# New Identity Based Encryption And Its Proxy Re-encryption

Xu An Wang, Xiaoyuan Yang

*Key Laboratory of Information and Network Security*
*Engineering University of Chinese Armed Police Force, Xi'an, 710086, P.R. China*
wangxahq@yahoo.com.cn

**Abstract**

Identity based encryption (IBE) has received great attention since Boneh and Franklin's breakthrough work on bilinear group based IBE [4]. Till now, many IBE schemes relying on bilinear groups with different properties have been proposed [5, 25, 29, 14]. However, one part of the user's private key in all these IBE schemes is constructed as $y = f(msk)$, where $msk$ is the master key and $y$ is an element in the underlying bilinear group $\mathbb{G}$. In this paper, we propose a new IBE: one part of the private key is $y = f(msk)$, where $msk$ is the master key and $y$ is an element in $\mathcal{Z}_p^*$. Here $p$ is the underlying bilinear group's prime order. By using some novel techniques, we prove this new IBE is semantic secure under the selective identity chosen plaintext attacks (IND-sID-CPA) in the standard model. Based on this IBE scheme, we construct an IND-ID-CCA secure identity based proxy re-encryption (IBPRE) scheme which is master secret secure and efficient for the proxy compared with other IND-ID-CCA (IBPRE) schemes.

*Key words:* Identity based encryption, identity based proxy re-encryption, master secret secure, IND-ID-CCA secure.

## 1. Introduction

[1]In 1984, Shamir [26] introduced the concept of identity-based cryptography to ease the certificate management in traditional public key system. A user's public key in an IBE scheme is the identity information of the user

[1]This paper is a revised and extended vision of conference proceedings [32, 33].

(e.g., email address). Hence the public key is implicit authenticated and the certificate management is simplified. However, the first practical IBE scheme [4] was only proposed 17 years after its concept was proposed. Since then, many practical IBE schemes with different properties have been proposed [5, 25, 29, 14]. However, one part of the private key in all these IBE schemes is of the form: $y = f(msk)$ where $msk$ is the master key and $y$ is an element in the underlying bilinear group $\mathbb{G}$.

The concept of proxy re-encryption (PRE) is proposed by Blaze et al. [3] in 1998, which allows a semi-trusted proxy, with some information (a.k.a., the re-encryption key), to translate a ciphertext under the delegator's public key into another ciphertext can be decrypted by the delegatee's secret key. However, the proxy cannot access the plaintext. According to the direction of transformation, PRE schemes can be classified into bidirectional schemes and unidirectional schemes. Also according to the times the transformation can apply on the ciphertext, PRE schemes can be classified into single-hop schemes and multi-hop schemes. At NDSS'05, Ateniese et al. [1] proposed a few unidirectional PRE schemes and discussed its several potential applications such as distributed secure file systems. Later, many unidirectional PRE schemes with different properties have been proposed [17, 34, 28, 23, 10]. Due to the simpler certificate management in IBE, Green and Ateniese [13] extended PRE to the IBE setting, i.e. identity based proxy re-encryption (IBPRE). They also discussed its several interesting applications such as bridging IBE and PKE. Since then, several IBPRE schemes have been proposed [9, 20, 28, 22, 10], but none of them except [23, 10] can achieve master secret secure: the corrupted proxy and delegatee can not derive the delegator's private key. However, IBPRE schemes in [23] are generic constructions relying on CCA-secure 2-level hierarchical ID-based (2,2) threshold cryptosystem, they are inefficient. IBPRE schemes in [10] rely on conditional proxy broadcast re-encryption, they are also inefficient and can only achieve secure against replayable chosen ciphertext attacks (RCCA).

### *1.1. Our Contribution*

In this paper, we construct a new identity based encryption scheme. The main novelty of our IBE is that: one part of the private key is $y = f(msk)$, where $msk$ is the master key and $y$ is an element in $\mathcal{Z}_p^*$. Here $p$ is the underlying bilinear group's prime order. To resist the adversary to extract useful information on the master key from this part of the private key, we introduce some randomness in the private key. We prove this new IBE is IND-

sID-CPA secure in the standard model based on a related DBDH assumption in the bilinear groups.

We also construct an IBPRE scheme on this new IBE. This new IBPRE does not follow Green's paradigm on which almost all the existing efficient IBPRE schemes are based. The main novelty in this IBPRE is that, the re-encryption key is almost independent with the delegatee's private key. As a result, our IBPRE can achieve *master secret security*.

### *1.2. Related Work*

**Identity Based Encryption.** Here we just recall the IBE schemes closely related to our work. At Crypto'01, Boneh and Franklin constructed the first practical identity based encryption based on bilinear groups [4] (BF IBE). In 2003, Sakai and Kasahara proposed a new identity based encryption with different structure based on bilinear groups (SK IBE) [25]. However, both of these work prove their security in the random oracle model. At Eurocrypt'04, Boneh and Boyen proposed two new efficient selective identity secure IBE schemes without random oracles ($\mathsf{BB_1}$ IBE and $\mathsf{BB_2}$ IBE) [5]. Later Boneh and Boyen [6], Waters [29] improved their work on IBE schemes with full security at Crypto'04 and Eurocrypt'05 (Waters' IBE). At Eurocrypt'06, Gentry proposed an efficient identity based encryption with tight security proof in the standard model but based on a strong assumption (Gentry's IBE)[14].

All the existing IBEs can lie in three frameworks: "Full Domain Hash" framework, " Exponent Inversion" framework and "Communicative Blinding" framework [7]. "Full Domain Hash" framework includes BF IBE, which is proven secure in the random oracle and support hierarchies and threshold variants. " Exponent Inversion" framework includes SK IBE, $\mathsf{BB_2}$ IBE and Gentry's IBE, which are always difficult to support extensions. "Communicative Blinding" framework includes $\mathsf{BB_1}$ IBE and Waters' IBE, which always support extensions like hierarchy IBE, threshold IBE, fuzzy IBE, attribute based encryption and broadcast encryption.

**Identity Based Proxy Re-encryption.** In ACNS'07, Green and Ateniese proposed the first identity based proxy re-encryption schemes [13]. They defined the algorithms and security models for identity based proxy re-encryption, and constructed their scheme by using a variant of the efficient Dodis/Ivan key splitting approach to settings with a bilinear map. The re-encryption key in their scheme is of the form $(\mathsf{H_1(Alice)}^{-s} \cdot \mathsf{H(X)}, \mathsf{IBE}_{Bob}\mathsf{(X)})$. When the proxy re-encrypt, it does some transformations and sends $\mathsf{IBE}_{Bob}\mathsf{(X)}$ to the delegatee. And then the delegatee decrypt $\mathsf{IBE}_{Bob}\mathsf{(X)}$

to recover X and use this X to recover the original message. In ISC'07, Chu and Tzeng proposed the first IND-CCA2 secure proxy re-encryption in the standard model based on Waters' IBE [9]. They follow the paradigm proposed in [13] (We denote it as Green's paradigm). Unfortunately Shao et al. found their scheme can not achieve IND-CCA2 secure and they fixed this flaw by proposing an improved scheme [24]. However, both of these schemes are not efficient due to the structure of Waters' IBE and Green's paradigm. In Pairing'07, Matsuo proposed four types of proxy re-encryption: IBE to IBE, CBE to IBE, IBE to CBE and CBE to CBE. They constructed a hybrid proxy re-encryption scheme from CBE to IBE and a proxy re-encryption scheme from IBE to IBE. But recently it was shown their proxy re-encryption scheme from IBE to IBE has some flaws [31]. In Inscrypt'08, Tang et al. proposed the new concept of inter-domain identity based proxy re-encryption [28]. They concern on constructing proxy re-encryption between different domains in identity based setting. They follow Green's paradigm but based on Boneh-Frankin IBE. Their scheme can only achieve IND-sID-CPA secure. Later, Ibraimi et al. construct a type and identity based proxy re-encryption, which aimed at combing type and identity properties in one proxy re-encryption system [16]. Recently Lai et al. [18] gave new constructions on IBPRE based on identity-based mediated encryption. Luo et al. [19] also gave a new generic IBPRE construction based on IBE. Wang et al. proposed the first multi-use CCA-secure unidirectional IBPRE scheme [30].

### *1.3. Organization*

In Section 2, we give some preliminaries we will use later. In Section 3, we construct our new IBE scheme and prove its IND-sID-CPA security. In Section 4, we construct our new IBPRE, prove it to be IND-ID-CCA secure and master secret secure. In Section 5, we give our comparison results. Finally, we concludes our paper in the last Section.

## 2. Preliminaries

### *2.1. Bilinear Groups*

Let $\mathcal{G}$ be an algorithm called a group generator that takes as input a security parameter $\lambda$ and outputs a tuple $(G, G_T, e)$ where $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups of order $p$, and $e$ is a function $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ satisfying the following properties:

- (Bilinear) $\forall u, v \in \mathbb{G}, \forall a, b \in Z, e(u^a, v^b) = e(u, v)^{ab}$.
- (Non-degenerate) $\exists g \in \mathbb{G}$ such that $e(g, g)$ has order $p$ in $\mathbb{G}_T$.

We assume that the group action in $\mathbb{G}$ and $\mathbb{G}_T$ as well as the bilinear map $e$ are all computable in polynomial time in $\lambda$. Furthermore, we assume that the description of $\mathbb{G}$ and $\mathbb{G}_T$ includes a generator of $\mathbb{G}$ and $\mathbb{G}_T$ respectively.

*2.2. EXDBDH Assumption*

EXDBDH assumption extends the DBDH assumption in the prime order bilinear group.

**Definition1.** Run $\mathcal{G}$ to obtain $(\mathbb{G}, \mathbb{G}_T, e)$. Next it generates $g$ as generators of $\mathbb{G}$. On input $(g, g^a, g^b, g^c, g^{(b+c)d}, g^d, T)$, for any probabilistic polynomial time algorithm $\mathcal{A}$ cannot distinguish $T = e(g, g)^{abd}$ from a random element in $\mathbb{G}$ with non-negligible probability, this is the EXDBDH assumption.

We note that the assumption is a falsifiable assumption [21]. Intuitively, there is no $g^{ab}, g^{ad}, g^{bd}$, hence the pairing cannot help to solve the decisional problem.

*2.3. Definition and Security Notion for IBE*

*2.3.1. Definition*

An IBE scheme consists of the following algorithms.

1. **Setup**$(1^k)$. On input a security parameter, outputs both the master public parameters params which are distributed to users, and the master key $msk$ which is kept private.
2. **KeyGen**$(msk,$ params, $ID)$. On input an identity $ID \in \{0,1\}^*$ and the master secret key $msk$, outputs a decryption key $sk_{ID}$ corresponding to that identity.
3. **Encrypt**$(ID,$ params, $m)$. On input a set of public parameters, an identity $ID \in \{0,1\}^*$ and a plaintext $m \in M$, outputs $C_{ID}$, the encryption of $m$ under the specified identity.
4. **Decrypt**$(sk_{ID},$ params, $C_{ID})$. Decrypts the ciphertext $C_{ID}$ using the secret key $sk_{ID}$, and outputs $m$ or $\perp$.

*2.3.2. Security Notion.*

We recall the IND-sID-CPA security in [5]. It is defined using the following game:

1. **Init:** The adversary outputs an identity $ID^*$ where it wishes to be challenged.
2. **Setup:** The challenger runs the Setup algorithm. It gives the adversary the resulting system parameters params. It keeps the master key to itself.
3. **Phase1:** The adversary issues $q_1 \cdots q_m$ where $q_i$ is one of private key query $ID_i$ where $ID_i \neq ID^*$. The challenger responds by running algorithm KeyGen to generate the private key $d_i$ corresponding to the public key $ID_i$. It sends $d_i$ to the adversary. These queries maybe asked adaptively, that is, each query $q_i$ may depend on the replies to $q_1, \cdots, q_{i-1}$.
4. **Challenge:** Once the adversary decides that Phase1 is over it outputs two equal length plaintexts $M_0, M_1 \in \mathsf{M}$ on which it wishes to be challenged. The challenger picks a random bit $b \in \{0, 1\}$ and sets the challenge ciphertext to $\mathsf{C} = \mathsf{Encryption}(\mathsf{params}, \mathsf{ID}^*, \mathsf{M}_b)$. It sends $C$ as the challenge to the adversary.
5. **Phase2:** The adversary issues additional queries $q_{m+1} \cdots q_n$ where $q_i$ is one of private key queries $ID_i$ where $ID_i \neq ID^*$. The challenger responds as in Phase1. These queries maybe asked adaptively as in Phase1.
6. **Guess:** Finally, the adversary outputs a guess $b' \in \{0, 1\}$. The adversary wins if $b = b'$.

We refer to such an adversary $\mathcal{A}$ as an IND-sID-CPA adversary. We define the advantage of the adversary $\mathcal{A}$ in attacking the scheme $\mathcal{E}$ as $Adv_{\epsilon,Aa} = | Pr[b = b'] - \frac{1}{2} |$, The probability is over the random bits used by the challenger and the adversary. If this probability is negligible, then we say scheme $\mathcal{E}$ is IND-sID-CPA secure.

*2.4. Definition for IBPRE*

*2.4.1. Definition*

An identity based (single-hop) proxy re-encryption scheme consists of the algorithms **(Setup, KeyGen, Encrypt, Decrypt, ReKeygen, Reencrypt):**

1. **Setup($1^k$).** On input a security parameter, outputs both the master public parameters params which are distributed to users, and the master key $msk$ which is kept private.

2. **KeyGen(**params, $msk$, $ID$**).** On input an identity $ID \in \{0,1\}^*$ and the master secret key $msk$, outputs a decryption key $sk_{ID}$ corresponding to that identity.
3. **Encrypt(**params, $ID$, $m$**).** On input a set of public parameters, an identity $ID \in \{0,1\}^*$ and a plaintext $m \in M$, outputs the second level ciphertext $C_{ID}$, which can be re-encrypted by the proxy.
4. **ReKeygen(**params, $sk_{ID_1}$, $ID_2$**).** On input secret key $sk_{ID_1}$, and identities $ID_2 \in \{0,1\}^*$, the delegator non-interactively generates the re-encryption key $rk_{ID_1 \to ID_2}$ and outputs it.
5. **Reencrypt(**params, $rk_{ID_1 \to ID_2}$, $C_{ID_1}$**).** On input a second level ciphertext $C_{ID_1}$ under identity $ID_1$, and a re-encryption key $rk_{ID_1 \to ID_2}$, outputs a first level re-encrypted ciphertext $C_{ID_2}$ which can not be re-encrypted.
6. **Decrypt$_2$(**params, $sk_{ID}$, $C_{ID}$**).** On input a second level ciphertext $C_{ID}$ under identity $ID$ with secret key $sk_{ID}$, decrypts the ciphertext $C_{ID}$, and outputs $m$ or $\perp$.
7. **Decrypt$_1$(**params, $sk_{ID}$, $C_{ID}$**).** On input a first level re-encrypted ciphertext $C_{ID}$ under identity $ID$ with secret key $sk_{ID}$, decrypts the re-encrypted ciphertext $C_{ID}$, and outputs $m$ or $\perp$.

**Correctness:** Intuitively, an IBPRE is correct if the Decrypt algorithm always outputs the expected decryption of a properly generated ciphertext. Slightly more formally, let $c_{ID_1} \leftarrow Encrypt(params, ID_1, m)$ be a properly generated ciphertext, Then $\forall m \in \mathcal{M}, \forall ID_1, ID_2 \in \{0,1\}^*$, where $sk_{ID_1} = KeyGen(msk, ID_1)$, $sk_{ID_2} = KeyGen(msk, ID_2)$, $rk_{ID_1 \to ID_2} \leftarrow ReKeygen(params, sk_{ID_1}, ID_1, ID_2)$, the following propositions hold:

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

### *2.5. Security Notion for IBPRE*

#### *2.5.1. IND-ID-CCA Security for the Second Level Ciphertext.*

IND-ID-CCA Security for the second level ciphertext is defined according to the following game.

1. Setup. Run Setup($1^k$) to get (params, $msk$), and give params to $\mathcal{A}$.
2. Find phase. $\mathcal{A}$ makes the following queries. At the conclusion of this phase $\mathcal{A}$ will select $ID^* \in \{0,1\}^*$ and $(m_0, m_1) \in \mathcal{M}^2$.

(a) For $\mathcal{A}$'s queries to extract oracle $O_{extract}$ with $(extract, ID)$, return $sk_{ID}$ =KeyGen(params, $msk, ID$) to $\mathcal{A}$.

(b) For $\mathcal{A}$'s queries to re-encryption key extract oracle $O_{rkextract}$ with $(rkextract, ID_1, ID_2)$, where $ID_1 \neq ID_2$, return $rk_{ID_1 \to ID_2}$=ReKeygen (params, KeyGen(params, msk, $\mathsf{ID}_1$), $\mathsf{ID}_2$) to $\mathcal{A}$.

(c) For $\mathcal{A}$'s queries to re-encrypt oracle $O_{reencrypt}$ with $(reencrypt, ID_1, ID_2, C)$, derive a re-encryption key $rk_{ID_1 \to ID_2}$ = ReKeygen(params, KeyGen(params, msk, $\mathsf{ID}_1$), $\mathsf{ID}_2$), and return $C'$=Reencrypt(params, $rk_{ID_1 \to ID_2}, ID_1, ID_2, C$) to $\mathcal{A}$.

(d) For $\mathcal{A}$'s queries to the first level ciphertext decrypt oracle $O_{1decrypt}$ with $(decrypt, ID, C)$ where $C$ is a first level ciphertext, return $m$ = $\mathsf{Decrypt}_1$(params, KeyGen(params, msk, ID), C) to $\mathcal{A}$.

Note that $\mathcal{A}$ is not permitted to choose $ID^*$ such that trivial decryption is possible using keys extracted during this phase (e.g. , by using extracted re-encryption keys to translate from $ID^*$ to some identity for which $\mathcal{A}$ holds a decryption key). Also note that the second level ciphertext decrypt oracle $O_{2decrypt}$ is no use here, for any second level ciphertext can be first re-encrypted and then be queried to the $O_{1decrypt}$ to get the decryption result.

3. Choice and Challenge. When $\mathcal{A}$ presents $(choice, ID^*, m_0, m_1)$, choose $i \leftarrow_R \{0, 1\}$, compute $C^*$= Encrypt(params, $ID^*$, $m_i$) and give $C^*$ to $\mathcal{A}$.
4. Guess stage. $\mathcal{A}$ continues to make queries as in the find stage, with the following restrictions. Let $\mathcal{C} = (C^*, ID^*)$. For all $rk$ given to $\mathcal{A}$, let $\mathcal{C}'$ be the set of all possible values derived via calls to Reencrypt oracle, e.g. on successful execution of re-encrypt query $(reencrypt, ID^*, ID', C^*)$, let $C'$ be the result and add the pair $(C', ID')$ to the set $\mathcal{C}'$. We call $\mathcal{C} \cup \mathcal{C}'$) is the Derivative of $(C^*, ID^*)$.

   (a) $\mathcal{A}$ is not permitted to issue any query of the form $(decrypt, ID, C)$ to decrypt oracle $O_{1decrypt}$ or $O_{2decrypt}$ where $(C, ID) \in (\mathcal{C} \cap \mathcal{C}')$.

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

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

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

The outcome of the game is determined as follows: If $i' = i$ then $\mathcal{A}$ wins the game. Let $Adv = \mid Pr(i' = i) - 1/2 \mid$. If for all probabilistic polynomial time algorithms $\mathcal{A}$, $Adv \leq v(k)$, we say that the IBPRE scheme $\mathcal{S}$ is IND-ID-CCA secure for the second level ciphertext.

*2.5.2. IND-ID-CCA Security for the First Level Ciphertext.*

IND-ID-CCA Security for the first level ciphertext is defined according to the following game.

1. Setup. Run Setup($1^k$) to get (params, $msk$), and give params to $\mathcal{A}$.
2. Find phase. $\mathcal{A}$ makes the following queries. At the conclusion of this phase $\mathcal{A}$ will select $(ID^\star, ID^*) \in \{0,1\}^*$ and $(m_0, m_1) \in \mathcal{M}^2$.
   (a) For $\mathcal{A}$'s queries to extract oracle $O_{extract}$ with $(extract, ID)$, return $sk_{ID}$ =KeyGen(params, $msk$, $ID$) to $\mathcal{A}$.
   (b) For $\mathcal{A}$'s queries to re-encryption key extract oracle $O_{rkextract}$ with $(rkextract, ID_1, ID_2)$, where $ID_1 \neq ID_2$, return $rk_{ID_1 \to ID_2}$=ReKeygen (params, KeyGen(params, msk, $\mathsf{ID}_1$), $\mathsf{ID}_2$) to $\mathcal{A}$.
   (c) For $\mathcal{A}$'s queries to the first level ciphertext decrypt oracle $O_{1decrypt}$ with $(decrypt, ID, C)$, return $m$ = Decrypt$_1$(params, KeyGen(params, msk, ID), C) to $\mathcal{A}$.

   Note here that $\mathcal{A}$ is permitted to get all the extracted re-encryption keys including $ID^*$ to some identity for which $\mathcal{A}$ holds a decryption key. Also note here that the re-encrypt oracle and second level ciphertext decrypt oracle are useless, since the $\mathcal{A}$ knows all the re-encryption key, he can do all the re-encryption and transform the second level ciphertext to the first level ciphertext.
3. Choice and Challenge. When $\mathcal{A}$ presents $(choice, ID^\star, ID^*, m_0, m_1)$, choose $i \leftarrow_R \{0,1\}$, compute $C^\star$= Encrypt(params, $ID^*$, $m_i$) and $C^*$=Reencrypt (params, $rk_{ID^* \to ID^\star}$, $ID^\star$, $ID^*$, $C^\star$) give $C^\star$ to $\mathcal{A}$.
4. Guess stage. $\mathcal{A}$ continues to make queries as in the find stage, with the following restrictions.
   (a) $\mathcal{A}$ is not permitted to issue any query of the form $(decrypt, ID^*, C^*)$ to decrypt oracle $O_{1decrypt}$ or $(decrypt, ID^\star, C^\star)$ to $O_{2decrypt}$. Note here that $C^\star$ maybe can be derived from $C^*$.
   (b) $\mathcal{A}$ is not permitted to issue any queries $(extract, ID^\star)$ or $(extract, ID^*)$ to extract oracle $O_{extract}$.

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

The outcome of the game is determined as follows: If $i' = i$ then $\mathcal{A}$ wins the game. Let $Adv = \mid Pr(i' = i) - 1/2 \mid$. If for all probabilistic polynomial time algorithms $\mathcal{A}$, $Adv \leq v(k)$, we say that the IBPRE scheme $\mathcal{S}$ is IND-ID-CCA secure for the first level ciphertext.

**Remark1.** In this security notion, we give two target identities $(ID^*, ID^\star)$ for our re-encryption not randomizing the second level ciphertext. From the the re-encrypted first level ciphertext, anyone can trivially derive its second level ciphertext.

*2.5.3. Master Secret Security.*

We extend Libert and Vergnaud's definition on master secret security of PRE[17], to IBPRE. This notion demands that no coalition of dishonest delegatees be able to pool their re-encryption keys in order to expose the private key of their common delegator. More formally, the following probability should be negligible as a function of the security parameter $\lambda$[2],

$$Pr[sk_{ID^\star} \leftarrow O_{extract}(ID^\star), sk_{ID_x} \leftarrow O_{extract}(ID_x)\},$$
$$\{R_{ID^\star \to ID_x} \leftarrow O_{rkextract}(ID^\star, ID_x)\}, \{R_{ID_x \to ID^\star} \leftarrow O_{rkextract}(ID_x, ID^\star)\},$$
$$\gamma \leftarrow \mathcal{A}(ID^\star, \{ID_x, sk_{ID_x}\}, \{R_{ID^\star \to ID_x}\}, \{R_{ID_x \to ID^\star}\}) : \gamma = sk_{ID^\star}]$$

## 3. New Identity Based Encryption

*3.1. Our Construction*

1. **Setup**$(\mathbf{1^k})$. Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, \mathbb{G}_T, e)$. Next it generates $g$ as generators of bilinear group of $\mathbb{G}$ with order $p$. For now, we assume public keys $(ID)$ are elements in $\mathcal{Z}_p^*$. We also assume messages to be encrypted are elements in $\mathbb{G}_T$. Select random $t_1, t_2, t_3 \in \mathcal{Z}_p^*$, let $g_2 = g^{t_1}, g_3 = g^{t_3}, h = g^{t_2}$. Pick a random $\alpha \in \mathcal{Z}_p^*$, set $g_1 = g^\alpha$, that is,

$$params = (g, g_1, g_2, g_3, h, p, \mathbb{G}, \mathbb{G}_T, e), msk = (\alpha, t_1, t_2, t_3)$$

2. **KeyGen**$(\mathbf{msk}, \mathbf{params}, \mathbf{ID})$. Given $msk = (\alpha, t_1, t_2, t_3)$ and $ID$ with $params$, the PKG picks random $x, y, n \in \mathcal{Z}_p^*$ and sets

$$d_{ID} = (d_1, d_2, d_3, d_4) = (\frac{\alpha + x}{\alpha ID + t_2} + y \bmod p, \quad g^x (g_1^{ID} h)^y, \quad g_3^x (g_1^{ID} h)^{-n}, \quad g_3^y g^n)$$

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

3. **Encrypt**$(\mathbf{ID}, \mathbf{params}, \mathbf{M})$. To encrypt a message $M \in \mathbb{G}_T$ under the public key $ID \in \mathcal{Z}_p^*$, pick a random $r \in \mathcal{Z}_p^*$ and compute

$$C_{ID} = (C_1, C_2, C_3, C_4) = (g^r, (g_2 g_3)^r, (g_1^{ID} h)^r, Me(g_1, g_2)^r)$$

4. **Decrypt**$(\mathbf{sk_{ID}}, \mathbf{params}, \mathbf{C_{ID}})$. Given ciphertext $C_{ID} = (C_1, C_2, C_3, C_4)$ and the secret key $d_{ID} = (d_1, d_2, d_3)$ with $params$, compute

$$M = \frac{C_4 e(C_2, d_2)}{e(g_2, C_3^{d_1}) e(C_1, d_3) e(C_3, d_4)}$$

**Correctness:**

$$\begin{aligned} M' &= \frac{C_4 e(C_2, d_2)}{e(g_2, C_3^{d_1}) e(C_1, d_3) e(C_3, d_4)} = \frac{Me(g_1, g_2)^r e((g_2 g_3)^r, g^x (g_1^{ID} h)^y)}{e(g_2, ((g_1^{ID} h)^r)^{(\frac{\alpha+x}{\alpha ID + t_2} + y)}) e(g^r, g^{t_3 x} (g_1^{ID} h)^{-n}) e((g_1^{ID} h)^r, g^{t_3 y} g^n)} \\ &= \frac{Me(g_1, g_2)^r e((g_2 g_3)^r, g^x (g_1^{ID} h)^y)}{e(g_2, ((g_1^{ID} h)^r)^y) e(g_2, g^{xr}) e(g_2, g_1^r) e(g_3^r, g^x (g_1^{ID} h)^y)} = \frac{Me(g_1, g_2)^r e(g_2, (g^x (g_1^{ID} h)^y)^r)}{e(g_2, ((g_1^{ID} h)^r)^y) e(g_2, g^{xr}) e(g_2, g_1^r)} \\ &= \frac{Me(g_1, g_2)^r e(g_2, ((g_1^{ID} h)^y)^r)}{e(g_2, ((g_1^{ID} h)^r)^y) e(g_2, g_1^r)} = \frac{Me(g_1, g_2)^r}{e(g_2, g_1^r)} = M \end{aligned}$$

*3.2. Security Analysis*

**Theorem 1.** *Suppose the EXDBDH assumption holds in* $(\mathbb{G}, \mathbb{G}_T, e)$*, then our proposed* IBE *is* IND-sID-CPA *secure.*

Proof. Suppose $\mathcal{A}$ can attack our scheme, we construct an algorithm $\mathcal{B}$ solves the EXDBDH problem in $(\mathbb{G}, \mathbb{G}_T, e)$. On input $(g, g^a, g^b, g^c, g^{(b+c)d}, g^d, T)$, algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g, g)^{abd}$ and 0 otherwise. Let $g_1 = g^a, g_2 = g^b, g_3 = g^c$, that is, $t_1 = a, t_2 = b, t_3 = c$. 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 $\alpha' \in \mathcal{Z}_p^*$ at random and defines $h = g_1^{-ID^*} g^{\alpha'} \in \mathbb{G}$. It gives $\mathcal{A}$ the parameters $params = (g, g_1, g_2, g_3, h)$. Note that the corresponding master key, which is unknown to $\mathcal{B}$, is $a$.

3. **Phase 1**. $\mathcal{A}$ issues up to private key query on $ID$. $\mathcal{B}$ returns

$$\begin{aligned} d_1^{sim} &= \frac{1}{(ID - ID^*)} + y \bmod p = \frac{a+x}{aID - aID^* + \alpha'} + y \bmod p \\ &= \frac{a+x}{aID + t_2} + y \bmod p \\ d_2^{sim} &= (g)^{(\frac{\alpha'}{ID-ID^*})}(g^a)^{y(ID-ID^*)}(g)^y = g^x(g^{a(ID-ID^*)}g)^y = g^x(g_1^{ID}h)^y \\ d_3^{sim} &= (g^c)^{(\frac{\alpha'}{ID-ID^*})}((g^a)^{ID-ID^*}g^{\alpha'})^{-n} = g^{cx}(g_1^{ID}h)^{-n} = g_3^x(g_1^{ID}h)^{-n} \\ d_4^{sim} &= (g^c)^y g^n = g_3^y g^n \end{aligned}$$

   where $x = \frac{\alpha'}{ID-ID^*} \bmod p$ and $y, n$ randomly chosen from $\mathcal{Z}_p^*$. We can verify $(d_1^{sim}, \cdots, d_4^{sim})$ is a valid private key for $ID$.
4. **Challenge**. When $\mathcal{A}$ decides that Phase 1 is over, it outputs two messages $M_0, M_1 \in \mathbb{G}$. Algorithm $\mathcal{B}$ picks a random bit $b$ and responds with the ciphertext $C = (g^d, g^{(b+c)d}, (g^{\alpha\prime})^d, M_b \cdot T)$. Hence if $T = e(g,g)^{abd}$, then $C$ is a valid encryption of $M_b$ under $ID^*$. Otherwise, $C$ is independent of $b$ in the adversary's view.
5. **Phase 2**. $\mathcal{A}$ issues private key query on $ID_i$ as he does in Phase 1 except $ID_i = ID^*$.
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 $T = e(g,g)^{abd}$. Otherwise it outputs 0 meaning $T \neq e(g,g)^{abd}$.

When $T = e(g,g)^{abd}$ then $\mathcal{A}$'s advantage for breaking the scheme is the same as $\mathcal{B}$'s advantage for solving EXDBDH problem.

## 4. New Identity Based Proxy Re-encryption

### *4.1. Our Construction*

1. **Setup**($\mathbf{1^k}$). Run $\mathbb{G}(1^n)$ to obtain $(\mathbb{G}, \mathbb{G}_T, e)$ with $\mathbb{G}$. Next it generates $g$ as generators of $\mathbb{G}$. It chooses a one time signature scheme $\mathcal{S}$ and an IND-CCA2 symmetric encryption SE. It also chooses three hash functions $G : \{0,1\}^* \to \mathcal{Z}_p^*$[3], $H_1 : \mathbb{S} \to \mathbb{G}$ where $\mathbb{S}$ is the one time signature scheme's public key $svk$'s space, $H_2 : G_T \to \mathcal{K}$ where $\mathcal{K}$ is the SE's key space. We also assume messages to be encrypted are elements in $\mathbb{G}_T$.

[3] $G$ maps the identity to $\mathcal{Z}_p^*$ which can be used to identify different IBE users.

Select random $\alpha, t_1, t_2, t_3$ and compute $(g_1, g_2, g_3, h)$ as the same as those in our $\mathsf{IBE}$ scheme, select random $s, s' \in \mathcal{Z}_p$ and compute $A = g^s$, that is

$$\begin{aligned} params &= (g, g_1, g_2, g_3, h, A, p, \mathbb{G}, \mathbb{G}_T, e, H, H_1, H_2, G, \mathsf{SE}, \mathcal{S}), \\ msk &= (\alpha, s, s', t_1, t_2, t_3) \end{aligned}$$

2. **KeyGen**$(\mathbf{msk}, \mathbf{params}, \mathbf{ID})$. Given $msk = (\alpha, t_1, t_2, t_3)$ and $ID$ with $params$, the PKG picks random $x, y, x', y', N, n, n', z \in \mathcal{Z}_p^*$, computes $u_{ID} = sG(ID)$ and outputs the private key $sk_{ID}$ associated with $ID$

$$\begin{aligned} sk_{ID} &= (d^A_{ID}, d^B_{ID}, d^C_{ID}) \\ d^A_{ID} &= (d_1, d_2, d_3, d_4, d_5, d_6) \\ &= (\frac{\alpha + x}{\alpha ID + t_2} + y \bmod p, g^x (g_1^{ID} h)^y, g_3^x (g_1^{ID} h)^{-N}, g_3^y g^N, A^y g^n, A^x (g_1^{ID} h)^{-n}) \\ d^B_{ID} &= (d'_1, d'_2, d'_3) = (\frac{t_2 + x'}{\alpha ID + t_2} + y' \bmod p, A^{y'} g^{n'}, A^{x'} (g_1^{ID} h)^{-n'} g^{s'}) \\ d^C_{ID} &= (d_7, d_8) = (g_2^{\alpha} (g_1^{ID} h)^{u_{ID}} g^{zG(ID)}, g^{zG(ID)} g^{s'G(ID)}) \end{aligned}$$

3. **Encrypt**$(\mathbf{ID}, \mathbf{params}, \mathbf{M})$. To encrypt a message $M \in \mathbb{G}_T$ under the public key $ID \in \mathcal{Z}_p^*$, pick a random $r \in \mathcal{Z}_p^*$, a one time signature instance with public/private keys $(svk, ssk)$, compute

$$\begin{aligned} C_{ID} &= (C_1, C_2, C_3, C_4, C_5, C_6, C_7) \\ &= (g^r, (g_2 g_3)^r, (g_1^{ID} h)^r, \mathtt{SE.Enc}(H_2(e(g_1, g_2)^r), M), H_1(svk)^r, svk, \sigma) \end{aligned}$$

where $\sigma = \mathcal{S}.\mathtt{sig}(ssk, C_1, C_2, C_3, C_4, C_5, C_6)$.

4. **ReKeygen**$(\mathbf{d_{ID}}, \mathbf{params}, \mathbf{ID'})$. Choose randomly $k_3 \in \mathcal{Z}_p^*$, generate

the re-encryption key $rk_{ID\to ID'}$ as following

$$\begin{aligned}
rk_{ID\to ID'} &= (rk_1, rk_2, rk_3, rk_4)\\
rk_1 &= \frac{1}{k_3}(d_1 \cdot ID' + d_1') \bmod p\\
&= \frac{1}{k_3}(\frac{(\alpha ID' + xID' + t_2 + x')}{\alpha ID + t_2} + yID' + y') \bmod p\\
&= \frac{(\alpha ID' + t_2 + k_1)}{k_3(\alpha ID + t_2)} + k_2 \bmod p\\
rk_2 &= A^{k_3 \cdot G(ID')} = g^{k_3 \cdot s \cdot G(ID')} = g^{k_3 u_{ID'}}\\
rk_3 &= (d_5^{ID'} d_2')^{G(ID')} = g^{(s\cdot(yID'+y')+(nID'+n'))\cdot G(ID')}\\
&= g^{s\cdot(yID'+y')\cdot G(ID')} g^{(nID'+n')G(ID')} = g^{k_2 k_3 u_{ID'}} g^{(nID'+n')G(ID')}\\
rk_4 &= (d_6^{ID'} d_3')^{G(ID')} = \frac{g^{s\cdot(xID'+x')\cdot G(ID')} g^{s' G(ID')}}{(g_1^{ID} h)^{(nID'+n')G(ID')}}
\end{aligned}$$

where

$$k_1 = xID' + x', \quad k_2 = \frac{yID' + y'}{k_3}$$

5. **Reencrypt**$(\mathbf{rk_{ID\to ID'}}, \mathbf{params}, \mathbf{C_{ID}}, \mathbf{ID'})$. Given ciphertext $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6, C_7)$, first check $C_{ID}$'s validity:

$$\mathcal{S}.\texttt{Verify}(C_6, C_7) = \texttt{Yes}, \quad e(g, C_5) = e(C_1, H_1(C_6))$$

if these conditions are not satisfied, then return $\perp$, else compute

$$\widehat{C_{ID'}} = (C_1', C_2', C_3', C_4', C_5', C_6', C_7')_{ID'} = (C_1, C_2, C_3, C_4, e(C_3^{rk_1}, rk_2), rk_3, rk_4)$$

6. **Deccrypt$_2$**$(\mathbf{sk_{ID}}, \mathbf{params}, \mathbf{C_{ID}})$. Given ciphertext $C_{ID} = (C_1, C_2, C_3, C_4, C_5, C_6, C_7)$ and the secret key $sk_{ID} = (d_{ID}^A, d_{ID}^B, d_{ID}^C)$ where $d_{ID}^A = (d_1, d_2, d_3)$ with $params$, first check $C_{ID}$'s validity:

$$\mathcal{S}.\texttt{Verify}(C_6, C_7) = \texttt{Yes}, \quad e(g, C_5) = e(C_1, H_1(C_6))$$

if these conditions can not be satisfied, then return $\perp$, else compute

$$K = H_2(\frac{e(g_2, C_3^{d_1}) e(C_1, d_3) e(C_3, d_4)}{e(C_2, d_2)}), \quad M = \texttt{SE.Dec}(K, C_4) \qquad (1)$$

and finally check $M$'s validity by using SE's IND-CCA2 property.

7. $\mathbf{Deccrypt_1}(\mathbf{sk_{ID}}, \mathbf{params}, \widehat{\mathbf{C_{ID}}})$. Given the re-encrypted ciphertext $\widehat{C_{ID}} = (C'_1, C'_2, C'_3, C'_4, C'_5, C'_6, C'_7)_{ID}$ with $d^C_{ID} = (d_7, d_8)$ with *params*, decrypt the re-encrypted ciphertext as

$$K = H_2(\frac{e(C'_3, C'_6)e(C'_1, C'_7)e(C'_1, d_7)}{C'_5 e(C'_2, d_8)}), \quad M = \mathtt{SE.Dec}(K, C'_3)$$

and finally check $M$'s validity by using SE's IND-CCA2 property.

**Correctness:** Assume the re-encrypted ciphertext is $\widehat{C_{ID}} = (C'_1, C'_2, C'_3, C'_4, C'_5, C'_6, C'_7)_{ID}$, which results from re-encrypting from $ID_x$ to $ID$ by using $rk_{ID_x \to ID}$. We can verify the correctness of $\mathsf{Deccrypt_1}(\mathsf{sk_{ID}}, \mathsf{params}, \widehat{\mathsf{C_{ID}}})$ as following

$$\begin{aligned}
T &= \frac{e(C'_3, C'_6)e(C'_1, C'_7)e(C'_1, d_7)}{C'_5 e(C'_2, d_8)} = \frac{e(C'_3, rk_3)e(C'_1, rk_4)e(C'_1, d_7)}{C'_5 e(C'_2, d_8)} \\
&= \frac{e((g_1^{ID_x}h)^r, g^{u_{ID}k_2k_3}g^{(nID+n')G(ID)})e(g^r, \frac{g^{k_1 u_{ID} g^{s'G(ID')}}}{(g_1^{ID_x}h)^{(nID+n')G(ID)}})e(g^r, g_2^\alpha (g_1^{ID}h)^{u_{ID}} g^{zG(ID)})}{e(g^{k_3 u_{ID}}, (g_1^{ID_x}h)^{r(\frac{\alpha ID + t_2 + k_1}{k_3(\alpha ID_x + t_2)} + k_2)})e(g^r, (g^z g^{s'})^{G(ID)})} \\
&= \frac{e((g_1^{ID_x}h)^r, g^{u_{ID}k_2k_3}g^{(nID+n')G(ID)})e(g^r, g^{k_1 u_{ID}})e(g^r, g^{s'G(ID)})e(g^r, g_2^\alpha (g_1^{ID}h)^{u_{ID}} g^{zG(ID)})}{e(g^r, (g_1^{ID_x}h)^{(nID+n')G(ID)})e(g^{k_3 u_{ID}}, (g_1^{ID_x}h)^{r(\frac{\alpha ID + t_2 + k_1}{k_3(\alpha ID_x + t_2)} + k_2)})e(g^r, g^{zG(ID)})e(g^r, g^{s'G(ID)})} \\
&= \frac{e((g_1^{ID_x}h)^r, g^{u_{ID}k_2k_3})e(g^r, g^{k_1 u_{ID}})e(g_2^\alpha (g_1^{ID}h)^{u_{ID}}, g^r)e(g^{zG(ID)}, g^r)}{e(g^{k_3 u_{ID}}, (g_1^{ID_x}h)^{k_2 r})e(g^{k_3 u_{ID}}, (g_1^{ID}h)^{\frac{r}{k_3}})e(g^{k_3 u_{ID}}, g^{\frac{k_1 r}{k_3}})e(g^r, g^{zG(ID)})} = e(g_2^\alpha, g^r) \\
K &= H_2(T), \quad M = \mathtt{SE.Dec}(K, C'_3)
\end{aligned}$$

*4.2. Security Analysis*

**Theorem 2.** *Suppose the EXDBDH assumption holds in* $(\mathbb{G}, \mathbb{G}_T, e)$, SE *is* IND-CCA2 *secure and* $\mathcal{S}$ *is strongly unforgeable, then our* IBPRE *scheme is* IND-sID-CCA2 *secure for the second level ciphertext.*

Proof. Suppose $\mathcal{A}$ can attack our scheme, we construct an algorithm $\mathcal{B}$ (or simulator $\mathcal{B}$) solves the EXDBDH problem in $(\mathbb{G}, \mathbb{G}_T, e)$.

Before describing $\mathcal{B}$, we first define an event $F_{OTS}$ and bound its probability to occur. Let $C^* = (C^*_1, C^*_2, C^*_3, C^*_4, C^*_5, svk^*, \sigma^*)$ denote the challenge ciphertext given to $\mathcal{A}$ in the game. Let $F_{OTS}$ be the event that, $\mathcal{A}$ issues a decryption query for a re-encryption query $C^* = (C_1, C_2, C_3, C_4, C_5, svk^*, \sigma)$ where $(C_1, C_2, C_3, C_4, C_5) = (C^*_1, C^*_2, C^*_3, C^*_4, C^*_5)$ but $\sigma \neq \sigma^*$ and $\mathcal{S}.\mathtt{Verify}(\sigma, svk^*, (C_1, C_2, C_3, C_4, C_5)) = \mathtt{Yes}$. In the "find" stage, $\mathcal{A}$ has simply no information on $svk^*$ . Hence, the probability of a pre-challenge occurrence of F does not exceed $q_O \cdot \delta$ if $q_O$ is the overall number of oracle queries and $\delta$

denotes the maximal probability (which by assumption does not exceed $1/p$) that any one-time verification key $svk$ is output by $\mathcal{S}$. In the "guess" stage $F_{OTS}$ clearly gives rise to an algorithm breaking the strong unforgeability of the one-time signature. Therefore, the probability $Pr[F_{OTS}] \leq \frac{q_O}{p} + Adv^{OTS}$[4] must be negligible by assumption.

On input $(g, g^a, g^b, g^c, g^{(b+c)d}, g^d, T)$, algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g,g)^{abd}$ and 0 otherwise. Let $g_1 = g^a, g_2 = g^b, g_3 = g^c$, that is, $t_1 = a, t_2 = b, t_3 = c$. It chooses a one time signature scheme $\mathcal{S}$ and an IND-CCA2 symmetric encryption SE. It also chooses $H, H_1, H_2, G$ as in the scheme. $\mathcal{B}$ 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 $\alpha' \in \mathcal{Z}_p^*$ at random and defines $h = g_1^{-ID^*} g^{\alpha'} \in \mathbb{G}$. It also picks random $w, r, s' \in \mathcal{Z}_p^*$, defines $s = r - bw$ and $A = g^s = g^{r-bw} = \frac{g^r}{g_2^w}$. It gives $\mathcal{A}$ the parameters $params = (g, g_1, g_2, g_3, h, A, H, H_1, H_2, G, \mathsf{SE}, \mathcal{S})$. Note that the corresponding master key, which is unknown to $\mathcal{B}$, is $a$.
3. **Phase 1**.
   (a) *$\mathcal{A}$ issues private key query on $ID$ to $O_{extract}$.* $\mathcal{B}$ returns

$$
\begin{aligned}
d_1^{sim} &= \frac{1}{(ID - ID^*)} + y \bmod p = \frac{a+x}{aID - aID^* + \alpha'} + y \bmod p \\
&= \frac{a+x}{aID + t_2} + y \bmod p \\
d_2^{sim} &= (g)^{(\frac{\alpha'}{ID - ID^*})} (g^a)^{y(ID-ID^*)} (g)^y = g^x (g^{a(ID-ID^*)} g)^y = g^x (g_1^{ID} h)^y \\
d_3^{sim} &= (g^c)^{(\frac{\alpha'}{ID-ID^*})} ((g^a)^{ID-ID^*} g^{\alpha'})^{-N} = g^{cx} (g_1^{ID} h)^{-N} = g_3^x (g_1^{ID} h)^{-N} \\
d_4^{sim} &= (g^c)^y g^N = g_3^y g^N \\
d_5^{sim} &= A^y g^n, \quad d_6^{sim} = A^{\frac{\alpha'}{ID-ID^*}} g^{\alpha'})^{-n} ((g^a)^{ID-ID^*} g^{\alpha'})^{-n} = A^x (g_1^{ID} h)^{-n} \\
d_1'^{sim} &= \frac{-ID^*}{(ID - ID^*)} + y' \bmod p = \frac{a(-ID^*) + \alpha' + aID + x'}{aID + \alpha' - aID^*} + y' \bmod p \\
d_2'^{sim} &= A^{y'} g^{n'}, \quad d_3'^{sim} = A^{\frac{(-ID^*)\alpha'}{ID-ID^*} - \alpha'} ((g^a)^{ID-ID^*} g^{\alpha'})^{-n'} g^{s'} = A^{x'} (g_1^{ID} h)^{-n'} g^{s'}
\end{aligned}
$$

[4] $Adv^{OTS}$ denotes the probability of breaking strong unforgeability of the one-time signature.

$$
\begin{aligned}
d_7^{sim} &= (g^b)^{-\alpha' wG(ID)}((g^a)^{(ID-ID^*)}g^{\alpha'})^{rG(ID)}g^{z'G(ID)} \\
&= g_2^{-\alpha' wG(ID)}(g_1^{(ID-ID^*)}g^{\alpha'})^{rG(ID)}g^{z'G(ID)} \\
&= g_2^{a(ID-ID^*)wG(ID)}(g_1^{(ID-ID^*)}g^{\alpha'})^{(r-bw)G(ID)}g^{z'G(ID)} \\
&= g_2^{a}(g_1^{(ID-ID^*)}g^{\alpha'})^{(r-bw)G(ID)}g^{a(ID-ID^*)wG(ID)-a+z'G(ID)} \\
&= g_2^{a}(g_1^{ID}h)^{sG(ID)}g^{a(ID-ID^*)wG(ID)-a+z'G(ID)} = g_2^{a}(g_1^{ID}h)^{sG(ID)}g^{zG(ID)} \\
d_8^{sim} &= (g^a)^{((ID-ID^*)wG(ID)-1)}g^{z'G(ID)}g^{s'G(ID)} \\
&= g^{a(ID-ID^*)wG(ID)-a+z'G(ID)}g^{s'G(ID)} = g^{zG(ID)}g^{s'G(ID)}
\end{aligned}
$$

where $x = \frac{\alpha'}{ID-ID^*} \bmod p, x' = \frac{(-ID^*)\alpha'}{ID-ID^*} - \alpha' \bmod p$, $y, y', N, n, n', z'$ randomly chosen from $\mathcal{Z}_p^*$, and $z = a(ID - ID^*)w - \frac{a}{G(ID)} + z'$ holds. We can verify $(d_1^{sim}, d_2^{sim}, \cdots, d_8^{sim})$ is a valid private key for $ID$. We call this simulation as "Normal Simulation".

(b) *$\mathcal{A}$ issues rekey generation queries on $(ID, ID')$ to re-encryption key extract oracle $O_{rkextract}$.*

i. $ID \neq ID^*$, in this case, $ID'$ can be any identity. The simulator $\mathcal{B}$ first simulates $\mathsf{KeyGen}(msk, params, ID)$ as above and gets $sk_{ID}$. Then it runs $\mathsf{ReKeygen}(sk_{ID}, params, ID')$, and returns the result $rk_{ID\to ID'}$ to the adversary.

ii. $ID = ID^*$, in this case, $ID'$ can not be a corrupted identity. The simulator $\mathcal{B}$ uses some other technique to generate the re-encryption key. The simulator can generate the valid re-encryption key as following

$$
\begin{aligned}
d_1^{sim} &= \frac{k}{\alpha'} + y \bmod pn = \frac{a + k - a}{aID^* + \alpha' - aID^*} + y \bmod p \\
d_2^{sim} &= \frac{g^k}{(g^a)}g^{\alpha' y} = g^{k-a}(g^{\alpha'})^y = g^x(g_1^{ID^*}h)^y \\
d_3^{sim} &= \frac{(g^c)^k}{g^{ac}}(g^c)^{\alpha' y} = g^{c(k-a)}(g^c)^{\alpha' y} = g^{t_3(k-a)}(g^{\alpha'})^{t_3 y} = g^{t_3 x}(g_1^{ID^*}h)^{t_3 y} \\
d_4^{sim} &= A^y g^n, \quad d_5^{sim} = A^{k-a}(g_1^{ID^*-ID^*}g^{\alpha'})^{-n} = A^x(g_1^{ID^*-ID^*}g^{\alpha'})^{-n} \\
d_1'^{sim} &= \frac{\alpha' + k'}{\alpha'} + y' \bmod p = \frac{a(-ID^*) + \alpha' + aID^* + k'}{aID^* + \alpha' - aID^*} + y' \bmod p \\
d_2'^{sim} &= A^{y'}g^{n'}, \quad d_3'^{sim} = A^{aID^*+k'}g^{m'}(g_2g_3)^{s'} = A^{x'}g^{m'}(g_2g_3)^{s'} \\
d_4'^{sim} &= (g_1^{ID^*-ID^*}g^{\alpha'})^{n'}g^{m'} = (g^{\alpha'})^{n'}g^{m'}
\end{aligned}
$$

$$
\begin{aligned}
d_7^{sim} &= (g^b)^{-\alpha' wG(ID^*)}((g^a)^{(ID^*-ID^*)}g^{\alpha'})^{rG(ID^*)}(g^b)^{z'G(ID^*)} \\
&\quad \cdot (g^{ac})^{((ID^*-ID^*)wG(ID^*)-1)}(g^c)^{z'G(ID^*)} \\
&= g_2^a(g_1^{ID^*}h)^{sG(ID^*)}(g_2g_3)^{-a+z'G(ID^*)} = g_2^a(g_1^{ID^*}h)^{sG(ID^*)}(g_2g_3)^{zG(ID^*)}
\end{aligned}
$$

$$
d_8^{sim} = (g^a)^{((ID^*-ID^*)wG(ID^*)-1)}g^{z'G(ID^*)} = g^{-a+z'G(ID^*)} = g^{zG(ID^*)}
$$

where $x = k - a, x' = aID^* + k'$, here $k, k', y, y', n, n', m, m', z'$ randomly chosen from $\mathcal{Z}_p^*$, and $z = -\frac{a}{G(ID^*)} + z'$ holds. After $\mathcal{B}$ generates private key for $ID^*$, it runs $\mathsf{ReKeygen}(sk_{ID^*}^{sim}, params, ID')$ with $sk_{ID^*}^{sim}$, and returns the result $rk_{ID^* \to ID'}$ to the adversary. We call this simulation as "Special Simulation".

(c) *$\mathcal{A}$ issues re-encryption queries on $(C_{ID}, ID, ID')$ to re-encrypt oracle $O_{reencrypt}$.* $\mathcal{B}$ first runs $rk_{ID \to ID'} = \mathsf{ReKeygen}(sk_{ID}, params, ID')$, then runs $\mathsf{Reencrypt}(rk_{ID \to ID'}, C_{ID}, ID, ID')$ and returns the result to the adversary.

(d) *$\mathcal{A}$ issues decryption queries on $(\widehat{C_{ID'}}, ID')$ to the first level ciphertext decrypt oracle $O_{1decrypt}$ under the only condition $(\widehat{C_{ID'}}, ID') \neq \mathsf{Derivative}(C_{ID^*}^*, ID^*)$ where* Derivative *defined in 2.5.1.*

i. $ID' \neq ID^*$, $\mathcal{B}$ first simulates $\mathsf{KeyGen}(msk, params, ID')$ as in "Normal Simulation" 3a, then runs $\mathsf{Decrypt}_1(sk_{ID'}, \widehat{C_{ID'}})$ and returns the result to the adversary.

ii. $ID' = ID^*$, $\mathcal{B}$ first simulates $\mathsf{KeyGen}(msk, params, ID^*)$ as in "Special Simulation" 3(b)ii, then runs $\mathsf{Decrypt}_1(sk_{ID^*}, \widehat{C_{ID^*}})$ and returns the result to the adversary.

4. **Challenge**. When $\mathcal{A}$ decides that Phase 1 is over, it outputs two messages $M_0, M_1 \in \mathbb{G}$, $\mathcal{B}$ picks a random bit $b$, a one time signature instance with public/private keys $(svk, ssk)$, and responds with the ciphertext $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, C_6^*, C_7^*) = (g^d, g^{(b+c)d}, (g^{\alpha'})^d, \mathtt{SE.Enc}(T, M_b), H_1(svk)^r, svk, \sigma)$ where $\sigma = \mathcal{S}(ssk, C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, C_6^*)$. Hence if $T = e(g,g)^{abd}$, then $C^*$ is a valid encryption of $M_b$ under $ID^*$. Otherwise, $C^*$ is independent of $b$ in the adversary's view.
5. **Phase 2**. $\mathcal{A}$ 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 $T = e(g,g)^{abd}$. Otherwise it outputs 0 meaning $T \neq e(g,g)^{abd}$.

When $T = e(g,g)^{abd}$ then $\mathcal{A}$'s advantage is the same as $\mathcal{B}$'s advantage for solving EXDBDH problem.

**Theorem 3.** *Suppose the EXDBDH assumption holds in* $(\mathbb{G}, \mathbb{G}_T, e)$ *and* SE *is* IND-CCA2 *secure, then our* IBPRE *scheme is* IND-sID-CCA2 *secure for the first level ciphertext.*

Proof. Following the same idea in the proof of theorem 2, we can prove this theorem, except this time the simulator needs to simulate re-encryption key on $(ID^*, ID')$ where $ID'$ is a corrupted identity. The simulator handles this query as following: it generates the private key for $ID^*$ as in "Special Simulation" 3(b)ii. And runs $\mathsf{ReKeygen}(sk^{sim}_{ID^*}, params, ID')$ with $sk^{sim}_{ID^*}$, returns the result to the adversary. Now even if the adversary gets the simulated private key for $ID'$ as in 3a, it can not get any useful information from these keys because they are independent with $sk^{sim}_{ID^*}$, that is, $(x, x', y, y', n', n', z')_{ID'}$ for any $ID'$ are independent with $(k, k', y, y', n, n', z')_{ID^*}$.

We follow the way in [5] of using $H(ID)$[5] instead of $ID$ to achieve full security for our IBPRE scheme.

**Theorem 4.** *In the standard model, let* $\mathcal{E}$ *be our* IBPRE *scheme, if it is a* $(t, q_s, \epsilon)$*-selective identity secure* IBPRE *system (*IND-sID-CCA2*). Suppose* $\mathcal{E}$ *admits* $N$ *distinct identities. Then* $\mathcal{E}$ *is also a* $(t, q_s, N\epsilon)$*-fully secure* IBPRE *(*IND-ID-CCA2*).*

Proof. The proof is directly following the proof for the similar theorem in [5], we omit it here due to page limitation.

**Theorem 5.** *Suppose the EXDBDH assumption holds in* $(\mathbb{G}, \mathbb{G}_T, e)$*,* SE *is* IND-CCA2 *secure and* $\mathcal{S}$ *is strongly unforgeable, then our* IBPRE *scheme can achieve master secret security.*

Proof. As shown in [17], CCA2 security for the first level ciphertext implies the master secret security, thus our IBPRE scheme can achieve master secret security.

[5]The space of $H(ID)$ is $N$.

## 5. Comparison

In this section, we give our comparison results with other IBPRE schemes: GA07A[13], GA07B[13], M07B [20], CT07[9], SXC08[24], LZD$^+$10[18], WCW10[30], LHC10[19]. Here A or B denotes the first scheme and the second scheme proposed in the corresponding papers. First we concern about schemes' security, then we concern about schemes' efficiency.

Notations: In Table 1, we denote W/O Random Oracle as with/without random oracle. In Table 2, we denote Enc as encryption, Reenc as re-encryption, Dec as decryption, Ciph as ciphertext and Ciph-Len as ciphertext length, $t_p$, $t_e$ and $t_{me}$ represent the computational cost of a bilinear pairing, an exponentiation and a multi-exponentiation respectively. $t_{se}$, $t_{sd}$ and $t_{sv}$ represent the computational cost of once symmetric encryption, once symmetric decryption and once symmetric checking decryption results' validity. $t_{\mathsf{s}}$ and $t_{\mathsf{v}}$ represent the computational cost of a one-time signature signing and verification respectively. $|\mathbb{G}|$ and $|\mathbb{G}_T|$ denote the bit-length of an element in groups $\mathbb{G}$ and $\mathbb{G}_T$ respectively. Here $\mathbb{G}_e$ and $\mathbb{G}_T$ are the prime order bilinear groups. $|SE|$ denotes the bit length of once symmetric encryption. Finally, $|vk|$ and $|s|$ denote the bit length of the one-time signature's public key and a one-time signature respectively.

From these two tables, we can conclude that our scheme is a new result on IBPRE. Our scheme can achieve master secret secure and is based on a novel IBE while all previous efficient IBPRE schemes are based on the traditional IBE. Furthermore, our scheme seems to be a more directly construction of IBPRE for its re-encryption key is operated on the exponent instead of on the underlying group. Our scheme is particularly efficient for the proxy, compared with other IND-ID-CCA secure and master secret secure IBPRE schemes [13, 18]. Considering the proxy is always a heavy work-load party, our scheme can greatly improve the efficiency for the whole IBPRE system.

**Remark2.** (1) Luo et al.'s IBPRE scheme [19] is a generic construction, therefore their scheme can be in random oracle and standard model, and the underlying assumption can be various. (2) Actually, our IBPRE's security also rely on the underlying symmetric encryption scheme's IND-CCA2 security. (3) Our first level ciphertext maps second level ciphertext and second level ciphertext maps first level ciphertext in [13, 9]. (4) GA07 and CT07 are multi-hop IBPRE but we just consider their single-hop variant. (5) We omit the comparison between our IBPRE with SXC08 [24], LZD$^+$10 [18], WCW10

[30], LHC10 [19] schemes, for the following reasons: SXC08 [24], LZD$^+$10 [18] schemes are based on Waters' IBE, which make their schemes have large parameters; WCW10 [30] scheme can not achieve master secret secure and is only proved secure in the random oracle model; LHC10 [19] scheme is a generic construction. (6) In our scheme, we compute $e(C'_1, C'_8)e(C'_1, d_7)$ as $e(C'_1, C'_8 d_7)$.

| Scheme | Security | W/O Random Oracle | Assumption | Master Secret Secure | Underlying IBE |
|---|---|---|---|---|---|
| GA07A | IND-ID-CPA | Random Oracle | DBDH | ✗ | BF IBE |
| GA07B | IND-ID-CCA | Random Oracle | DBDH | ✗ | BF IBE |
| M07B | IND-ID-CPA | Standard Model | DBDH | ✗ | $BB_1$ IBE |
| CT07 | IND-ID-CPA | Standard Model | DBDH | ✗ | Waters' IBE |
| SXC08 | IND-ID-CCA | Standard Model | DBDH | ✗ | Waters' IBE |
| LZD$^+$10 | IND-ID-CCA | Standard Model | DBDH | ✓ | Waters' IBE |
| WCW10 | IND-ID-CCA | Random Oracle | DBDH | ✗ | Variant of BF IBE |
| LHC10 | IND-ID-CPA | Generic | Generic | ✓ | Generic |
| Ours | IND-ID-CCA | Standard Model | EXDBDH | ✓ | New IBE |

Table 1: IBPRE Security Comparison

| Scheme | Enc | Check | Reenc | Dec | | Ciph-Len | |
|---|---|---|---|---|---|---|---|
| | | | | 1stCiph | 2ndCiph | 1stCiph | 2ndCiph |
| GA07A | $1t_e + 1t_p$ | 0 | $1t_p$ | $2t_p$ | $1t_p$ | $2\|G\| + 2\|G_e\|$ | $1\|G\| + 1\|G_e\|$ |
| GA07B | $1t_p + 1t_e$ | $2t_p$ | $2t_e + 2t_p$ | $1t_e + 2t_p$ | $2t_e + 2t_p$ | $1\|G\| + 1\|G_e\|$ $+2\|m\| + \|id\|$ | $1\|G\| + 1\|G_T\|$ $+1\|G_e\| + \|m\|$ |
| M07B | $1t_p + 2t_e$ | $2t_p$ | $1t_p$ | $2t_p$ | $2t_p$ | $2\|G_e\| + 1\|G_T\|$ | $2\|G_e\| + 1\|G_T\|$ |
| CT07 | $3t_e + 1t_p + 1t_s$ | $1t_v$ | $2t_e$ | $2t_e + 10t_p + 1t_v$ | $2t_e + 3t_p$ | $9\|G\| + 2\|G_T\|$ $+\|vk\| + \|s\|$ | $3\|G\| + \|G_T\|$ $+\|vk\| + \|s\|$ |
| Ours | $2t_e + 2t_{me}$ $+1t_s + 1t_{se}$ | $1t_v + 2t_p$ | $t_e + t_p$ | $2t_p + 1t_{sd}$ | $5t_p + 1t_{sd}$ $+1t_{sv}$ | $5\|G\| + 1\|G_T\| + 1\|SE\|$ | $4\|G\| + 1\|s\|$ $+1\|vk\| + 1\|SE\|$ |

Table 2: IBPRE Efficiency Comparison

## 6. Conclusion

In this paper, we propose a new IBE scheme which does not lie in the IBE's three frameworks [7]. The main novelty is the way we embed the master key in the private key. We prove this IBE is IND-sID-CPA secure in the standard model based on a related DBDH assumption in the bilinear groups. Based on this new IBE scheme, we propose a new IBPRE scheme which is IND-ID-CCA2 secure, efficient for the proxy and master secret secure. As the future work, it is interesting to find more applications of our IBE and IBPRE.

**Acknowledgment**

The authors would like to express their gratitude thanks for Prof. Liqun Chen's many helpful comments. This work is still in progress and supported by the National Natural Science Foundation of China under contract no.61103230, Natural Science Foundation of Shaanxi Province under contract no.2010JM8034 and Natural Science Foundation of Engineering University of Chinese Armed Police Force.

**References**

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

[2] 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.

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

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

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

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

[7] X. Boyen. A tapestry of identity-based encryption: practical frameworks compared, In *International Journal of Applied Cryptography*, Vol.1, No.1, pp. 3–20.

[8] R. Canetti and S. Hohenberger. Chosen ciphertext secure proxy re-encryption. In *ACM CCS 2007*, pages 185–194, 2007. Full vision available at Cryptology ePrint Archive: `http://eprint.iacr.org/2007/171.pdf`.

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

[10] C. Chu, J. Weng, S.S.M. Chow, J. Zhou and R.H. Deng. Conditional proxy broadcast re-encryption. In *ACISP 2009*, volume 5594 of *LNCS*, pages 327–342, 2009.

[11] R. Deng, J. Weng, S. Liu and K. Chen. Chosen iiphertext secure proxy re-encryption without pairing. In *CANS 2008*, volume 5339 of *LNCS*, pages 1–17, 2008.

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

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

[14] C. Gentry. Practical identity-based encryption without random oracles. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464, 2006.

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

[16] 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.

[17] B. Libert and D. Vergnaud. Unidirectional chosen ciphertext secure proxy re-encryption. In *PKC 2008*, volume 4939 of *LNCS*, pages 360–379, 2008. full vision available at `http://www.dice.ucl.ac.be/~libert/`.

[18] J. Lai, W. Zhu, R. Deng, S. Liu and W. Kou New constructions for identity-based unidirectional proxy re-encryption. In *Journal of Computer Science and Technology*, no. 25(4), pages 793–806. 2010.

[19] S. Luo, J. Hu and Z. Chen. New construction of identity-based proxy re-encryption. Cryptology ePrint Archive, Report 2010/444, 2010.

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

[21] M. Naor. On cryptographic assumptions and challenges. In *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109, 2003.

[22] J. Shao and Z. Cao. CCA-secure proxy re-encryption without pairing. In *PKC 2009*, volume 5443 of *LNCS*, pages 357–376, 2009.

[23] J. Shao, Z. Cao and P. Liu. SCCR: a generic approach to simultaneously achieve CCA security and collusion-resistance in proxy re-encryption. In *Security and Communication Networks*, 2009.

[24] 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`.

[25] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive: `http://eprint.iacr.org/2003/054.pdf`.

[26] A. Shamir. Identity-based cryptosystems and signature Schemes. In *CRYPTO 1984*, volume 196 of *LNCS*, pages 47–53, 1984.

[27] 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.

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

[29] B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127, 2005.

[30] H. Wang, Z. Cao, L. Wang. Multi-use and unidirectional identity-based proxy re-encryption schemes. In *Information Science*, No 180, pages 4042-4059, 2010.

[31] X. A. Wang and X. Yang On the insecurity of an identity based proxy re-encryption. In *Fundamental Informaticae*, no. 98(2-3), pages 277–281. 2010.

[32] X. A. Wang, W. Zhong. A new identity based encryption scheme. In *The International Conference on Biomedical Engineering and Computer Science (ICBECS2010)*, IEEE Press, 381-384, 2010.

[33] X. A. Wang, W. Zhong. A new identity based proxy re-encryption scheme. In *The International Conference on Biomedical Engineering and Computer Science (ICBECS2010)*, IEEE Press, 384-388, 2010.

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