_{IBE}}$ and $\mathsf{Enc2_{IBE}}$ algorithms. $\mathsf{Enc2_{IBE}}$ outputs a second level ciphertext which can be re-encrypted as a first level ciphertext. $\mathsf{Enc1_{IBE}}$ outputs a first level ciphertext which can not be re-encrypted. In our proposed PRE from CBE to IBEIII-A, we distinguish $\mathsf{Dec_{IBE}}$ as a two level algorithm. $\mathsf{Dec2_{IBE}}$ can only decrypt the second level ciphertext- normal IBE ciphertext while $\mathsf{Dec1_{IBE}}$ can only decrypt the first level ciphertext- the re-encrypted ciphertext.

A. Security Model

In this section, we give our security models for PRE from CBE to IBE which based on [4], [9]. *Internal and External Security*. Our security model protects users from two types of attacks: those launched from parties outside the system (*External Security*), and those launched from parties inside the system, such as the proxy, another partner, PKG, or some collusion between them (*Internal Security*). Generally speaking, internal adversaries are more powerful than external adversaries. And our scheme can achieve reasonable internal security. We just provide formalization of *internal security* notions.

Delegatee Security.

Because in PRE from CBE to IBE, PKG knows every IBE's normal secret key. So for every level 2 normal ciphertext, PKG can decrypt them and ciphertext generated by $\mathsf{Enc_{IBE}}(\mathsf{ID}, \mathsf{parms}, \mathsf{M})$. Thus we only consider the case that proxy and delegator are colluding for level 2 ciphertext.

Definition 2: **(IBE-LV2-IND-ID-CPA)** A PRE scheme from CBE to IBE is IBE-LV2-IND-ID-CPA[2] secure if the probability

$$\begin{aligned}
Pr[\{(ID^\star, sk_{ID^\star})\} \leftarrow KeyGen_{IBE}(\cdot) \\
,\{(pk_x, sk_x) \leftarrow KeyGen_{CBE}(\cdot)\}, \\
\{(ID_x, sk_{ID_x}) \leftarrow KeyGen_{IBE}(\cdot)\}, \\
\{(pk_h, sk_h) \leftarrow KeyGen_{CBE}(\cdot)\}, \\
\{(ID_h, sk_{ID_h}) \leftarrow KeyGen_{IBE}(\cdot)\}, \\
\{R_{hx} \leftarrow KeyGen_{PRO}(sk_h, ID_x, mk, parms)\}, \\
\{R_{xh} \leftarrow KeyGen_{PRO}(sk_x, ID_h, mk, parms)\}, \\
\{R_{hh} \leftarrow KeyGen_{PRO}(sk_h, ID_h, mk, parms)\}, \\
\{R_{xx} \leftarrow KeyGen_{PRO}(sk_x, ID_x, mk, parms)\}, \\
\{R_{x\star} \leftarrow KeyGen_{PRO}(sk_x, ID^\star, mk, parms)\}, \\
\{R_{h\star} \leftarrow KeyGen_{PRO}(sk_h, ID^\star, mk, parms)\}, \\
(m_0, m_1, St) \leftarrow A^{\mathcal{O}_{renc}}(ID^\star, \{(pk_x, sk_x)\}, \\
\{(ID_x, sk_{ID_x})\}, \{pk_h\}, \{ID_h\}, \{R_{xh}\}, \\
\{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\}, \{R_{x\star}\}, \{R_{h\star}\}), \\
d^\star \xleftarrow{R} \{0,1\}, C^\star = Enc_{IBE}(m_{d^\star}, ID^\star, parms), \\
d' \leftarrow \mathcal{A}^{\mathcal{O}_{renc}}(C^\star, St) : d' = d^\star]
\end{aligned}$$

[2]LV2 denotes Level 2 ciphertext.

is negligibly close to $1/2$ for any PPT adversary $\mathcal{A}$. 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 $\mathcal{A}$.

Remark 3: The Re-encryption Oracle $\mathcal{O}_{renc}$ can not give the adversary more help, because we consider the case the proxy and the delegator corrupted. When the proxy is corrupted, the adversary can do re-encryption himself. The reason why we do not delete the Re-encryption Oracle $\mathcal{O}_{renc}$ oracle in the above definition is that this makes our definition more general and consistent with other definitions in the literature [4], [9].

In PRE from CBE to IBE, the delegator certainly can decrypt the ciphertext which will be re-encrypted. Thus we consider only the case that proxy and PKG are colluding, We must point out this model is not considered in the current literature. The goal of solving the key escrow problem for PRE from CBE to IBE is just constructing a scheme which can resist the malicious PKG attack. But we consider a stronger model which can resist the the malicious PKG and proxy colluding attack.

Definition 3: **(IBE-LV1-IND-ID-CPA)** A PRE scheme from CBE to IBE is IBE-LV1-IND-ID-CPA[3] secure if the probability

$$\begin{aligned}
Pr[(parms, master-key) \leftarrow Setup_{IBE}(\cdot),\\
\{(ID^\star, sk_{ID^\star}) \leftarrow KeyGen_{IBE}(\cdot)\},\\
\{(pk^\star, sk^\star) \leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(pk_x, sk_x) \leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_x, sk_{ID_x}) \leftarrow KeyGen_{IBE}(\cdot)\},\\
\{(pk_h, sk_h) \leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_h, sk_{ID_h}) \leftarrow KeyGen_{IBE}(\cdot)\},\\
\{R_{hx} \leftarrow KeyGen_{PRO}(sk_h, ID_x, mk, parms)\},\\
\{R_{xh} \leftarrow KeyGen_{PRO}(sk_x, ID_h, mk, parms)\},\\
\{R_{hh} \leftarrow KeyGen_{PRO}(sk_h, ID_h, mk, parms)\},\\
\{R_{xx} \leftarrow KeyGen_{PRO}(sk_x, ID_x, mk, parms)\},\\
\{R_{x\star} \leftarrow KeyGen_{PRO}(sk_x, ID^\star, mk, parms)\},\\
\{R_{h\star} \leftarrow KeyGen_{PRO}(sk_h, ID^\star, mk, parms)\},\\
\{R_{\star h} \leftarrow KeyGen_{PRO}(sk^\star, ID_h, mk, parms)\},\\
\{R_{\star x} \leftarrow KeyGen_{PRO}(sk^\star, ID_x, mk, parms)\},\\
\{R_{\star\star} \leftarrow KeyGen_{PRO}(sk^\star, ID^\star, mk, parms)\}\\
(m_0, m_1, St) \leftarrow A^{O_{renc}}(ID^\star, pk^\star\{(pk_x, sk_x)\},\\
\{(ID_x, sk_{ID_x})\}, \{pk_h\}, \{ID_h\}, \{R_{xh}\},\\
\{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\},\\
\{R_{\star h}\}, \{R_{\star x}\}, \{R_{h\star}\}, \{R_{x\star}\}, \{R_{\star\star}\}, \{master-key\}),\\
d^\star \xleftarrow{R} \{0,1\}, C^\star = ReEnc(Enc_{CBE}(m_{d^\star}, pk^\star),\\
ID^\star, R_{\star\star}, parms), d' \leftarrow \mathcal{A}^{O_{renc}}(C^\star, St) : d' = d^\star]
\end{aligned}$$

is negligibly close to $1/2$ for any PPT adversary $\mathcal{A}$. The notations in this game are same as Definition 2 except the definition of Re-encryption Oracle $\mathcal{O}_{renc}$. In this game, any input makes $\mathcal{O}_{renc}$ outputting $C^\star$ will be returned with $\perp$.

Remark 4: In this definition, we set two target users - $pk^\star$, $ID^\star$. The reason is that the target ciphertext can be seen as the ciphertext for $ID^\star$ and its second level ciphertext can be seen as the ciphertext for $pk^\star$. In our definition, we consider the proxy being corrupted. That means, the proxy can know which second level ciphertext can be re-encrypted as the target first level ciphertext. Of course, if the proxy is not corrupted, and the proxy re-encryption is untraceable, the security model can allow any delegator corrupting including $pk^\star$.

Delegator Security.

In PRE from CBE and IBE, the delegator is a CBE user. In this case, we consider the delegatee, proxy and PKG are all colluding.

Definition 4: **(CBE-IND-CPA)** A PRE scheme from CBE to IBE is CBE-IND-CPA secure if the probability

$$\begin{aligned}
\Pr[(parms, master-key) \leftarrow Setup_{IBE}(\cdot),\\
\{(pk^\star, sk^\star) \leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(pk_x, sk_x) \leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_x, sk_{ID_x}) \leftarrow KeyGen_{IBE}(\cdot)\},\\
\{(pk_h, sk_h) \leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_h, sk_{ID_h}) \leftarrow KeyGen_{IBE}(\cdot)\},\\
\{R_{hx} \leftarrow KeyGen_{PRO}(sk_h, ID_x, mk, parms)\},\\
\{R_{xh} \leftarrow KeyGen_{PRO}(sk_x, ID_h, mk, parms)\},\\
\{R_{hh} \leftarrow KeyGen_{PRO}(sk_h, ID_h, mk, parms)\},\\
\{R_{xx} \leftarrow KeyGen_{PRO}(sk_x, ID_x, mk, parms)\},\\
\{R_{\star h} \leftarrow KeyGen_{PRO}(sk^\star, ID_h, mk, parms)\},\\
\{R_{\star x} \leftarrow KeyGen_{PRO}(sk^\star, ID_x, mk, parms)\},\\
(m_0, m_1, St) \leftarrow A^{O_{renc}}(pk^\star\{(pk_x, sk_x)\},\\
\{(ID_x, sk_{ID_x})\}, \{pk_h\}, \{ID_h\}, \{R_{xh}\},\\
\{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\},\\
\{R_{\star h}\}, \{R_{\star x}\}, \{master-key\}),\\
d^\star \xleftarrow{R} \{0,1\}, C^\star = Enc_{CBE}(m_{d^\star}, pk^\star),\\
d' \leftarrow A^{O_{renc}}(C^\star, St) : d' = d^\star]
\end{aligned}$$

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

PKG **Security.**

[3]LV1 denotes Level 1 ciphertext.

In PRE from CBE and IBE, PKG's master − key can not leverage even if the delegator, the delegatee and proxy collude. We denote this security property as **(PKG-OW)**.

III. A Hybrid PRE from CBE to IBE without Key Escrow Scheme

A. The Proposed Scheme

We construct our scheme based on the above PRE scheme. Our scheme shares the same underlying CBE scheme (ElGamal-type CBE scheme) as [10] scheme. The difference lies in the underlying IBE scheme and delegation scheme.

- The underlying IBE scheme (Variant of BB_1 IBE scheme):
  1) **SetUp**$_{\mathsf{IBE}}(k)$. Given a security parameter k, select a random generator $g \in G$ and random elements $g_2, h \in G$. Pick a random $\alpha \in Z_p^*$. Set $g_1 = g^\alpha$,$\mathsf{mk} = g_2^\alpha$, and $\mathsf{parms} = (g, g_1, g_2, h)$. Let mk be the master − key and let parms be the public parameters.
  2) **KeyGen**$_{\mathsf{IBE}}(mk, \mathsf{parms}, ID)$. Given $\mathsf{mk} = g_2^\alpha$ and ID with parms, pick a random $u \in Z_p^*$. Set $(d_0, d_1) = (g_2^\alpha (g_1^{ID} h)^u, g^u)$. The delegatee chooses a collision resistent hash function $H : \{0,1\}^{3|p|} \rightarrow Z_p^*$ and a random seed $r \in Z_p^*$, and computes $k = H(pk, ID, r)$. The delegatee's private key is $sk_{\mathsf{ID}} = (d_0, d_1, k) = (g_2^\alpha (g_1^{ID} h)^u, g^u, k)$.
  3) **Enc**$_{\mathsf{IBE}}(\mathbf{ID}, \mathsf{parms}, M)$. To encrypt a message $M \in G_1$ under the public key $\mathsf{ID} \in Z_p^*$, pick a random $r \in Z_p^*$ and compute $\widetilde{C_{ID}} = (\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3}) = (g^r, (g_1^{ID} h)^r, Me(g_1, g_2)^r)$.
  4) **Dec1**$_{\mathsf{IBE}}(sk_{\mathsf{ID}}, \mathsf{parms}, C_{\mathsf{ID}})$. Given a re-encrypted ciphertext $\widehat{C_{ID}} = (\widehat{C_1}, \widehat{C_2}, \widehat{C_3}, \widehat{C_4})$, $sk_{ID} = (d_0, d_1, k)$, parms, compute $M = (\frac{\widehat{C_3}\widehat{C_4}^k e(d_1, \widehat{C_2}^k)}{e(d_0, \widehat{C_1}^k)})^{\frac{1}{k}}$.
  5) **Dec2**$_{\mathsf{IBE}}(sk_{\mathsf{ID}}, \mathsf{parms}, C_{\mathsf{ID}})$. Given ciphertext $C_{ID} = (\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3})$ and the secret key $sk_{ID} = (d_0, d_1)$ with parms, compute $M = \widetilde{C_3} e(d_1, \widetilde{C_2}) / e(d_0, \widetilde{C_1})$.
- The underlying CBE scheme (ElGamal-type CBE scheme):
  1) **KeyGen**$_{\mathsf{CBE}}(k, \mathsf{parms})$. Given a security parameter k , parms, pick a random $\theta, \beta, \delta \in Z_p$. Set $g_3 = g^\theta, g_4 = g_1^\beta, g_5 = h^\delta$. The public key is $pk = (g_3, g_4, g_5)$. The secret random key is $sk = (\theta, \beta, \delta)$.
  2) **Enc**$_{\mathsf{CBE}}(pk, parms, M)$. Given $pk = (g_3, g_4, g_5)$ and a message M with parms, pick a random $r \in Z_p^*$ and compute $C_{pk} = (C_1, C_2, C_3, C_4) = (g_3^r, g_4^r, g_5^r, Me(g_1, g_2)^r)$.
  3) **Dec**$_{\mathsf{CBE}}(sk, parms, C_{pk})$. Given $C_{pk} = (C_1, C_2, C_3, C_4)$ and the secret key $sk = (\theta, \beta, \delta)$ with parms, compute $M = C_4 / e(C_2^{1/\beta}, g_2)$.
- The delegation scheme:
  1) **KeyGen**$_{PRO}(sk, sk_{ID}, mk, \mathsf{parms})$. On input (θ, β, δ) from the delegator and input (g^u, k) from the delegatee, outputs the re-encryption key $rk_{pk \rightarrow ID} = (1/\theta, g^{ku/\beta}, 1/\delta)$.
  2) **ReEnc**$(rk_{ID}, \mathsf{parms}, C_{pk}, ID)$. Given a CBE ciphertext $C_{pk} = (C_1, C_2, C_3, C_4)$, the re-encryption key $rk_{pk \rightarrow ID} = (1/\theta, g^{ku/\beta}, 1/\delta)$ and ID with parms, re-encrypt the ciphertext C_{pk}into C_{ID} as following: $\widehat{C_{ID}} = (\widehat{C_1}, \widehat{C_2}, \widehat{C_3}, \widehat{C_4}) = (C_1^{1/\theta}, C_3^{1/\delta}, e(g^{ku/\beta}, C_2^{ID}), C_4)$.
  3) **Check**(parms, C_{pk}, pk). Given $C_{pk} = (C_1, C_2, C_3, C_4)$ and $pk = (g_3, g_4, g_5)$ with parms, set $v_1 = e(C_1, g_4)$, $v_2 = e(C_2, g_3)$, $v_3 = e(C_2, g_5)$ and $v_4 = e(C_3, g_4)$. If $v_1 = v_2$ and $v_3 = v_4$, output 1, otherwise output 0.

We verify correctness of our scheme. Following the $\mathsf{Dec2}_{\mathsf{IBE}}(sk_{\mathsf{ID}}, \mathsf{parms}, C_{\mathsf{ID}})$ algorithm, we get

$$\begin{aligned} & (\frac{\widehat{C_3}\widehat{C_4}^k e(d_1, \widehat{C_2}^k)}{e(d_0, \widehat{C_1}^k)})^{\frac{1}{k}} \\ = \; & (\frac{e(g^{ku/\beta}, C_2'^{ID}) M^k e(g_1, g_2)^{rk} e(g^u, h^{kr})}{e(g_2^\alpha (g_1^{ID} h)^u, g^{rk})})^{\frac{1}{k}} = M \end{aligned}$$

Remark 5: In our scheme, every IBE user has a self generated private key k. It's this k that can make our scheme resist malicious PKG decrypting IBE user's re-encrypted ciphertext.

B. Security Analysis

Theorem 1: Suppose the DBDH assumption holds, then our scheme is IBE-LV2-IND-sID-CPA secure for the proxy and delegator's colluding.

Proof: Suppose $\mathcal{A}$ can attack our scheme, we construct an algorithm $\mathcal{B}$ solves the DBDH problem in $\mathbb{G}$. On input (g, g^a, 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 $ID^\star$ 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 $h = g_1^{-ID^\star} g^{\alpha'}$. It gives $\mathcal{A}$ the parameters $\mathsf{parms} = (g, g_1, g_2, h)$. Note that the corresponding master − key, which is unknown to $\mathcal{B}$, is $g_2^a = g^{ab}$. B picks random $x_i, y_i, z_i \in Z_p$, computes $g_{i_1} = g^{x_i}, g_{i_2} = g^{y_i}, g_{i_3} = h^{z_i}$. It gives $\mathcal{A}$ the public key $pk_i = (g_{i_1}, g_{i_2}, g_{i_3})$.
3) **Phase 1**
   - *"$\mathcal{A}$ issues up to private key queries on ID_i."* $\mathcal{B}$ selects randomly $r_i \in Z_p{}^\star$ and $k' \in Z_p$, sets $sk_{ID_i} = (d_0, d_1, d_2) = (g_2^{\frac{-\alpha'}{ID_i - ID^\star}} (g_1^{(ID_i - ID^\star)} g^{\alpha'})^{r_i}, g_2^{\frac{-1}{ID_i - ID^\star}} g^{r_i}, k')$. We claim sk_{ID_i} is a valid random private key for ID_i. To see this, let $\widetilde{r_i} = r_i - \frac{b}{ID - ID^\star}$.

Then we have that $d_0 = g_2^{\frac{-\alpha'}{ID_i - ID^\star}} (g_1^{(ID_i - ID^\star)} g^\alpha)^{r_i} = g_2^\alpha (g_1^{(ID_i - ID^\star)} g^\alpha)^{r_i - \frac{b}{ID - ID^\star}} = g_2^a (g_1^{ID_i} h)^{\widetilde{r_i}}$. $d_1 = g_2^{\frac{-1}{ID_i - ID^\star}} g^{r_i} = g^{\widetilde{r_i}}$.

- *"$\mathcal{A}$ issues up to private key queries on pk_i".* $\mathcal{B}$ returns (x_i, y_i, z_i).
- *"$\mathcal{A}$ issues up to re-encryption key queries on (pk_j, ID_i)".* The challenge $\mathcal{B}$ computes $rk_{pk_j \to ID_i} = (k'/x_j, (g_2^{\frac{-1}{ID_i - ID^\star}} g^{r_i})^{\frac{k'}{y_j}}, k'/z_j)$ and returns it to $\mathcal{A}$.
- *"$\mathcal{A}$ issues up to re-encryption key queries on $(pk_j, ID^\star)$".* The challenge $\mathcal{B}$ randomly choose a $k' \in Z_p$, and computes $rk_{pk_j \to ID^\star} = (k'/x_j, (g^{u'})^{k'/y_j}, k'/z_j)$ where u' is a randomly choose from Z_p^* and returns it to A.
- *"$\mathcal{A}$ issues up to re-encryption queries on (C, pk_j, ID_i) or $(C, pk_j, ID^\star)$"* The challenge $\mathcal{B}$ runs $\mathsf{ReEnc}(rk_{pk_j \to ID_i}, C, pk_j, ID_i)$ or $\mathsf{ReEnc}(rk_{pk_j \to ID^\star}, C, pk_j, ID^\star)$ 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 $C^\star = (g^c, (g^\alpha)^c, M_b \cdot T)$. Hence if $T = e(g,g)^{abc} = e(g_1, g_2)^c$, then $C^\star$ is a valid encryption of M_b under $ID^\star$. Otherwise, $C^\star$ is independent of b in the adversary's view.
5) **Phase2** $\mathcal{A}$ issues queries as he does in Phase 1 excepts 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: Our scheme is IBE-LV1-IND-ID-CPA secure for the proxy and PKG's colluding.

Proof: The security proof follows the security of symmetrical encryption.

1) **Setup**. To generate the system's parameters, the challenger $\mathcal{B}$ picks $\alpha \in Z_p$, it randomly choose $x \in Z_q^*$,$y \in Z_q^*$ and computes $h = g^x$, $g_1 = g^\alpha$, $g_2 = g^y$, $\mathsf{master-key} = g_2^\alpha$. It gives $\mathsf{parms} = (g, g_1, g_2, h)$ to $\mathcal{A}$.
2) **Phase 1**
   - *"$\mathcal{A}$ issues up to master-key query "*. The challenger $\mathcal{B}$ returns (α, g_2^α).
   - *"$\mathcal{A}$ issues up to private key queries on ID".* Given $mk = g_2^\alpha$ and ID with parms, pick a random $u, k' \in Z_p^*$. Set $sk_{ID} = (d_0, d_1, d_2) = (g_2^\alpha (g_1^{ID} h)^u, g^u, k')$.
   - *"$\mathcal{A}$ issues up to private key queries on pk".* B returns (θ, β, δ).
   - *"$\mathcal{A}$ issues up to rekey generation queries on (pk, ID)".* The challenge $\mathcal{B}$ chooses randomly $k' \in Z_p^*$ and computes $rk_{pk \to ID} = (k'/\theta, g^{k'u/\beta}, k'/\delta)$ and returns it to $\mathcal{A}$.
   - *"$\mathcal{A}$ issues up to re-encryption queries on (C, pk, ID)".* The challenge $\mathcal{B}$ runs $ReEnc(rk_{pk \to ID}, C, pk, ID)$ and return the results.
3) **Challenge** When $\mathcal{A}$ decides that Phase1 is over, it outputs two messages $M_0, M_1 \in G$ and the attack identity $ID^\star$, Algorithm $\mathcal{B}$ picks g^u as the $ID^\star$'s second item of its private key, he picks a random bit b and $r, k^\star \in Z_p^*$ responds with the ciphertext $C^\star = (g^r, h^r, e(g^{k^\star u}, g_1^{ID r}), M_b \cdot e(g_2, (g^{r\alpha}))$. Hence if $k^\star$ is the real secret key of $ID^\star$, then $C^\star$ is a valid encryption of M_b under $ID^\star$. Otherwise, $C^\star$ is independent of b in the adversary's view.
4) **Phase 2** $\mathcal{A}$ issues queries as he does in Phase 1 except natural constraints.
5) **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. Otherwise it outputs 0.

Thus the maximal probability of $\mathcal{A}$ successes is $1/p$, which is negligible.

■

Theorem 3: Our scheme is CBE-IND-CPA secure for the proxy, PKG and delegatee's colluding except the case of the target CBE ciphertext has not been re-encrypted by the proxy.

Proof: In this case, the PKG and delegatee's colluding just likes [10]'s PRE scheme from CBE to IBE, the proof is the same as [10]. ■

Theorem 4: Our scheme is not CBE-IND-CPA secure for the proxy, PKG and delegatee's colluding in the case of the target CBE ciphertext has been re-encrypted by the proxy.

Proof: Suppose the target CBE ciphertext is $C_{pk} = (C_1, C_2, C_3, C_4)$ which has been re-encrypted by proxy to be $\widehat{C_{ID}} = (\widehat{C_1}, \widehat{C_2}, \widehat{C_3}, \widehat{C_4}) = (C_1, C_3^{1/\delta}, e(g^{ku/\beta}, C_2^{ID}), C_4)$, PKG can decrypt the ciphertext as following. Because $\widehat{C_1} = g^r$, he can compute $w = g^{r\alpha}$ and gets the plaintext by computing

$$\frac{\widehat{C_4}}{e(w, g_2)} = \frac{Me(g_1, g_2)^r}{e(g^{r\alpha}, g_2)} = \frac{Me(g_1, g_2)^r}{e(g_1, g_2)^r} = M$$

■

Theorem 5: Suppose the DBDH assumption holds, then our scheme is PKG-OW secure for all of the proxy, delegatee and delegator's colluding.

Proof: We just give the intuition for this theorem. When considering the proxy, delegatee and delegator's colluding, PKG only interacts with the delegatee-its IBE user. And we know the BB_1 identity based encryption is IND-sID-CPA secure under DBDH assumption. That's imply the attacker can not recover the PKG's $\mathsf{master-key}$. ■

IV. HYBRID PRE FROM IBE TO CBE

Definition 5: PRE from IBE to CBE consists of: 1)the four algorithms making up an IBE system $\mathsf{SetUp}_{\mathsf{IBE}}$, $\mathsf{KeyGen}_{\mathsf{IBE}}$, $\mathsf{Enc}_{\mathsf{IBE}}$ and $\mathsf{Dec}_{\mathsf{IBE}}$ 2)the three algorithms making up a CBE system $\mathsf{KeyGen}_{\mathsf{CBE}}$, $\mathsf{Enc}_{\mathsf{CBE}}$ and $\mathsf{Dec}_{\mathsf{CBE}}$ 3)and three algorithms for re-encryption, which are

1) **KeyGen**$_{PRO}(\mathsf{sk}_{\mathbf{ID}}, \mathsf{sk}, \mathsf{pk}, \mathsf{mk}, \mathsf{parms})$. Given an IBE secret key sk_{ID} for the IBE user ID, a CBE secret key sk, PKG's master − key mk with parms,pk, generate a re-encryption key rk which can re-encrypt the IBE ciphertexts for ID into CBE ciphertexts for pk.
2) **ReEnc**$(\mathsf{rk}, \mathsf{parms}, \mathsf{C}_{\mathbf{ID}}, \mathsf{pk})$. Given the re-encryption key rk, a ciphertext C_{ID} encrypted under the identity ID, and pk with parms, re-encrypt ciphertext C_{ID} for ID into C_{pk} that can be decrypted by sk.
3) **Check**$(\mathsf{parms}, \mathsf{C}_{\mathbf{ID}}, \mathbf{ID})$. Given C_{ID} and ID with parms, output 0 if C_{ID} is a malformed ciphertext. Otherwise, output 1.

A. Security Model

Delegator Security.

In PRE from IBE and CBE, the delegator is a IBE user. In this case, we consider the delegatee, proxy are colluding.

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

$$\begin{aligned}
Pr[\{(ID^\star, sk_{ID^\star})\} &\leftarrow KeyGen_{IBE}(\cdot),\\
\{(pk_x, sk_x) &\leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_x, sk_{ID_x}) &\leftarrow KeyGen_{IBE}(\cdot)\},\\
\{(pk_h, sk_h) &\leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_h, sk_{ID_h}) &\leftarrow KeyGen_{IBE}(\cdot)\},\\
\{R_{hx} \leftarrow KeyGen_{PRO}(sk_{ID_h}, sk_x, pk_x, mk, \cdot)\},&\\
\{R_{xh} \leftarrow KeyGen_{PRO}(sk_{ID_x}, sk_h, pk_h, mk, \cdot)\},&\\
\{R_{hh} \leftarrow KeyGen_{PRO}(sk_{ID_h}, sk_h, pk_h, mk, \cdot)\},&\\
\{R_{xx} \leftarrow KeyGen_{PRO}(sk_{ID_x}, sk_x, pk_x, mk, \cdot)\},&\\
\{R_{\star x} \leftarrow KeyGen_{PRO}(sk_{ID^\star}, sk_x, pk_x, mk, \cdot)\},&\\
\{R_{\star h} \leftarrow KeyGen_{PRO}(sk_{ID^\star}, sk_h, pk_h, mk, \cdot)\},&\\
(m_0, m_1, St) &\leftarrow A^{\mathcal{O}_{renc}}(ID^\star, \{(pk_x, sk_x)\},\\
\{(ID_x, sk_{ID_x})\}, \{pk_h\}, \{ID_h\}, \{R_{xh}\},&\\
\{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\}, \{R_{\star x}\}, \{R_{\star h}\}),&\\
d^\star \xleftarrow{R} \{0,1\}, C^\star = Enc_{IBE}(m_{d^\star}, ID^\star, parms),&\\
d' \leftarrow \mathcal{A}^{\mathcal{O}_{renc}}(C^\star, St) : d' = d^\star]&
\end{aligned}$$

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

Delegatee Security.

In PRE from IBE and CBE, the delegatee is a CBE user. We consider the second level CBE ciphertext [4]. In this case, we assume the delegator, proxy and PKG are colluding.

Definition 7: **(CBE-LV2-IND-CPA)** A PRE scheme from IBE to CBE is CBE-LV2-IND-CPA secure for CBE if the probability

$$\begin{aligned}
\Pr[(parms, master-key) &\leftarrow Setup_{IBE}(\cdot),\\
\{(pk^\star, sk^\star) &\leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(pk_x, sk_x) &\leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_x, sk_{ID_x}) &\leftarrow KeyGen_{IBE}(\cdot)\},\\
\{(pk_h, sk_h) &\leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_h, sk_{ID_h}) &\leftarrow KeyGen_{IBE}(\cdot)\},\\
\{R_{hx} \leftarrow KeyGen_{PRO}(sk_{ID_h}, sk_x, pk_x, mk, \cdot)\},&\\
\{R_{xh} \leftarrow KeyGen_{PRO}(sk_{ID_x}, sk_h, pk_h, mk, \cdot)\},&\\
\{R_{hh} \leftarrow KeyGen_{PRO}(sk_{ID_h}, sk_h, pk_h, mk, \cdot)\},&\\
\{R_{xx} \leftarrow KeyGen_{PRO}(sk_{ID_x}, sk_x, pk_x, mk, \cdot)\},&\\
\{R_{x\star} \leftarrow KeyGen_{PRO}(sk_{ID_x}, sk^\star, pk^\star, mk, \cdot)\},&\\
\{R_{h\star} \leftarrow KeyGen_{PRO}(sk_{ID_h}, sk^\star, pk^\star, mk, \cdot)\},&\\
(m_0, m_1, St) &\leftarrow A^{O_{renc}}(pk^\star, \{(pk_x, sk_x)\},\\
\{(ID_x, sk_{ID_x})\}, \{pk_h\}, \{ID_h\}, \{R_{xh}\},&\\
\{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\},&\\
\{R_{h\star}\}, \{R_{x\star}\}, \{master-key\}),&\\
d^\star \xleftarrow{R} \{0,1\}, C^\star = Enc_{CBE}(m_{d^\star}, pk^\star),&\\
d' \leftarrow A^{O_{renc}}(C^\star, St) : d' = d^\star]&
\end{aligned}$$

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

In PRE from IBE and CBE, the delegatee is a CBE user. We consider the first level CBE ciphertext [5]. In this case, we assume the proxy and PKG are colluding.

Definition 8: **(CBE-LV1-IND-CPA)** A PRE scheme from IBE to CBE is CBE-LV1-IND-CPA secure for CBE if the probability

$$\begin{aligned}
Pr[(parms, master-key) &\leftarrow Setup_{IBE}(\cdot),\\
\{(ID^\star, sk_{ID^\star}) &\leftarrow KeyGen_{IBE}(\cdot)\},\\
\{(pk^\star, sk^\star) &\leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(pk_x, sk_x) &\leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_x, sk_{ID_x}) &\leftarrow KeyGen_{IBE}(\cdot)\},\\
\{(pk_h, sk_h) &\leftarrow KeyGen_{CBE}(\cdot)\},\\
\{(ID_h, sk_{ID_h}) &\leftarrow KeyGen_{IBE}(\cdot)\},\\
\{R_{hx} \leftarrow KeyGen_{PRO}(sk_{ID_h}, sk_x, pk_x, mk, \cdot)\},&\\
\{R_{xh} \leftarrow KeyGen_{PRO}(sk_{ID_x}, sk_h, pk_h, mk, \cdot)\},&\\
\{R_{hh} \leftarrow KeyGen_{PRO}(sk_{ID_h}, sk_h, pk_h, mk, \cdot)\},&\\
\{R_{xx} \leftarrow KeyGen_{PRO}(sk_{ID_x}, sk_x, pk_x, mk, \cdot)\},&
\end{aligned}$$

[4] Second level ciphertext means the normal CBE ciphertext

[5] first level ciphertext means the re-encrypted CBE ciphertext

$$\{R_{x\star} \leftarrow KeyGen_{PRO}(sk_{ID_x}, sk^\star, pk^\star, mk, \cdot)\},$$
$$\{R_{h\star} \leftarrow KeyGen_{PRO}(sk_{ID_h}, sk^\star, pk^\star, mk, \cdot)\},$$
$$\{R_{\star x} \leftarrow KeyGen_{PRO}(sk_{ID^\star}, sk_x, pk_x, mk, \cdot)\},$$
$$\{R_{\star h} \leftarrow KeyGen_{PRO}(sk_{ID^\star}, sk_h, pk_h, mk, \cdot)\},$$
$$\{R_{\star\star} \leftarrow KeyGen_{PRO}(sk_{ID^\star}, sk^\star, pk^\star, mk, \cdot)\}$$
$$(m_0, m_1, St) \leftarrow A^{O_{renc}}(ID^\star, pk^\star\{(pk_x, sk_x)\},$$
$$\{(ID_x, sk_{ID_x})\}, \{pk_h\}, \{ID_h\}, \{R_{xh}\},$$
$$\{R_{hx}\}, \{R_{hh}\}, \{R_{xx}\}, \{R_{\star h}\}, \{R_{\star x}\},$$
$$\{R_{h\star}\}, \{R_{x\star}\}, \{R_{\star\star}\}, \{master - key\}),$$
$$d^\star \xleftarrow{R} \{0,1\}, C^\star = ReEnc(Enc_{IBE}(m_{d^\star}, ID^\star), pk^\star,$$
$$sk^\star, R_{\star\star}, parms), d' \leftarrow \mathcal{A}^{O_{renc}}(C^\star, St) : d' = d^\star]$$

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

PKG **Security.**

In PRE from IBE to CBE, PKG's $\mathsf{master-key}$ can not leverage even if the delegator, the delegatee and proxy collude. We denote this security property as **(PKG-OW)**.

V. A Hybrid PRE from IBE to CBE Scheme

The PRE scheme from IBE to CBE involves the ElGamal-type CBE scheme and the BB_1 IBE scheme.

- The underlying IBE scheme is the BB_1 scheme (the first scheme in [3].)
- The underlying CBE scheme (ElGamal-type CBE scheme):
  1) **KeyGen**$_{\mathsf{CBE}}(k, \mathsf{parms})$. Given a security parameter k , parms, pick a random $\theta \in Z_p^*, k \in Z_p^*$. Set $g_3 = {g_1}^\theta$. The public key is $pk = g_3$. The secret key is $sk = (d_0, d_1) = (\theta, k)$.
  2) **Enc**$_{\mathsf{CBE}}(\mathsf{pk}, \mathsf{parms}, M)$. Given $pk = g_3$ and a message M with parms, pick a random $r \in Z_p^*$ and compute $C_{pk} = (g_3^r, Me(g_1, g_2)^r)$.
  3) **Dec1**$_{\mathsf{CBE}}(sk, \mathsf{parms}, C_{pk})$. Given $C_{pk} = (C_1, C_2)$ and the secret key $sk = (d_0, d_1) = (\theta, k)$ with parms, compute $M = C_2/e(C_1^{1/d_0}, g_2)$.
  4) **Dec2**$_{\mathsf{CBE}}(sk, \mathsf{parms}, C_{pk})$. Given a re-encrypted ciphertext $\widehat{C_{pk}} = (\widehat{C_1}, \widehat{C_2})$ and the secret key $sk = (d_0, d_1) = (\theta, k)$ with parms, compute $M = \widehat{C_2}/e(\widehat{C_1}^{\frac{1}{d_0 d_1}}, g_2)$.
- The delegation scheme:
  1) **KeyGen**$_{PRO}(\mathsf{sk_{ID}}, \mathsf{sk}, \mathsf{pk}, \mathsf{mk}, \mathsf{parms})$. The PKG first chooses a collision resistent hash function $H : \{0,1\}^{3|p|} \rightarrow Z_p^*$ and a random seed $s_1, s_2 \in Z_p^*$, and computes $k_1 = H(ID, pk, s_1), k_2 = H(ID, pk, s_2)$. The PKG computes $(\frac{\alpha+k_1}{ID\alpha+t_2} \mod p, g_2^{k_1})$ and sends it to the proxy. The delegatee sends $k\theta$ to the proxy. The proxy sets the re-encryption key $rk_{\mathsf{ID}\rightarrow\mathsf{pk}} = (rk_1, rk_2) = (\frac{(\alpha+k_1)k\theta}{ID\alpha+t_2}, g_2^{k_1})$.
  2) **ReEnc**$(rk_{\mathsf{ID}\rightarrow\mathsf{pk}}, \mathsf{parms}, C_{ID}, pk)$. Given an IBE ciphertext $\widetilde{C_{ID}} = (\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3}) = (g^r, (g_1^{ID}h)^r, Me(g_1, g_2)^r)$ and re-encryption key $rk_{\mathsf{ID}\rightarrow\mathsf{pk}} = (rk_1, rk_2)$, the proxy re-encrypt the ciphertext $\widetilde{C_{ID}}$ into $\widehat{C_{pk}}$ as following. $\widehat{C_{pk}} = (\widehat{C_1}, \widehat{C_2}) = (\widetilde{C_2}^{rk_1}, \widetilde{C_3}e(\widetilde{C_1}, rk_2))$.
  3) **Check**$(\mathsf{parms}, \widetilde{C_{ID}})$. Given $\widetilde{C_{ID}} = (\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3})$ with parms, set $v_1 = e(\widetilde{C_1}, g_1^{ID}h)$, $v_2 = e(\widetilde{C_2}, g)$. If $v_1 = v_2$ then output "Valid", otherwise output "Invalid".

We can verify its correctness as the following

$$\widehat{C_2}/e(\widehat{C_1}^{\frac{1}{d_0 d_1}}, g_2) = \frac{Me(g_1, g_2)^r e(g^r, rk_2)}{e(((g_1^{ID}h)^{r\cdot\frac{\alpha+k_1}{ID\alpha+t_2}\cdot k\theta})^{\frac{1}{k\theta}}, g_2)} = M$$

Remark 6: In our scheme, we must note that the PKG needs to compute a different k_1 for every different user pair $(\mathsf{ID}, \mathsf{pk})$. Otherwise, if the adversary know $\frac{\alpha+k_1}{ID\alpha+t_2} \mod p$ for three different ID_1, ID_2, ID_3 but the same k_1 and pk, he can compute α, t_2, which is not secure at all.

Remark 7: In our scheme, $rk_1 = \frac{\alpha+k_1}{ID\alpha+t_2} \mod p$. One may wonder that every rk_1 for ID has a factor of form $\frac{1}{ID\alpha+t_2} \mod p$ which can help the adversary find $ID\alpha + t_2$. We comment that this attack can not succeed for this reason: when k_1 runs along $(1, 2, \cdots, p-1)$, $rk_1 = \frac{\alpha+k_1}{ID\alpha+t_2} \mod p$ distribute uniformly over Z_p^* and this means $rk_1 = \frac{\alpha+k_1}{ID\alpha+t_2} \mod p$ can not help adversary to find $ID\alpha + t_2$.

A. Security Analysis

Theorem 6: Suppose the mDBDH assumption holds, then our scheme is IBE-IND-sID-CPA secure for the proxy and delegatee's colluding.

Proof: We omit the proof here, interested readers can refer [12] to get the proof. ■

Theorem 7: Our scheme is CBE-LV2-IND-CPA and CBE-LV1-IND-CPA secure for the proxy, delegator and PKG's colluding.

Proof: We just give the intuition for this theorem. The security proof follows the principle of symmetrical encryption. The only information about CBE user's private key just relying on $k\theta$. But even if the proxy, delegator and PKG are colluding, they can only get $k\theta$ where k blinding the private key θ perfectly. Thus they can only guess θ. The adversaries' success probability is at most $1/p$ which is negligible, whether for CBE first level ciphertext or for CBE second level ciphertext. ■

Theorem 8: Suppose the mDBDH 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. When considering the proxy, delegatee and delegator colluding, the PKG only interact with delegator and proxy. The re-encryption key $rk = (\frac{(\alpha+k_1)k\theta}{ID\alpha+t_2}, g_2^{k_1})$ is distributed same as $(x, \frac{g_4^{(ID-ID^\star)x} g_1^{\alpha' x}}{g_4})$ where x is randomly choose from Z_p^*. That is to say, the adversaries can not get any information about α except randomly guessing. And we know the BB_1 identity based encryption is secure

TABLE I.
HYBRID PRE SECURITY COMPARISON

Scheme	Security		W/O RO	Assum	SecMod	Colluding	UnderlyIBE	Remark
M07A [10]	IND-Pr-ID-CPA		Std	DBDH	Sec.3.4 [10]	P or DGA or DGE	BB_1 IBE	Weak
OursAIII-A	DGA	CBE-IND-CPA CBE-ciph-no-re-encrypted	Std	DBDH	II-A	P and DGE and PKG	BB_1 IBE	Weak
OursAIII-A	DGA	No CBE-IND-CPA CBE-ciph-re-encrypted	␣	␣	II-A	P and DGE and PKG	BB_1 IBE	Weak
OursAIII-A	DGE	IBE-LV2-IND-sID-CPA	Std	DBDH	II-A	P and DGA	BB_1 IBE	Weak
OursAIII-A	DGE	IBE-LV1-IND-sID-CPA	Std	SymEnc-Sec	II-A	P and PKG and DGA	BB_1 IBE	Weak
OursAIII-A	PKG	PKG-OW	Std	DBDH	II-A	P and DGA and DGE	BB_1 IBE	Strong
OursBV	DGA	IBE-IND-sID-CPA	Std	mDBDH	IV-A	P and DGE	BB_1 IBE	Weak
OursBV	DGE	CBE-LV1-IND-CPA	Std	SymEnc-Sec	IV-A	P and DGA and PKG	BB_1 IBE	Weak
OursBV	DGE	CBE-LV2-IND-CPA	Std	SymEnc-Sec	IV-A	P and DGA and PKG	BB_1 IBE	Weak
OursBV	PKG	PKG-OW	Std	mDBDH	IV-A	P and DGA and DGE	BB_1 IBE	Strong

TABLE II.
HYBRID PRE EFFICIENCY COMPARISON

Scheme	Type	$\text{Enc}_{\mathsf{CBE}}$	$\text{Enc}_{\mathsf{IBE}}$	Check	Reenc	Dec		Ciph-Len		ReMal
						1stCiph	2-ndCiph	1stCiph	2-ndCiph	
M07A [10]	CBE $\rightarrow$ IBE	$3t_e + 1t_p$	$1t_p + 2t_e$	$4t_p$	$2t_e + 1t_p$	$2t_p$	$2t_p$	$2\|G_e\|+ 1\|G_T\|$	$2\|G_e\|+ 1\|G_T\|$	NO
OursA III-A	CBE $\rightarrow$ IBE	$3t_e + 1t_p$	$1t_p + 2t_e$	$4t_p$	$2t_e + 1t_p$	$4t_e+ 1t_p$	$2t_p$	$3\|G_e\|+ 1\|G_T\|$	$2\|G_e\|+ 1\|G_T\|$	YES
OursB V	IBE $\rightarrow$ CBE	$2t_e + 1t_p$	$1t_p + 1t_e$	$2t_p$	$1t_e + 1t_p$	$1t_e+ 1t_p$	$1t_e+ 1t_p$	$1\|G_e\|+ 1\|G_T\|$	$1\|G_e\|+ 1\|G_T\|$	␣

under DBDH assumption. That's imply the attacker can not recover the PKG's $\mathsf{master-key}$. Thus our scheme is PKG-OW secure for the proxy, delegatee and delegator's colluding. ■

VI. COMPARISON

In this section, we give our comparison results with other hybrid proxy re-encryption schemes [10]. We compare our schemes with other schemes from two ways. First we concern about schemes' security, then we concern about schemes' efficiency.

Notations: In 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, CBE-ciph-no-re-encrypted means CBE ciphertext having not been re-encrypted, CBE-ciph-re-encrypted means the CBE ciphertext having been re-encrypted

In II, we denote encryption as Enc, re-encryption as Reenc, decryption as Dec, ciphertext as Ciph and ciphertext length as Ciph-Len, resisting malicious PKG attack as ReMal. 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 $e : \mathbb{G}_e \times \mathbb{G}_e \rightarrow \mathbb{G}_T$. Finally, $|vk|$ and $|s|$ denote the bit length of the one-time signature's public key and a one-time signature respectively.

From I and II, we can know that the security models of our PRE from CBE to IBE and PRE from IBE to CBE schemes are stronger than the security model of M07A scheme. Thus our schemes are more secure than M07A scheme. We construct the first PRE from CBE to IBE which can resist malicious PKG attack. But we note that our scheme needs to add one more secret key k to the delegatee.

VII. CONCLUSIONS

In this paper, we extend Matsuo's research on hybrid PRE. We propose the concept of hybrid PRE from CBE to IBE without key escrow, we try to detail its threat model and construct such a concrete scheme. Also we fulfill the security model for hybrid PRE from IBE to CBE and construct the first such scheme by requiring PKG using his $\mathsf{master-key}$ in plain form for generating re-encryption key. But we note that both of our scheme can only achieve IND-ID-CPA or IND-CPA secure, it is an interesting future work to construct hybrid PRE with chosen ciphertext security. It is also an interesting work

to find more application for these schemes in emerging fields such as Personal Health Record protection.

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, S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *ACM Transaction on Information and System Security*, no. 1, pages 1–30, 2006.

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

[3] 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.

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

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

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

[7] C. Gentry. Certificate-based encryption and the certificate revocation problem. In *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 272–293, 2003.

[8] 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.

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

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

[11] J. Shao, D. Xing and Z. Cao. Identity-based proxy re-encryption schemes with multiuse, unidirection, and CCA security. Cryptology ePrint Archive: http://eprint.iacr.org/2008/103.

[12] X. A. Wang, X. Yang, M. Zhang. Proxy Re-encryption Scheme from IBE to CBE. In *Proceeding of International Workshop on Database Technology and Applications (DBTA 2009)*, IEEE Press, 99-102, 2009.

[13] K. Niu, X. A. Wang, M. Zhang. How to Solve Key Escrow Problem in Proxy Re-encryption from CBE to IBE. In *Proceeding of International Workshop on Database Technology and Applications (DBTA 2009)*, IEEE Press, 95-98, 2009.

[14] 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 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. His main research interests include cryptography and information hiding.