New Identity Based Encryption And Its Proxy Re-encryption

Xu An Wang, Xiaoyuan Yang, and Yiliang Han

Key Laboratory of Information and Network Security
Engineering College of Chinese Armed Police Force, P.R. China
wangxahq@yahoo.com.cn

Abstract. Identity based encryption(IBE) have been received great attention since Boneh and Franklin's breakthrough work on IBE by using bilinear groups. Till now, many IBE schemes relying on bilinear maps with different properties have been proposed. They are including the BB_1 [5], BB_2 [5], SK [30], Waters [34], Gentry's [16] IBE. However, these IBE schemes have one common character: they all embed the $master-key$ in the private key at the exponential. In this paper, we propose a new way to embed $master-key$ in the private key and construct a new IBE scheme. To prove our scheme's security, we introduce some new technique which maybe has independent interest. As our new IBE's application, we construct a new efficient identity based proxy re-encryption(IBPRE) which can achieve *master secret security*. It can also resist *transferring of delegation attack*, where all previous PREs can not achieve.

1 Introduction

In 1984, Shamir [31] introduced the concept of identity-based encryption (IBE), whose motivation is to ease the certificate management in the e-mail system. A user's public key in an identity-based system is some unique information about the identity of the user (e.g., email address). For example, when Alice wants to send an encrypted message to another user Bob's email address `Bob@university.edu.country`, Alice simply encrypts the message with the string "`Bob@university.edu.country`". However, practical identity based encryption was only realized by Boneh and Franklin relying on bilinear maps on elliptic curve in 2001, almost two decade years after its first appearance. Since then, many practical IBE schemes with different properties have been proposed. It has also been shown to be very useful to construct IND-CCA2 cryptosystems [8] and have many other interesting applications. Now there are over 200 papers related to IBE in the literature. In 2008, IEEE P1363 set up P1363.3 to standardize identity based cryptography by using bilinear groups [24]. Undoubtedly, IBE will be one of the most successful research results in our cryptographic community.

The concept of proxy re-encryption (PRE) comes from the work of Blaze et al. in 1998 [3]. 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]. In ACNS'07, Green et al. proposed the first identity based proxy re-encryption schemes and discussed its many unique interesting applications such as secure transfer encrypted email for Alice to Bob, attribute based delegations, bridging IBE and PKE etc [15]. Recently, PRE have been received great attention from researchers, many good papers have been proposed around this topic. However, there are still only a few results on IBPRE, specially, all the IBPRE schemes proposed rely on "secret sharing" technique to realize proxy re-encryption, which suffer from the delegatee and proxy collusion attack. That is, they all can not achieve *master secret security*, which is an important property for applications.

1.1 Related Work

Identity Based Encryption Till now, there are three ways to construct identity based encryption. The first way is to use bilinear groups [5,6,30,34,16], the second way is relying on residue quadratic [12] and the third way is to use lattice [17]. For our idea is closely related to identity based encryption based on bilinear pairings, we just recall work in this area.

In Crypto'01, Boneh and Franklin constructed the first practical identity based encryption based on bilinear groups [4] with provable security in the random oracle model (BF IBE). Except constructing the first practical identity based encryption, their contribution included initialing the work on constructing cryptographic primitives on bilinear groups and formally giving the security model for identity based encryption. In 2003, Sakai and Kasahara also proposed an identity based encryption based on bilinear groups (SK IBE) [30], which based on their original work in 2001 [29]. However, both of these work are relying on random oracle to prove their security. In Eurocrypt'04, Boneh and Boyen proposed two new efficient selective identity secure identity based encryption schemes without random oracles ($\mathsf{BB_1}$ IBE and $\mathsf{BB_2}$ IBE) [5]. Later in Crypto'04, they improved their scheme which can achieve full security but has loose reduction [6]. In Eurocrypt'05, Waters improve their work by proposing an identity based encryption with tight security proof in the standard model (Waters' IBE) [34]). In Eurocrypt'06, Gentry proposed an interesting efficient identity based encryption with tight security proof in the standard model but based on a strong assumption (Gentry's IBE) [16].

According to Boyen's work [7], all the IBE, HIBE and AIBE by using bilinear group can be divided into three types: "Full Domain hash" framework, " Exponent Inversion" framework and "Communicative Blinding" framework. "Full Domain hash" framework includes BF IBE and Gentry's HIBE, these schemes always prove their security in random oracle and support hierarchies and threshold variants. " Exponent Inversion" framework includes SK IBE, $\mathsf{BB_2}$ IBE and Gentry's IBE, these schemes are also called vanilla IBE which are difficult to support extensions. "Communicative Blinding" framework includes $\mathsf{BB_1}$ IBE and Waters' IBE, these schemes always easily to support extensions like hierarchies, threshold, fuzzy, attribute identity 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 [15]. 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 [10]. They follow the paradigm proposed in [15] (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 [28]. 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 [37]. In Inscrypt'08, Tang et al. proposed the new

concept of inter-domain identity based proxy re-encryption [33]. 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 [19]. Recently Lai et al. [20] gave new constructions on IBPRE based on identity-based mediated encryption. Luo et al. [22] also gave a new generic IBPRE construction based on IBE. Wang et al. proposed the first multi-use CCA-secure unidirectional IBPRE scheme [36].

1.2 Our Contribution

In this paper, we first construct a new identity based encryption. Our new identity based encryption can not lie in the three frameworks above. The main novelty of our IBE is that we embed the $\mathsf{master-key}$ in the plain form while all the other IBEs embed the $\mathsf{master-key}$ in the exponential form. At first looking, this way seems to be dangerous for adversary maybe can easily extract information on $\mathsf{master-key}$, but we avoid this problem by introducing randomness in the private keys. To prove our IBE, we introduce some new technique including constructing IBE in composite order group and adding easily cancel "randomness". Our idea maybe have independent interest excluding this new IBE.

We then construct an identity based proxy re-encryption based on this new IBE. This new IBPRE do not follow Green's paradigm again. It generates the re-encryption key by introducing some non easily cancel "randomness" to the delegator's private key. The main novelty in this IBPRE is that, the re-encryption key is independent with the delegatee's private key, where all the other IBPRE even PRE can not have this property. As a result, our IBPRE can achieve *master secret security*, and can resist *transferring of delegation attack*, where all previous PREs can not.

1.3 Organization

In Section 2, we give preliminaries which our schemes need. In Section 3, we construct our new identity based encryption and prove its IND-sID-CPA security. In Section 4.1, we construct our new identity based proxy re-encryption and enhance it to be IND-ID-CCA2 secure, prove its IND-ID-CCA secure, master secret secure and resisting transferring of delegation attack. In Section 5, we give our comparison results. In the last Section 6, we concludes our paper with some open problem.

2 Preliminaries

2.1 Bilinear Groups of Composite Order

Let $\mathcal{G}$ be an algorithm called a group generator that takes as input a security parameter $\lambda \in Z^{>0}$ and outputs a tuple (p, q, G, G_T, e) where p, q are two distinct primes, $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups of order $n = pq$, and e is a function $e : \mathbb{G}^2 \to \mathbb{G}_T$ 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 n 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 λ. Furthermore, we assume that the description of $\mathbb{G}$ and $\mathbb{G}_T$ includes a generator of $\mathbb{G}$ and $\mathbb{G}_T$ respectively. We will use the notation $\mathbb{G}_p$, $\mathbb{G}_q$ to denote the respective subgroups of order p and order q of $\mathbb{G}$.

Bilinear groups of composite order have found many applications in cryptography.

2.2 EcDBDH Assumption in Composite Order Group

EcDBDH assumption extends the DBDH assumption in bilinear group of prime order to bilinear group of composite order.

Definition 1. *Run $\mathcal{G}$ to obtain (p, q, G, G_T, e) with $G = G_p \cdot G_q$. Next it generates g, g_p, g_q as generators of G, G_p and G_q. On input $(p, q, g, g^a, g^b, g^c, g^{ac}, g^{bp}, g^{(bp+c)d}, g^d, T)$ where $(p, q) \nmid (a, b, c, d)$, for any P.P.T algorithm $\mathcal{A}$ can not distinguish $T = g^{abd}$ from a random element in $\mathbb{G}$ with non-negligible probability, this is the ecDBDH assumption.*

We note that this assumption is not a very standard assumption, but it is a non-interactive assumption [25].

2.3 Definition and Security Notion for IBE

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

Setup(1^k). Given a security parameter 1^k, PKG generate a pair (params, msk), where params denotes the public parameters and msk is the master − key.

KeyGen(msk, params, ID). Given the master − key msk and an identity ID with params, generate a secret key sk_{ID} for ID.

Encrypt(ID, params, m). Given a message m and the identity ID with params, compute the encryption of m, C_{ID} for ID.

Decrypt(sk_{ID}, params, C_{ID}). Given the secret key sk, decrypt the ciphertext C_{ID}.

Security Notion We recall the IND-sID-CPA security. it is defined using the following game:

Init: The adversary outputs an identity ID^* where it wishes to be challenged.

Setup: The challenger runs the Setup algorithm. It gives the adversary the resulting system parameters params. It keeps the master − key to itself.

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 $q_1, \cdots, q_{i-1}$.

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.

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.

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 $Adv_{\epsilon,Aa} =\mid Pr[b = b'] - \frac{1}{2} \mid$, 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 and Security Notion for IBPRE

Definition An identity based proxy re-encryption scheme is tuple of algorithms (Setup, KeyGen, Encrypt, Decrypt, ReKeygen, Reencrypt):

Setup(1^k). On input a security parameter, the algorithm outputs both the master public parameters which are distributed to users, and the master − key (msk) which is kept private.
KeyGen(params, msk, id). On input an identity $id \in \{0,1\}^*$ and the master secret key, outputs a decryption key sk_{id} corresponding to that identity.
Encrypt(params, id, m). On input a set of public parameters, an identity $id \in \{0,1\}^*$ and a plaintext $m \in M$, output c_{id}, the encryption of m under the specified identity.
ReKeygen(params, msk, sk_{id_1}, sk_{id_2}, id_1, id_2). On input secret keys msk, sk_{id_1}, sk_{id_2}, and identities $id \in \{0,1\}^*$, PKG, the delegator and the delegatee interactively generate the re-encryption key $rk_{id_1 \to id_2}$, the algorithm output it.
Reencrypt(params, $rk_{id_1 \to id_2}$, c_{id_1}). On input a ciphertext c_{id_1} under identity id_1, and a re-encryption key $rk_{id_1 \to id_2}$, outputs a re-encrypted ciphertext c_{id_2}.
Decrypt(params, sk_{id}, c_{id}). Decrypts the ciphertext c_{id} using the secret key sk_{id}, and outputs m or $\perp$.

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

Security Notion First we recall the IND-ID-ATK(CPA, CCA) Security, then we recall the Master Secret Security. Let $\mathcal{S}$ be an IBPRE scheme defined as a tuple of algorithms (Setup, KeyGen, Encrypt, Decrypt, ReKeygen, Reencrypt).

For ATK ∈ (CPA, CCA), IND-ID-ATK Security is defined according to the following game.

Setup. Run Setup(1^k) to get (params, msk), and give params to $\mathcal{A}$.
Find phase. $\mathcal{A}$ makes the following queries. At the conclusion of this phase $\mathcal{A}$ will select $id^* \in \{0,1\}^*$ and $(m_0, m_1) \in \mathcal{M}^2$.
1. For $\mathcal{A}$'s queries of the form $(extract, id)$, return $sk_{id} = KeyGen(\text{params}, msk, id)$ to $\mathcal{A}$.
2. For $\mathcal{A}$'s queries of the form $(rkextract, id_1, id_2)$, where $id_1 \neq id_2$, return $rk_{id_1 \to id_2}$=ReKeygen (params, msk, KeyGen(params, msk, id_1), KeyGen(params, msk, id_2), id_1, id_2) to $\mathcal{A}$.
3. For $\mathcal{A}$'s queries of the form $(decrypt, id, c)$, if ATK=CCA then return m=Decrypt(params, KeyGen(params, msk, id), c) to $\mathcal{A}$. Otherwise, if ATK=CPA, return $\perp$ to $\mathcal{A}$.

4. For $\mathcal{A}$'s queries of the form $(reencrypt, id_1, id_2, c)$, if ATK=CCA then derive a re-encryption key $rk_{id_1 \to id_2}$ = ReKeygen(params, msk, KeyGen(params, msk, id_1), KeyGen(params, msk, id_2), id_1, id_2), and return $c' = Reencrypt(params, rk_{id_1 \to id_2}, id_1, id_2, c)$ to $\mathcal{A}$. If $ATK = CPA$, return $\perp$ 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).

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 $\mathcal{A}$.

Guess stage. $\mathcal{A}$ continues to make queries as in the find stage, with the following restrictions. Let $(\mathcal{C}, ID)$ be a set of ciphertext/identity pairs, initially containing the single pair (c^*, id^*). For all $c \in \mathcal{C}$ and for all rk given to $\mathcal{A}$, let $\mathcal{C}'$ be the set of all possible values derived via calls to Reencrypt:

1. $\mathcal{A}$ is not permitted to issue any query of the form (decrypt, id, c) where $(c, id) \in (\mathcal{C} \cap \mathcal{C}')$.
2. $\mathcal{A}$ is not permitted to issue any queries $(extract, id)$ or (rkextract, id_1, id_2) that would permit trivial decryption of any ciphertext in (C, C').
3. $\mathcal{A}$ is not permitted to issue any query of the form (reencrypt, id_1, id_2, c) where $\mathcal{A}$ possesses the keys to trivially decrypt ciphertexts under id_2 and $(c, id_1) \in (\mathcal{C} \cap \mathcal{C}')$.
4. $\mathcal{A}$ is not permitted to issue any query of the form (reencrypt, id_1, id_2, c) where $\mathcal{A}$ possesses the keys to trivially decrypt ciphertexts under id_2 and $(c, id_1) \in (\mathcal{C} \cap C')$. On successful execution of any re-encrypt query, let c' be the result and add the pair (c', id_2) to the set 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 $Adv_A^{IND-ID-ATK} = | \ Pr(i' = i) - 1/2 \ |$. If for all probabilistic polynomial time algorithms A, $Adv_A^{IND-ID-ATK(CPA,CCA)} \leq v(k)$, we say that the Identity-Based Proxy Re-encryption scheme $\mathcal{S}$ is IND-ID-ATK(CPA, CCA) secure.

Master Secret Security. We borrow this definition from [21], just extending the definition for unidirectional PRE to unidirectional IBPRE. Libert and Vergnaud's definition is as following:

"In [1], Ateniese et al. define an important security requirement for unidirectional PRE schemes. This notion, termed master secret security, 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 λ[1].

$$\begin{aligned} Pr[(pk^\star, sk^\star) \leftarrow \mathsf{KeyGen}(\lambda), \{(\mathsf{pk_x}, \mathsf{sk_x})\} \leftarrow \mathsf{KeyGen}(\lambda)\}, \\ \{R_{\star x} \leftarrow \mathsf{ReKeygen}(\mathsf{sk}^\star, \mathsf{pk_x})\}, \{\mathsf{R_{x\star}} \leftarrow \mathsf{ReKeygen}(\mathsf{sk_x}, \mathsf{pk}^\star)\}, \\ \gamma \leftarrow A(pk^\star, \{pk_x, sk_x\}, \{R_{\star x}\}, \{R_{x\star}\}) : \gamma = sk^\star] \end{aligned}$$

At first glance, this notion might seem too weak in that it does not consider colluding delegatees who would rather undertake to produce a new re-encryption key $R_{\star x'}$ that was not originally given and allows re-encrypting from the target user to another malicious party x'. As stressed

[1] Notations: ($pk^\star$, $sk^\star$) denotes the target user's public and private key and (pk_x, sk_x) denotes the colluding user's public key and private key.

in [1], however, all known unidirectional schemes fail to satisfy such a stronger security level. It remains an open problem to construct systems withstanding these *transfer of delegation attacks*."

We extend this definition to the identity based setting. Formally, the following probability should be negligible as a function of the security parameter λ,

$$\begin{aligned} &Pr[(ID^\star, sk_{ID^\star}) \leftarrow \mathsf{KeyGen}(\lambda), \{(\mathsf{ID_x}, \mathsf{sk_{ID_x}})\} \leftarrow \mathsf{KeyGen}(\lambda)\}, \\ &\{R_{ID^\star \to ID_x} \leftarrow \mathsf{ReKeygen}(\mathsf{sk_{ID^\star}}, \mathsf{ID_x})\}, \{\mathsf{R_{ID_x \to ID^\star}} \leftarrow \mathsf{ReKeygen}(\mathsf{sk_{ID_x}}, \mathsf{ID^\star})\}, \\ &\gamma \leftarrow A(ID^\star, \{ID_x, sk_{ID_x}\}, \{R_{ID^\star \to ID_x}\}, \{R_{ID_x \to ID^\star}\}) : \gamma = sk_{ID^\star}] \end{aligned}$$

And the situation is even worse for IBPRE. Until now, all the IBPREs [15,10,28,32] can even not achieve Master Secret Security, of course they can not withstand *transfer of delegation attacks*. In this paper, we construct the first IBPRE which can achieve *master secret security*, the first PRE which can withstand *transfer of delegation attacks*.

3 New Identity Based Encryption

3.1 Our Construction

Setup($\mathbf{1^k}$). Run $G(1^n)$ to obtain (p, q, G, G_T, e) with $G = G_p \cdot G_q$. Next it generates g, g_p, g_q as generators of G, G_p and G_q. For now, we assume public keys (ID) is element in Z_n^*. We later extend the construction to public keys over $\{0,1\}^*$ by first hashing ID using a collision resistant hash $H : \{0,1\}^* \to Z_n^*$. We also assume messages to be encrypted are elements in G_T. Given a security parameter 1^k, select a random generator $g \in G$ and random t_1, t_2, t_3, let $g_2 = g^{pt_1} \in G_q, g_3 = g^{t_3}, h = g^{t_2}$. Pick a random $\alpha \in Z_n^*$. We require that $p, q \nmid t_1, t_2, t_3, \alpha$. Set $g_1 = g^\alpha$, that is,

$$\mathsf{params} = (g, g_1, g_2, g_3, h, n, G, G_T, e), msk = (\alpha, p, q, t_1, t_2, t_3)$$

KeyGen($\mathbf{msk}, \mathsf{params}, \mathbf{ID}$). Given $msk = (\alpha, p, q, t_1, t_2, t_3)$ and ID with $params$, the PKG picks random $x, y, x', y' \in Z_n^*$. If $q \mid \alpha ID + t_2$, then return $\perp$, else set [2]

$$\begin{aligned} sk_{ID} &= (d_{ID}^A, d_{ID}^B, d_{ID}^C) \\ d_{ID}^A &= (d_1, d_2, d_3) = (\frac{\alpha + x}{\alpha ID + t_2} + y \mod n, g^x (g_1^{ID} h)^y, g^{t_3 x} (g_1^{ID} h)^{t_3 y}) \\ d_{ID}^B &= (d_1', d_2', d_3') = (\frac{(t_2 + x')}{\alpha ID + t_2} + y' \mod n, g^{x'} (g_1^{ID} h)^{y'}, g^{t_3 x'} (g_1^{ID} h)^{t_3 y'}) \\ d_{ID}^C &= d_4 = (g_1^{ID} h)^{t_3} \end{aligned}$$

Encrypt($\mathbf{ID}, \mathsf{params}, \mathbf{M}$). To encrypt a message $M \in G_T$ under the public key $ID \in Z_n^*$, pick a random $r \in Z_n^*$ and compute

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

if $Me(g_1, g_2)^r = M$, then choose another r and try again.

[2] Note here the key generator center knows $n = pq$, thus he can compute $\frac{\alpha+x}{\alpha ID+t_2} + y \mod n$, $\frac{(t_2+x')}{\alpha ID+t_2} + y' \mod n$, we can also first hash on ID to avoid the case there are no inverse for $\alpha ID + t_2$, but this probability is negligible.

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

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

Correctness: See the appendix A.

3.2 Security Analysis

Intuition. At first sight, it is impossible to prove our IBE. It is no way to simulate $d_1 = \frac{(\alpha+x)}{\alpha ID+t_2} + y \mod n$ without knowing α. We show this is not true. Our scheme comes from the BB_1 IBE, in the simulation of BB_1, they let $h = g_1^{-ID^*} g^{\alpha'}$, we also follow this strategy. That means, $d_1 = \frac{(a+x)}{aID - aID^* + \alpha'} + y \mod n$. Although the simulator can not know a, it can let $x = \frac{\alpha'}{ID - ID^*} \mod n$ and get $d_1 = \frac{1}{ID-ID^*} + y \mod n$. Because our scheme relying on composite order bilinear group , $C_4 = Me(g_2, g_1)^r$ and the Decrypt needs to compute $e(g_2, C_3^{d_1})$, we can set $d_1 = \frac{1}{ID-ID^*} + y + kq \mod n$ which can still decrypt the ciphertext. Now the adversary can not distinguish the simulated d_1 from the real d_1 for non q-order group elements for the additional randomness kq in d_1. But the adversary still has some chance to distinguish the simulated d_1 from the real d_1 by using g_2. It can distinguish in two ways: verifying $\frac{g_2^{d_1}}{g_2^y} = g_2^{\frac{1}{ID-ID^*}}$ or verifying $\frac{e(g_2, g_x^{d_1})}{e(g_2, g_x)^y} = e(g_2, g_x)^{\frac{1}{ID-ID^*}}$ where g_x is some easily computable function from g_1, g, h (for example, $(g_1^{ID} h)^r$). But in our IBE, this is impossible for the adversary can not compute g_2^y or $e(g_2, g_x)^y$. The simulation of d_1' is same as the simulation of d_1.

Theorem 1. *Suppose the ecDBDH assumption holds in the composite order group G, 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 ecDBDH problem in G . On input $(p, q, g, g^a, g^b, g^c, g^{ac}, g^{bp}, g^{(bp+c)d}, g^d, T)$ where $(p, q) \nmid (a, b, c, d)$, algorithm $\mathcal{B}$'s goal is to output 1 if $T = g^{abd}$ and 0 otherwise. Let $g = g, g_1 = g^a, g_2 = g^{bp}, g_3 = g^c$. Algorithm $\mathcal{B}$ works by interacting with $\mathcal{A}$ in a selective identity game as follows:

1. **Initialization**. The selective identity game begins with $\mathcal{A}$ first outputting an identity ID^* that it intends to attack.
2. **Setup**.To generate the system's parameters, algorithm $\mathcal{B}$ picks $\alpha' \in Z_n^*$ at random and defines $h = g_1^{-ID^*} g^{\alpha'} \in G$. 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 queries on ID".*
   We observe that

$$d_1 = \frac{\alpha + x}{\alpha ID + t_2} + y \mod n$$
$$d_1' = \frac{t_2 + x'}{\alpha ID + t_2} + y' \mod n$$

where y, y' randomly chosen from Z_n^*. From the simulation, we know that $\alpha = a$, $t_2 = \alpha' - aID^*$, thus we can get

$$d_1 = \frac{a+x}{aID + \alpha' - aID^*} + y \mod n$$
$$d_1' = \frac{a(-ID^*) + \alpha' + x'}{aID + \alpha' - aID^*} + y' \mod n$$

If we let

$$x = \frac{\alpha'}{ID - ID^*} \mod n$$
$$x' = \frac{(-ID^*)\alpha'}{ID - ID^*} - \alpha' \mod n$$

we can get

$$d_1 = \frac{1}{(ID - ID^*)} + y \mod n$$
$$d_1' = \frac{-ID^*}{(ID - ID^*)} + y' \mod n$$

But $\mathcal{B}$ return

$$d_1^{sim} = \frac{1}{(ID - ID^*)} + y + k_1 q \mod n$$
$$d_1'^{sim} = \frac{-ID^*}{(ID - ID^*)} + y' + k_2 q \mod n$$

to $\mathcal{A}$ where k_1, k_2 chosen randomly from Z_n^*. In the following we will show that this modification is reasonable.

– For g_2, d_1 needs to satisfy

$$e(g_2, g_1)^r = \frac{e(g_2, (g_1^{ID-ID^*} g^{\alpha'})^{d_1 r})}{e(g_2, g^x) e(g_2, ((g_1^{ID-ID^*} g^{\alpha'})^r)^y}$$
$$e(g_2, g_1^{-ID^*} g^{\alpha'})^r = \frac{e(g_2, (g_1^{ID-ID^*} g^{\alpha'})^{d_1 r})}{e(g_2, g^x) e(g_2, ((g_1^{ID-ID^*} g^{\alpha'})^r)^{y'}}$$

we can verify these equations are satisfied by $x, x', d_1^{sim}, d_1'^{sim}$. Next we show that the simulator can give other private keys for ID.

$$d_2^{sim} = g^x (g_1^{ID} h)^y = g^{\frac{\alpha'}{ID-ID^*}} (g_1^{ID} h)^y$$
$$d_3^{sim} = g^{t_3 x} (g_1^{ID} h)^{t_3 y} = g^{cx} (g^{ac(ID-ID^*)} g^c)^y = (g^c)^{(\frac{\alpha'}{ID-ID^*})} (g^{ac})^{y(ID-ID^*)} (g^c)^y$$
$$d_2'^{sim} = g^{x'} (g_1^{ID} h)^{y'} = g^{\frac{(-ID^*)\alpha'}{ID-ID^*} - \alpha'} (g_1^{ID} h)^{y'}$$
$$d_3'^{sim} = g^{t_3 x'} (g_1^{ID} h)^{t_3 y'} = (g^c)^{\frac{(-ID^*)\alpha'}{ID-ID^*} - \alpha'} (g^{ac(ID-ID^*)} g^c)^{y'} = (g^c)^{\frac{(-ID^*)\alpha'}{ID-ID^*} - \alpha'} (g^{ac})^{y'(ID-ID^*)} (g^c)^{y'}$$

the adversary can use these private keys to correctly decrypt the ciphertext, thus this is a computation sound simulation for g_2.

– For g_x(g_x is some easily computable function from g_1, g, h), the adversary can not distinguish the simulated $d_1^{sim}, d_1'^{sim}$ from real d_1, d_1' for it can not get any information on randomness k_1q, k_2q. No other private keys give any information on $g_x^{k_1q}, g_x^{k_2q}$ or $e(g_x, g_x')^{k_1q}, e(g_x, g_x')^{k_2q}$. thus this is also a computation sound simulation for g_x.

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

4 New Identity Based Proxy Re-encryption

4.1 Our Construction

– The underlying IBE: our IBE constructed above.

– The delegation scheme:

ReKeygen($\mathbf{d_{ID}}, \mathbf{params}, \mathbf{ID'}$). ID generates the re-encryption key as follows:

1. We first define an algorithm Rand to randomize the secret key. ID runs Rand as follows: It first chooses $\widehat{y}, \widehat{y'} \in Z_n$ randomly, then it randomize $d_1, d_2, \cdots, d_3'$ as follows:

$$R(d_1) = d_1 + \widehat{y}, R(d_2) = d_2 \cdot (g_1^{ID}h)^{\widehat{y}}, R(d_3) = d_3 \cdot (d_4)^{\widehat{y}}$$

$$R(d_1') = d_1' + \widehat{y'}, R(d_2') = d_2' \cdot (g_1^{ID}h)^{\widehat{y'}}, R(d_3') = d_3' \cdot (d_4')^{\widehat{y'}}$$

2. Then for every re-encryption key query, ID first randomizes its secret key, then chooses randomly $z, \widehat{y}, \widehat{y'} \in Z_n^*$ and computes[3]

$$\begin{aligned} rk_{ID \to ID'} &= (rk_1, rk_2, rk_3) \\ &= (R(d_1) \cdot ID' + R(d_1') + z \mod n, R(d_2)^{ID'} R(d_2')(g_1^{ID}h)^z, R(d_3)^{ID'} R(d_3') d_4^z) \end{aligned}$$

Reencrypt($\mathbf{rk_{ID \to ID'}}, \mathbf{params}, \mathbf{C_{ID}}, \mathbf{ID'}$). On input $C_{ID} = (C_1, C_2, C_3, C_4)$, computes

$$\widehat{C_{ID'}} = (\bar{C_1}, \bar{C_2}, \bar{C_3}, \bar{C_4}) = (C_1, C_2, \frac{e(g_2, C_3^{rk_1}) e(C_1, rk_3)}{e(C_2, rk_2)}, C_4)$$

Deccrypt($\mathbf{sk_{ID'}}, \mathbf{params}, \mathbf{C_{1ID'}}$). ID' with $d_{ID'}^A = (d_1', d_2', d_3')$ decrypts the re-encrypted ciphertext as

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

Correctness: See the appendix B.

[3] In the afterwards algorithms, to express the relationships clearly, we implicit set $R(d_1) = d_1, \cdots, R(d_3') = d_3$, that is, we do not randomize the secret key. But note all these relationships hold for the randomized secret key also.

4.2 Enhancing It to Be IND-ID-CCA2 Secure

In this subsection, we show how to enhance the IBE scheme to be IND-ID-CCA2 Secure. First we follow the way in [5] by hashing ID using a properly collision resistant hash function before using ID to achieve full security, that is, IND-ID-CPA Secure. There are two security results we can get

Theorem 2. *In the standard model, let $\mathcal{E}$ be our* IBE *scheme, if it is a (t, q_s, ϵ)-selective identity secure* IBE *system (IND-sID-CPA). Suppose $\mathcal{E}$ admits N distinct identities. Then $\mathcal{E}$ is also a $(t, q_s, N\epsilon)$-fully secure* IBE *(IND-ID-CPA).*

Theorem 3. *In the random oracle model, let $\mathcal{E}$ be our* IBE *scheme, if it is a (t, q_s, ϵ) selective-ID secure* IBE*. Suppose identities in $\mathcal{E}$ are n-bits long. Let H be a hash function $H : \{0,1\}^* \to \{0,1\}^n$ modeled as a random oracle. Then $\mathcal{E}_H$ is a (t, q_s, ϵ') fully secure* IBE*(in the random oracle model) for $\epsilon' = \epsilon \cdot q_H/(1 - q_S/2^n) \approx q_H \cdot \epsilon$, where q_H is the maximum number of oracle calls to H that the adversary can make.*

Next we rely on one time signature $\mathcal{S}$ and an IND-CCA2 secure symmetric encryption SE to achieve IND-ID-CCA2 security. The new identity based proxy re-encryption (Enhancing IBPRE) is as following:

Setup$(\mathbf{1^k})$. Same as Section 3 except choosing a collision resistant hash $H : \{0,1\}^* \to Z_n^*$ and another collision resistant hash $H_1 : G_T \to \mathcal{K}$ where $\mathcal{K}$ is the SE's key space.

KeyGen$(\mathbf{msk}, \mathsf{params}, \mathbf{ID})$. Same as Section 3 except replacing every ID by $H(ID)$.

Encrypt$(\mathbf{ID}, \mathsf{params}, \mathbf{M})$. Same as Section 3 except the encrypter also choose a one time signature scheme $\mathcal{S}$ and computes:

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

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

ReKeygen$(\mathbf{d_{ID}}, \mathbf{params}, \mathbf{ID'})$. Same as Section 4.1 except replacing every ID by $H(ID)$.

Reencrypt$(\mathbf{rk_{ID \to ID'}}, \mathbf{params}, \mathbf{C_{ID}}, \mathbf{ID'})$. First checking C_{ID}'s validity:

$$Verify(\sigma, svk) = Yes$$
$$e(g, C_5) = e(C_1, H(svk))$$

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

$$\widehat{C_{ID'}} = (\bar{C}_1, \bar{C}_2, \bar{C}_3, \bar{C}_4) = (C_1, C_2, \frac{e(g_2, C_3^{rk_1}) e(C_1, rk_3)}{e(C_2, rk_2)}, C_4)$$

Deccrypt$_2$ $(\mathbf{sk_{ID}}, \mathbf{params}, \mathbf{C_{ID}})$. Same as Section 3 except computing

$$K = H_1(\frac{e(C_2, d_2)}{e(g_2, C_3^{d_1}) e(C_1, d_3)})$$
$$M = SE.Dec(K, C_4)$$

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

Deccrypt$_1$ $(\mathbf{sk_{ID'}}, \mathbf{params}, \mathbf{C_{ID'}})$. Same as Section 4.1 except computing

$$K = H_1(\frac{e(\bar{C}_2, d_2')}{\bar{C}_3^{d_1'} e(\bar{C}_1, d_3')})$$
$$M = SE.Dec(K, \bar{C}_4)$$

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

4.3 Security Analysis

Theorem 4. *Suppose the ecDBDH assumption holds in the composite order group G, then our Enhancing* IBPRE *is* IND-ID-CCA2 *secure.*

Proof. The proof follows the IBE proof except this time the simulator needs to handle other following queries:

– *"$\mathcal{A}$ issues up to rekey generation queries on (ID, ID')".*
1. When $ID \neq ID^*$, the simulator $\mathcal{B}$ first simulates $\mathsf{KeyGen}(msk, \mathsf{params}, ID)$ as in the proof of our IBE 3.2 and gets sk_{ID}. Then it runs $\mathsf{ReKeygen}(sk_{ID}, \mathsf{params}, ID')$, and return the results $rk_{ID\rightarrow ID'}$ to the adversary.
2. When $ID = ID^*$, the simulator $\mathcal{B}$ adapt other technique to generate the re-encryption key. Surprisingly, the simulator can even generate the valid simulated private keys for ID^* as following, observe

$$d_1 = \frac{a+x}{aH(ID)+\alpha'-aH(ID^*)} + y \mod n$$
$$d_1' = \frac{a(-H(ID^*))+\alpha'+x'}{aH(ID)+\alpha'-aH(ID^*)} + y' \mod n$$

for $ID = ID^*$, if we let $x = k - a, x' = aID^* + k'$, we can get

$$d_1 = \frac{a+k-a}{aH(ID^*)+\alpha'-aH(ID^*)} + y = \frac{k}{\alpha'} + y \mod n$$
$$d_1' = \frac{a(-H(ID^*))+\alpha'+aH(ID^*)+k'}{aH(ID^*)+\alpha'-aH(ID^*)} + y' = \frac{\alpha'+k'}{\alpha'} + y \mod n$$

then $\mathcal{B}$ returns

$$d_1^{sim} = = \frac{k}{\alpha'} + y \mod n$$
$$d_1'^{sim} = = \frac{\alpha'+k'}{\alpha'} + y \mod n$$

as the simulated private keys for d_1, d_1'. Then we show $\mathcal{B}$ also can generate other private keys for $H(ID^*)$,

$$d_2^{sim} = g^x (g_1^{H(ID^*)} h)^y = g^{k-a} (g^{\alpha'})^y = \frac{g^k}{(g^a)} g^{\alpha' y}$$
$$d_3^{sim} = g^{t_3 x} (g_1^{H(ID^*)} h)^{t_3 y} = g^{t_3(k-a)} (g^{\alpha'})^{t_3 y} = g^{c(k-a)} (g^c)^{\alpha' y} = \frac{(g^c)^k}{g^{ac}} (g^c)^{\alpha' y}$$
$$d_2'^{sim} = g^{x'} (g_1^{H(ID^*)} h)^{y'} = g^{aH(ID^*)+k'} (g^{\alpha' y'}) = (g^a)^{H(ID^*)} g^{k'} g^{\alpha' y'}$$
$$d_3'^{sim} = g^{t_3 x'} (g_1^{H(ID^*)} h)^{t_3 y'} = (g^c)^{aH(ID^*)+k'} (g^{c\alpha'})^{y'} = (g^{ac})^{H(ID^*)} g^{k'} (g^c)^{\alpha' y'}$$

After $\mathcal{B}$ generates these simulated private keys for ID^*, it runs $\mathsf{ReKeygen}(sk_{ID^*}^{sim}, \mathsf{params}, ID')$, and returns the results $rk_{ID^*\rightarrow ID'}$ to the adversary.

– *"$\mathcal{A}$ issues up to re-encryption queries on (C_{ID}, ID, ID')".* The simulator $\mathcal{B}$ runs $\mathsf{Reencrypt}$ $(rk_{ID\rightarrow ID'}, C_{ID}, ID, ID')$ and returns the results to the adversary.

– *'$\mathcal{A}$ issues up to decryption queries on (C_{ID}, ID)".* The simulator $\mathcal{B}$ runs $\mathsf{Decrypt}_2(sk_{ID}, C_{ID})$ under the only condition $(C_{ID}, ID) \neq (C^*_{ID^*}, ID^*)$ and returns the results to the adversary.
– *'$\mathcal{A}$ issues up to decryption queries on $(\widehat{C_{ID'}}, ID')$".* The simulator $\mathcal{B}$ runs $\mathsf{Decrypt}_2(sk_{ID'}, \widehat{C_{ID'}})$ under the only condition $(\widehat{C_{ID'}}, ID') \neq Derivative(C^*_{ID^*}, ID^*)$ where $\mathsf{Derivative}$ defined in security notion for IBPRE 2.4, and returns the results to the adversary.

from Theorem 1 and the above analysis this theorem holds.

Theorem 5. *Suppose the ecDBDH assumption holds in the composite order group G, then our Enhancing* IBPRE *is master secret secure.*

Proof. Master secret security means that the proxy and the delegatee can not collude to get the delegator's private key. The re-encryption keys are

$$\begin{aligned} rk_1 &= \frac{(\alpha ID' + xID' + t_2 + x')}{\alpha ID + t_2} + yID' + y' + z \mod n \\ rk_2 &= g^{xID'+x'}(g_1^{ID}h)^{yID'+y'+z} \\ rk_3 &= g^{t_3(xID'+x')}(g_1^{ID}h)^{t_3(yID'+y'+z)} \end{aligned}$$

and the delegatee's private keys are

$$\begin{aligned} d_{ID'} &= (d^A_{ID'}, d^B_{ID'}, d^C_{ID'}) \\ d^A_{ID'} &= (d_{de1}, d_{de2}, d_{de3}) = (\frac{(\alpha + x_{de1})}{\alpha ID' + t_2} + y_{de1} \mod n, g^{x_{de1}}(g_1^{ID'}h)^{y_{de1}}, g^{t_3 x_{de1}}(g_1^{ID'}h)^{t_3 y_{de1}}) \\ d^B_{ID'} &= (d'_{de1}, d'_{de2}, d'_{de3}) = (\frac{(t_2 + x'_{de1})}{\alpha ID' + t_2} + y'_{de1} \mod n, g^{x'_{de1}}(g_1^{ID'}h)^{y'_{de1}}, g^{t_3 x'_{de1}}(g_1^{ID'}h)^{t_3 y'_{de1}}) \\ d^C_{ID'} &= d_{de4} = (g_1^{ID'}h)^{t_3} \end{aligned}$$

the re-encryption keys are independently with the delegatee's key. Any one can not get $d_1, d'_1, d_2, d'_2, d_3, d'_3$ from these keys. These facts even holds for $rk_{ID^* \to ID'}$ and $sk_{ID'}$ (ID' and the proxy are colluded). Thus our scheme can achieve *master secret secure.*

Theorem 6. *Suppose the ecDBDH assumption holds in the composite order group G, then our Enhancing* IBPRE *can withstand transferring of delegation attack.*

Proof. From the proof for Theorem 5, we know that the re-encryption keys are independently with the delegatee's key. That means, the delegatee can not give the proxy any help for extracting any information on the delegator's private key. But from

$$\begin{aligned} rk_1 &= \frac{(\alpha ID' + xID' + t_2 + x')}{\alpha ID + t_2} + yID' + y' + z \mod n \\ rk_2 &= g^{xID'+x'}(g_1^{ID}h)^{yID'+y'+z} \\ rk_3 &= g^{t_3(xID'+x')}(g_1^{ID}h)^{t_3(yID'+y'+z)} \end{aligned}$$

we can know that every re-encryption key have a randomness z, which make rk_1 is indistinguishable from a random element in Z_n, rk_2, rk_3 is indistinguishable from a random element in $\mathbb{G}$. That means, the proxy and the delegatee can not get any "implicit secret" of the delegator in our scheme, they can get only randomness. And "implicit secret" is the root for failing withstand transferring of delegation attack in all the previous PREs, so our scheme can withstand transferring of delegation attack.

Scheme	Security	W/O Random Oracle	Assumption	Master Secret Secure	Resist Trans-Dele-attack
GA07A[15]	IND-ID-CPA	Random Oracle	DBDH	✗	✗
GA07B[15]	IND-ID-CCA	Random Oracle	DBDH	✗	✗
M07B [23]	✗	Standard Model	DBDH	✗	✗
CT07[10]	IND-ID-CPA	Standard Model	DBDH	✗	✗
SXC08[28]	IND-ID-CCA	Standard Model	DBDH	✗	✗
LZD+10[20]	IND-ID-CCA	Standard Model	DBDH	✓	✗
WCW10[36]	IND-ID-CCA	Random Oracle	DBDH	✗	✗
LHC10[22]	IND-ID-CPA	Generic[4]	Generic[5]	✓	✗
OursA4.1	IND-sID-CPA	Standard Model	ecDBDH	✓	✓
OursB4.2	IND-ID-CCA	Standard Model	ecDBDH[6]	✓	✓

Table 1. IBPRE Security Comparison

Scheme	Enc	Check	Reenc	Dec		Ciph-Len	
				1ndCiph[7]	2ndCiph	1stCiph	2ndCiph
GA07A[15][8]	$1t_e + 1t_p$	0	$1t_p$	$2t_p$	$1t_p$	$2\|G\| + 2\|G_e\|$[9]	$1\|G\| + 1\|G_e\|$
GA07B[15]	$1t_p + 1t_e$	$2t_p$	$2t_e + 2t_p$	$1t_e + 2t_p$	$2t_e + 2t_p$	$1\|G\| + 1\|G_e\|$ $+2\|m\| + \|id\|$	$1\|G\| + 1\|G_T\|$ $+1\|G_e\| + \|m\|$
M07B [23]	$1t_p + 2t_e$	$2t_p$	$1t_p$	$2t_p$	$2t_p$	$2\|G_e\| + 1\|G_T\|$	$2\|G_e\| + 1\|G_T\|$
CT07[10]	$3t_e + 1t_p + 1t_s$	$1t_v$	$2t_e$	$2t_e + 10t_p + 1t_v$	$2t_e + 3t_p$	$9\|G\| + 2\|G_T\|$ $+\|vk\| + \|s\|$	$3\|G\| + \|G_T\|$ $+\|vk\| + \|s\|$
SXC08[28]	$3t_e + 1t_p + 1t_s$	$1t_v$	$2t_e + 1t_s$	$2t_e + 10t_p + 2t_v$	$2t_e + 3t_p + 1t_v$	$9\|G\| + 2\|G_T\|$ $+2\|vk\| + 2\|s\|$	$3\|G\| + \|G_T\|$ $+1\|vk\| + 1\|s\|$
OursA4.1	$1t_e + 2t_{me} + 1t_p$	0	$3t_p$	$2t_p + 1t_e$	$3t_p$	$2\|G_c\| + 2\|G_{cT}\|$	$3\|G_c\| + 1\|G_{cT}\|$
OursB4.2	$2t_e + 2t_{me}$ $+1t_s + 1t_{se}$	$1t_v + 2t_p$	$3t_p$	$2t_p + 1t_e$ $+1t_{sd} + 1t_{sv}$	$3t_p + 1t_{sd}$ $+1t_{sv}$	$2\|G_c\| + 1\|G_{cT}\|$ $+1\|SE\|$	$4\|G_c\| + 1\|s\|$ $+1\|SE\|$

Table 2. IBPRE Efficiency Comparison

[4] Luo et al.'s IBPRE scheme is a generic construction, therefore their scheme can be in random oracle and standard model.

[5] Luo et al.'s IBPRE scheme is a generic construction and the underlying assumption can be various.

[6] Actually, our IBPRE's security also rely on the underlying symmetric encryption scheme's IND-CCA2 security.

[7] Our first level ciphertext maps second level ciphertext and second level ciphertext maps first level ciphertext in [15,10,28].

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

[9] Sometimes in our schemes we use $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ or $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, in the former cases, $\mathbb{G}$ maps to $\mathbb{G}_e$, $\mathbb{G}_1$ maps $\mathbb{G}_T$, in the latter case, $\mathbb{G}_1$ maps to $\mathbb{G}_e$, $\mathbb{G}_T$ maps $\mathbb{G}_T$.

5 Comparison

In this section, we give our comparison results with other identity based proxy re-encryption schemes [15,10,23,28]. First we concern about schemes' security, then we concern about schemes' efficiency. Notations: In Table 1, we denote with/without random oracle as W/O Random Oracle, Resist Trans-Dele-attack means resisting transferring of delegation attack. In Table 2, we denote encryption as Enc, re-encryption as Reenc, decryption as Dec, ciphertext as Ciph and ciphertext length as Ciph-Len, t_p, t_e and t_{me} represent the computational cost of a bilinear pairing, an exponentiation and a multi-exponentiation respectively. 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_{s} and t_{v} represent the computational cost of a one-time signature signing and verification respectively. $|\mathbb{G}_c|$, $|\mathbb{G}_{cT}|$, $|\mathbb{G}|$ and $|\mathbb{G}_T|$ denote the bit-length of an element in groups $\mathbb{G}_c$, $\mathbb{G}_{cT}$, $\mathbb{G}$ and $\mathbb{G}_T$ respectively. Here $\mathbb{G}_c$ and $\mathbb{G}_{cT}$ denote the composite order bilinear groups used in our scheme, while $\mathbb{G}_e$ and $\mathbb{G}_T$ are the prime order bilinear groups used in GA07, CT07, SXC08 schemes, i.e., the bilinear pairing is $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. $|SE|$ 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 IBPRE advance the previous results on IBPRE both on security and efficiency.

6 Conclusion

In this paper, we propose a new identity based encryption which does not lie in the three frameworks proposed by Boyen [7]. The main novelty is the way we embed the $\mathsf{master-key}$ in the private key, we embed it in the plain form instead of exponential form. Based on this new IBE, we propose a new IBPRE which is efficient, master secret secure and resisting transferring delegation attack. However, we note our IBPRE is only single-hop, it is an interesting work to construct a multi-hop IBPRE in our way.

Acknowledgment

Dr. Jun Shao has joined us on this work during the early stage of this paper. The authors would like to express their gratitude thanks to him for his generous help. This work is supported by the National Natural Science Foundation of China under contract no. 60842006, Natural Science Foundation of Shaanxi Province and Natural Science Foundation of Engineering College 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, International Journal of Applied Cryptography, Vol.1, No.1, pp. 3–20.
8. R. Canetti, S. Halevi, and J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 207–222, 2004.
9. 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`.
10. C. Chu and W. Tzeng. Identity-based proxy re-encryption without random oracles. In *ISC 2007*, volume 4779 of *LNCS*, pages 189–202, 2007.
11. 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.
12. C. Cocks. An identity based encryption scheme based on quadratic residues. In *IMACC'01*, volume 2260 of *LNCS*,pages 360–363, 2001.
13. 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.
14. Y. Dodis and A. Ivan. Proxy cryptography revisited. In Internet Society (ISOC): NDSS 2003, 2003.
15. M. Green and G. Ateniese. Identity-based proxy re-encryption. In *ACNS 2007*, volume 4521 of *LNCS*, pages 288–306, 2007.
16. C. Gentry. Practical identity-based encryption without random oracles. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464, 2006.
17. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC 2008*, pages 197–206, 2008.
18. M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In *PKC 1999*, volume 1560 of *LNCS*, pages 112–121, 1999.
19. 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.
20. 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.
21. 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/`.
22. S. Luo, J. Hu and Z. Chen. New construction of identity-based proxy re-encryption. Cryptology ePrint Archive, Report 2010/444, 2010.
23. T. Matsuo. Proxy re-encryption systems for identity-based encryption. In *PAIRING 2007*, volume 4575 of *LNCS*, pages 247–267, 2007.
24. L. Martin(editor). P1363.3(TM)/D1, Draft standard for identity-based public cryptography using pairings, May 2008.
25. M. Naor. On cryptographic assumptions and challenges. In *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109, 2003.
26. J. Shao and Z. Cao. CCA-secure proxy re-encryption without pairing. In *PKC 2009*, volume 5443 of *LNCS*, pages 357–376, 2009.
27. 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.
28. J. Shao, D. Xing and Z. Cao. Identity-based proxy rencryption schemes with multiuse, unidirection and CCA security. Cryptology ePrint Archive: `http://eprint.iacr.org/2008/103.pdf`.
29. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairings. In *Symposiumon Cryptography and Information Security-SCIS 2000*, Japan.
30. R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive: `http://eprint.iacr.org/2003/054.pdf`.
31. A. Shamir. Identity-based cryptosystems and signature Schemes. In *CRYPTO 1984*, volume 196 of *LNCS*, pages 47–53, 1984.
32. 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.
33. Q. Tang. Type-based proxy re-encryption and its construction. In *INDOCRYPT 2008*, volume 5365 of *LNCS*, pages 130–144, 2008.

34. B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127, 2005.
35. 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.
36. 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.
37. X. 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.

A Correctness for Our IBE

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

B Correctness for Our IBPRE

Actually the re-encryption keys are

$$rk_1 = \frac{(\alpha ID' + x ID' + t_2 + x')}{\alpha ID + t_2} + y ID' + y' + z \mod n$$
$$rk_2 = g^{x ID' + x'} (g_1^{ID} h)^{y ID' + y' + z}$$
$$rk_3 = g^{t_3 (x ID' + x')} (g_1^{ID} h)^{t_3 (y ID' + y' + z)}$$

Thus we get

$$\bar{C_3} = \frac{e(g_2, C_3^{rk_1}) e(C_1, rk_3)}{e(C_2, rk_2)}$$
$$= \frac{e(g_2, ((g_1^{ID} h)^r)^{\frac{(\alpha ID' + k_1 q ID' + x ID' + t_2 + x' + k_2 q)}{\alpha ID + t_2} + y ID' + y' + z}) e(g^r, g^{t_3 (x ID' + x')} (g_1^{ID} h)^{t_3 (y ID' + y' + z)})}{e((g_2 g_3)^r, g^{x ID' + x'} (g_1^{ID} h)^{y ID' + y' + z})}$$
$$= \frac{e(g_2, ((g_1^{ID} h)^r)^{\frac{(\alpha ID' + k_1 q ID' + x ID' + t_2 + x' + k_2 q)}{\alpha ID + t_2} + y ID' + y' + z})}{e(g_2^r, g^{x ID' + x'} (g_1^{ID} h)^{y ID' + y' + z})}$$
$$= e(g_2, (g_1^{ID'} h)^r)$$

Let $\widehat{C_3} = (g_1^{ID'} h)^r$, from the Decrypt algorithm of our IBE, we can get

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