Lai JZ, Zhu WT, Deng RH *et al.* New constructions for identity-based unidirectional proxy re-encryption. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 25(4): 793–806 July 2010. DOI 10.1007/s11390-010-1062-y

New Constructions for Identity-Based Unidirectional Proxy Re-Encryption

Jun-Zuo Lai[1,3] (赖俊祚), Wen-Tao Zhu[2,3] (朱文涛), *Member*, *IEEE*
Robert H. Deng[3,*] (邓慧杰), *Senior Member*, *IEEE*, Sheng-Li Liu[1] (刘胜利), and Wei-Dong Kou[4] (寇卫东)

[1] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, China*

[2] *State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049, China*

[3] *School of Information Systems, Singapore Management University, Singapore 178902*

[4] *School of Computer Science and Technology, Xidian University, Xi'an 710071, China*

E-mail: {laijunzuo, slliu}@sjtu.edu.cn; wtzhu@ieee.org; robertdeng@smu.edu.sg; kou_weidong@yahoo.com.cn

Received August 17, 2009; revised March 13, 2010.

Abstract We address the cryptographic topic of proxy re-encryption (PRE), which is a special public-key cryptosystem. A PRE scheme allows a special entity, known as the proxy, to transform a message encrypted with the public key of a delegator (say Alice), into a new ciphertext that is protected under the public key of a delegatee (say Bob), and thus the same message can then be recovered with Bob's private key. In this paper, in the identity-based setting, we first investigate the relationship between so called mediated encryption and unidirectional PRE. We provide a general framework which converts any secure identity-based unidirectional PRE scheme into a secure identity-based mediated encryption scheme, and vice versa. Concerning the security for unidirectional PRE schemes, Ateniese *et al.* previously suggested an important property known as the master secret security, which requires that the coalition of the proxy and Bob cannot expose Alice's private key. In this paper, we extend the notion to the identity-based setting, and present an identity-based unidirectional PRE scheme, which not only is provably secure against the chosen ciphertext attack in the standard model but also achieves the master secret security at the same time.

Keywords identity-based encryption (IBE), unidirectional proxy re-encryption, mediated encryption (mE), chosen ciphertext attack (CCA), master secret security (MSS).

1 Introduction

In this paper, we are concerned with the identity-based encryption (IBE), a special kind of public-key cryptosystem where any user's public key can be directly derived from his unique identifier like his user name or email address. The concept of IBE was first proposed by Shamir in 1984[1] as an effort to reduce the operation requirement on the public key infrastructure (PKI). By mapping a well-known and unique aspect of a client's identity to his public key, IBE simplifies the system management, as the certification involved in the traditional PKI now becomes implicit. That is, a message sender no longer needs to check whether the intended recipient is certified or not; instead, prior to decryption, the recipient must identify himself to a trusted authority for a designated private key corresponding to his identity.

Since the pioneering work[1], identity-based cryptography has received more and more research interest. Many IBE schemes have been proposed[2-7], but a noticeable problem lies in that none of them can provide an efficient solution to user identity revocation. In such an identity-based setting, we respectively introduce two related topics of particular interest in this paper: mediated encryption (mE) and proxy re-encryption (PRE). The relationship between the involved cryptographic domains is illustrated in Fig.1.

1.1 Identity-Based Mediated Encryption

Mediated Encryption. In the conventional PKI, efficient revocation of public key certificates has been a non-trivial task. In 2001, Boneh *et al.*[8] introduced mediated cryptography as an approach to instantaneous revocation of public keys. The basic idea is to employ

Regular Paper
This work is partially supported by the National Natural Science Foundation of China under Grant No. 60873229 and Shanghai Rising-Star Program under Grant No. 09QA1403000, and the Office of Research, Singapore Management University.

*Corresponding Author

an online semi-trusted mediator (SEM) to provide the security control for transactions. Once the SEM is notified that a user's key is to be revoked, its use can be immediately banned. Particularly, the proposed mRSA[8] is a simple and practical method of splitting an RSA private key between the user and an SEM, which enables fast and fine-grained control of users' security privileges. Their idea of mediated cryptography[8] has then motivated research on mediated IBE briefly reviewed as follows.

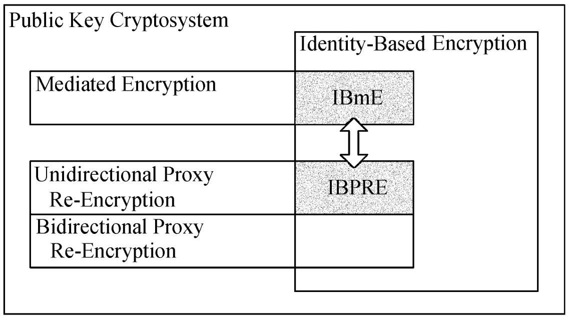
Public Key Cryptosystem
Identity-Based Encryption
Mediated Encryption
IBmE
Unidirectional Proxy Re-Encryption
IBPRE
Bidirectional Proxy Re-Encryption

Fig.1. Relationship between identity-based mediated encryption and identity-based unidirectional proxy re-encryption.

Identity-Based Mediated Encryption. In the literature, many IBE schemes[2-7] have been proposed, but none of them provides an efficient solution to identity revocation. Since IBE eliminates the use of traditional public key certificates (which have been employed to indicate the validity of the corresponding keys), no revocation of user identities inherently implies no revocation of user keys, which may be understood as an undesirable drawback of the identity-based cryptography compared with the traditional PKI solution.

Concerning the fact that mRSA[8] still relies on conventional certificates to store and communicate public keys, Ding and Tsudik[9] transformed mRSA into an identity-based mediated RSA (IB-mRSA) scheme[9], which is an initiative towards addressing the challenge of user key revocation in IBE. Although IB-mRSA offers remarkable performance and practicality, a common RSA modulus is shared among all users in the system. As a result, to guarantee the security of IB-mRSA, the private key of the SEM has to be well protected throughout the entire system lifetime, which seems a bit too risky since the SEM in nature is only a semi-trusted mediator.

Later, based on an IBE scheme proposed by Boneh and Franklin[2], Libert and Quisquater proposed a new mediated IBE scheme[10]. Although the scheme[10] does not exhibit the critical security dependence observed in Ding and Tsudik's IB-mRSA[9], it turns out to be vulnerable to the chosen ciphertext attack (CCA) by an inner adversary (i.e., a malicious client who possesses the user part of the private key). In other words, the system security is still highly dependent; compared to IB-mRSA[9], the prohibitive trust is just shifted from the mediator side to the user side.

Recently, Baek and Zheng[11] presented yet another mediated IBE scheme, which is secure against the chosen ciphertext attack in the random oracle model[12] but in a strong sense, that is, secure against CCA even conducted by an attacker who has obtained the user part of a private key.

1.2 Identity-Based Proxy Re-Encryption

Proxy Re-Encryption. In 1998, Blaze, Bleumer, and Strauss[13] introduced the concept of proxy re-encryption (PRE), in which a semi-trusted entity known as the proxy, not necessarily knowing the underlying plaintext message, converts a ciphertext intended for Alice into another ciphertext intended for Bob. They also proposed the first proxy re-encryption scheme, which we shall refer to as the BBS scheme.

A PRE scheme may be either bidirectional (i.e., two-way) or unidirectional (i.e., one-way). The underlying construction in the BBS scheme[13] falls into the former case: the cryptographic information for transforming the ciphertext from for Alice to for Bob can also be employed to transform the ciphertext from for Bob to for Alice. However, in reality, the latter (i.e., one-way) case may be more desired, where Alice clearly plays the role of the delegator and Bob plays the exact role of the delegatee, but not vice versa. Such a unidirectional case is considered in this paper, and for brevity we only refer to "PRE" when it is obvious to see from the context that we are referring to the unidirectional case.

Concerning the security for unidirectional PRE schemes, in [14] Ateniese *et al.* defined an important security requirement. This notion, termed master secret security (MSS), demands that even the coalition of the proxy and the delegatee should not be able to expose the private key of the corresponding delegator. Later we shall show that it is possible to export the concept of MSS to the identity-based setting.

In [14], Ateniese *et al.* also showed the first examples of unidirectional PRE schemes based on pairings. They are only resilient to the chosen plaintext attack (CPA), and thus may not be sufficiently secure for practical applications. Canetti and Hohenberger[15] proposed the definition of CCA security for PRE schemes, and demonstrated a scheme that satisfies the definition. However, just like the BBS scheme[13], their CCA-secure PRE scheme is bidirectional. Libert and Vergnaud[16] generalized Canetti and Hohenberger's work[15], and proposed the first construction of unidirectional PRE scheme that is CCA-secure in the standard model. More recently, there have been efforts on how to construct a secure PRE scheme without using pairings[17-18].

Identity-Based Proxy Re-Encryption. In [19], Green and Ateniese addressed the topic of identity-based PRE. Based on Boneh and Franklin's IBE scheme[2], they proposed the first identity-based unidirectional PRE scheme, which is secure in the random oracle model[12]. Then, Chu and Tzeng[20] proposed an identity-based unidirectional PRE scheme without random oracles. Unfortunately, Shao *et al.*[21] recently revealed a security flaw in the proposal[20], and an improvement was also proposed.

This work has also been motivated by existent research on PRE outside the identity-based setting. For example, some[14] are unidirectional but only CPA-secure, while [15] is CCA-secure but bidirectional. Therefore, one of our incentives is to construct a concrete PRE scheme similar to [16] that is both unidirectional and CCA-secure, but in the identity-based setting. In addition, we make an effort to achieve the precious MSS property[14] at the same time.

1.3 Contributions and Paper Organization

In this paper, we present two new constructions for identity-based unidirectional proxy re-encryption, a general one and a concrete one, both provably secure. Therefore, our technical contributions are two-fold:

- First, we investigate the relationship between identity-based mediated encryption (IBmE) and identity-based unidirectional PRE (IBPRE). We provide a general framework for protocol conversion, in which a secure IBmE scheme can be constructed from any secure IBPRE scheme, and vice versa (as depicted in Fig.1). The conversion itself works in the standard model.
- We then propose the model of master secret security[14] for IBPRE schemes. All existent IBPRE schemes[19-20], plus the ones constructed from IBmE schemes following our general conversion, do not obtain this MSS property. Nevertheless, we show it is possible to achieve the property by presenting a concrete IBPRE scheme, which is also CCA-secure in the standard model.

The rest of the paper is organized as follows. Section 2 presents necessary backgrounds like formalized descriptions; readers familiar with a certain topic can skip the corresponding subsection. Our general framework for mutual IBmE-IBPRE conversion and the corresponding security proofs are presented in Section 3. A CCA-secure identity-based unidirectional PRE scheme with master secret security is proposed in Section 4. Finally, we conclude this work in Section 5, where an open problem is also presented.

2 Preliminaries

2.1 Pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic multiplicative groups of the same prime order p. A (symmetric) pairing is a function $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties:

- Bilinearity: $\forall g_1, g_2 \in \mathbb{G}$, $\forall a, b \in \mathbb{Z}_p$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$;
- Non-degeneracy: if g_1 and g_2 are both generators in $\mathbb{G}$, then $e(g_1, g_2)$ generates $\mathbb{G}_T$;
- Computability: there exists an efficient algorithm to compute $e(g_1, g_2)$ for $\forall g_1, g_2 \in \mathbb{G}$.

The cryptographic pairing is actually a special kind of mapping mathematically known as the bilinear map. In Subsection 4.1, we shall employ a pairing group system $\langle p, \mathbb{G}, \mathbb{G}_T, e\rangle$ to construct a concrete IBPRE scheme, whose two security properties shall be formally proved in Subsection 4.2 based on two basic cryptographic assumptions, respectively. Next, we introduce the two assumptions.

2.2 Decisional Bilinear Diffie-Hellman (DBDH) Assumption

Following the above notions, let $g \in \mathbb{G}$ be a generator. Given five elements $g, g^a, g^b, g^c \in \mathbb{G}$, and $e(g, g)^z \in \mathbb{G}_T$, where the four secret exponents a, b, c, z are uniformly and randomly selected from $\mathbb{Z}_p^*$, a fair binary coin $\beta \in \{0, 1\}$ is flipped to generate a tuple $\mathcal{T}_\beta = (g, g^a, g^b, g^c, T)$: if $\beta = 1$, output $\mathcal{T}_{\beta=1}$ where $T = e(g, g)^{abc}$; otherwise, output $\mathcal{T}_{\beta=0}$ where $T = e(g, g)^z$. The Decisional Bilinear Diffie-Hellman (DBDH) problem is to guess the value of β from $\mathcal{T}_\beta$.

Assume $\mathcal{A}$ is an algorithm (interchangeably, an adversary) for guessing β. We say $\mathcal{A}$ has at least an advantage of ϵ in solving the DBDH problem if

$$| \Pr[\mathcal{A}(\mathcal{T}_{\beta=1}) = 1] - \Pr[\mathcal{A}(\mathcal{T}_{\beta=0}) = 1] | \geqslant \epsilon,$$

where both probabilities are computed with respect to uniformly and randomly chosen a, b, c, z and the random bits consumed by $\mathcal{A}$.

Definition 1 (DBDH Assumption). *We say that the (t, ϵ)-DBDH assumption holds in a group $\mathbb{G}$ if no algorithm running in the time of at most t can solve the DBDH problem in $\mathbb{G}$ with an advantage of at least ϵ.*

2.3 Computational Diffie-Hellman (CDH) Assumption

Let $\mathbb{G}$ be a multiplicative group of a prime order p, and g be its generator. Given the tuple (g, g^a, g^b) for random $a, b \in \mathbb{Z}_p^*$, the Computational Diffie-Hellman (CDH) problem in group $\mathbb{G}$ is to compute g^{ab}.

We say an adversary $\mathcal{A}$ has at least an advantage of ϵ in solving the CDH problem if

$$\mathsf{Pr}[\mathcal{A}(g, g^a, g^b) = g^{ab}] \geqslant \epsilon,$$

where the probability is computed with respect to randomly chosen a, b and the random bits consumed by $\mathcal{A}$.

Definition 2 (CDH Assumption). *We say that the (t, ϵ)-CDH assumption holds in a group $\mathbb{G}$ if no algorithm running in the time of at most t can solve the CDH problem in $\mathbb{G}$ with an advantage of at least ϵ.*

2.4 Identity-Based Mediated Encryption

An identity-based mediated encryption (IBmE) scheme is a tuple of algorithms described as follows:

$\mathsf{Setup}(\lambda)$: Taking as input a security parameter λ, it outputs a public key PK and a master secret key MSK.

$\mathsf{Extract}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID})$: Taking as input PK, the master secret key MSK, and an identity ID, it outputs a private key d_{ID}.

$\mathsf{DistributeKey}(\mathsf{PK}, \mathsf{ID}, d_{\mathsf{ID}})$: Taking as input PK, an identity ID, and the private key d_{ID}, it outputs the SEM-part private key $d_{\mathsf{ID},\mathrm{sem}}$ and the user-part private key $d_{\mathsf{ID},\mathrm{user}}$. Note that the algorithm should be a *random* one.

$\mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}, m)$: Taking as input PK, an identity ID, and a message m, it outputs a ciphertext C.

$\mathsf{SEMDecrypt}(\mathsf{PK}, C, \mathsf{ID}, d_{\mathsf{ID},\mathrm{sem}})$: Taking as input PK, a ciphertext C, an identity ID, and the SEM's private key $d_{\mathsf{ID},\mathrm{sem}}$, it outputs the SEM's decryption share $\delta_{C,\mathsf{ID},\mathrm{sem}}$ or an error symbol $\perp$.

$\mathsf{UserDecrypt}(\mathsf{PK}, C, \mathsf{ID}, d_{\mathsf{ID},\mathrm{user}}, \delta_{C,\mathsf{ID},\mathrm{sem}})$: Taking as input PK, a ciphertext C, an identity ID, the user's private key $d_{\mathsf{ID},\mathrm{user}}$, and the SEM's decryption share $\delta_{C,\mathsf{ID},\mathrm{sem}}$, it outputs a message m or $\perp$. This algorithm should check the validity of the SEM's decryption share before the decryption.

$\mathsf{Decrypt}(\mathsf{PK}, C, \mathsf{ID}, d_{\mathsf{ID}})$: Taking as input PK, a ciphertext C, an identity ID, and the private key d_{ID}, it outputs a message m or $\perp$.

All IBmE schemes should satisfy the correctness condition that decryption "undoes" encryption. The $\mathsf{IND\text{-}ID\text{-}CCA}$ security for IBmE is defined with the following game between an attack algorithm $\mathcal{A}$ and a challenger.

Setup. The challenger runs $\mathsf{Setup}(\lambda)$ to obtain a public key PK and gives it to the adversary.

Query Phase 1. The adversary $\mathcal{A}$ adaptively issues:

• Extraction query, on input an identity ID: the challenger forwards the corresponding private key d_{ID} to the adversary.

• SEMKeyExtraction query, on input an identity ID: the challenger runs the $\mathsf{Extract}$ and $\mathsf{DistributeKey}$ algorithms to obtain the SEM-part private key $d_{\mathsf{ID},\mathrm{sem}}$ and sends it to the adversary.

• UserKeyExtraction query, on input an identity ID: the challenger runs the $\mathsf{Extract}$ and $\mathsf{DistributeKey}$ algorithms to obtain the user-part private key $d_{\mathsf{ID},\mathrm{user}}$ and sends it to the adversary.

• SEMDecryption query, on input an identity ID and a ciphertext C: the challenger runs the $\mathsf{SEMDecrypt}$ algorithm, and forwards the partial decryption result to the adversary.

• UserDecryption query, on input an identity ID, a ciphertext C, and the SEM's decryption share $\delta_{C,\mathsf{ID},\mathrm{sem}}$: the challenger runs the $\mathsf{UserDecrypt}$ algorithm, and forwards the result to the adversary.

• Decryption query, on input an identity ID and a ciphertext C: the challenger runs the $\mathsf{Decrypt}$ algorithm, and forwards the result to the adversary.

Challenge. The adversary $\mathcal{A}$ selects two plaintexts (m_0, m_1) of equal length, and a target identity ID^* for which their's is the natural constraint that neither of the following queries has ever been made in Query phase 1:

1) Extraction(ID^*),

2) SEMKeyExtraction(ID^*) and UserKeyExtraction(ID^*).

The challenger then chooses $\beta \xleftarrow{R} \{0, 1\}$, sets $C^* \leftarrow \mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}^*, m_\beta)$, and gives the target ciphertext C^* to $\mathcal{A}$.

Query Phase 2. The adversary continues to adaptively issue queries as specified in Phase 1, but none of the following is allowed:

1) Extraction(ID^*),

2) Decryption(ID^*, C^*),

3) SEMKeyExtraction(ID^*) and UserKeyExtraction(ID^*),

4) UserDecryption(ID^*, C^*, SEMDecryption(ID^*, C^*)).

Guess. The adversary $\mathcal{A}$ outputs its guess $\beta' \in \{0, 1\}$ for β, and wins the game if $\beta = \beta'$.

We define $\mathcal{A}$'s advantage in attacking the identity-based mediated encryption system IBmE with parameter λ as

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IBmE}(\lambda)} = \left|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}\right|.$$

Definition 3. *We say that an identity-based mediated encryption scheme IBmE is $(t, q_e, q_{e,\mathrm{user}}, q_{e,\mathrm{sem}}, q_{d,\mathrm{user}}, q_{d,\mathrm{sem}}, q_d, \epsilon)$-$\mathsf{IND\text{-}ID\text{-}CCA}$ secure, if for any t-time algorithm $\mathcal{A}$ who makes in all q_e Extraction, $q_{e,\mathrm{sem}}$ SEMKeyExtraction, $q_{e,\mathrm{user}}$ UserKeyExtraction, $q_{d,\mathrm{sem}}$ SEMDecryption, $q_{d,\mathrm{user}}$ UserDecryption, and q_d Decryption queries, we have that $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IBmE}(\lambda)}$ is at most ϵ.*

2.5 Identity-Based Unidirectional Proxy Re-Encryption

An identity-based unidirectional proxy re-encryption (IBPRE) scheme is a tuple of algorithms described as follows:

$\mathsf{Setup}(\lambda)$: Taking as input a security parameter λ, it outputs a public key PK and a master secret key MSK.

$\mathsf{Extract}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID})$: Taking as input PK, the master secret key MSK, and a user identity ID, it outputs a user private key d_{ID}.

$\mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}, m)$: Taking as input PK, an identity ID, and a message m, it outputs a ciphertext C.

$\mathsf{RKGen}(\mathsf{PK}, \mathsf{ID}_1, d_{\mathsf{ID}_1}, \mathsf{ID}_2)$: Taking as input PK, two identities $\mathsf{ID}_1, \mathsf{ID}_2$, and the private key d_{ID_1} of ID_1, it outputs a re-encryption key $d_{\mathsf{ID}_1 \to \mathsf{ID}_2}$.

$\mathsf{ReEncrypt}(\mathsf{PK}, d_{\mathsf{ID}_1 \to \mathsf{ID}_2}, C_{\mathsf{ID}_1})$: Taking as input PK, a re-encryption key $d_{\mathsf{ID}_1 \to \mathsf{ID}_2}$, and a ciphertext C_{ID_1}, it outputs a second (i.e., the re-encrypted) ciphertext C_{ID_2} or an error symbol $\perp$.

$\mathsf{Decrypt}(\mathsf{PK}, C_{\mathsf{ID}_2}, \mathsf{ID}_2, d_{\mathsf{ID}_2})$: Taking as input PK, a ciphertext C_{ID_2}, an identity ID_2, and his private key d_{ID_2}, it outputs a message m or $\perp$.

All IBPRE schemes should satisfy the correctness condition that decryption "undoes" encryption. The $\mathsf{IND\text{-}ID\text{-}CCA}$ security for IBPRE is defined with the following game between an attack algorithm $\mathcal{A}$ and a challenger.

Setup. The challenger runs $\mathsf{Setup}(\lambda)$ to obtain a public key PK and gives it to the adversary.

Query Phase 1. The adversary $\mathcal{A}$ adaptively issues:

- Extraction query, on input an identity ID: the challenger forwards the corresponding private key d_{ID} to the adversary.
- RKGeneration query, on input two identities $\mathsf{ID}_1, \mathsf{ID}_2$: the challenger runs the RKGen algorithm to obtain the re-encryption key $d_{\mathsf{ID}_1 \to \mathsf{ID}_2}$ and sends it to the adversary.
- ReEncryption query, on input two identities $\mathsf{ID}_1, \mathsf{ID}_2$ and a ciphertext C_{ID_1}: the challenger runs the $\mathsf{ReEncrypt}$ algorithm, and sends the re-encrypted ciphertext C_{ID_2} to the adversary.
- Decryption query, on input an identity ID and a ciphertext C: the challenger runs the $\mathsf{Decrypt}$ algorithm, and forwards the result to the adversary.

Challenge. The adversary $\mathcal{A}$ selects two plaintexts (m_0, m_1) of equal length, and a target identity ID^* for which there is the natural constraint that neither of the following queries has ever been made in Query Phase 1:

1) Extraction(ID^*),
2) RKGeneration($\mathsf{ID}^*, \mathsf{ID}'$) and Extraction($\mathsf{ID}'$) for any identity ID'.

Note that the above constraint in itself is recursive, as the second item is actually an indirect form of the first one. Particularly, if the adversary can somehow compute the private key of ID' (for example, by enquiring both RKGeneration($\mathsf{ID}', \mathsf{ID}''$) and Extraction($\mathsf{ID}''$) for some ID''), the adversary is still regarded to have enquired Extraction(ID') (and thus is not allowed to further make the query RKGeneration($\mathsf{ID}^*, \mathsf{ID}'$)).

The challenger then chooses $\beta \xleftarrow{R} \{0,1\}$, sets $C^* \leftarrow \mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}^*, m_\beta)$, and gives the target ciphertext C^* to $\mathcal{A}$.

Query Phase 2. The adversary continues to adaptively issue queries as specified in Phase 1, but none of the following is allowed:

1) Extraction(ID^*),
2) Decryption(ID^*, C^*),
3) RKGeneration($\mathsf{ID}^*, \mathsf{ID}'$) and Extraction($\mathsf{ID}'$) for any identity ID',
4) ReEncryption($\mathsf{ID}^*, \mathsf{ID}', C^*$) and Extraction($\mathsf{ID}'$) for any identity ID',
5) Decryption(ID', ReEncryption($\mathsf{ID}^*, \mathsf{ID}', C^*$)) for any identity ID'.

Guess. The adversary $\mathcal{A}$ outputs its guess $\beta' \in \{0,1\}$ for β and wins the game if $\beta = \beta'$.

We define $\mathcal{A}$'s advantage in attacking the identity-based proxy re-encryption system IBPRE with parameter λ as

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IBPRE}(\lambda)} = \left|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}\right|.$$

Definition 4. *We say that an identity-based proxy re-encryption scheme* IBPRE *is* $(t, q_e, q_{rk}, q_{re}, q_d, \epsilon)$-$\mathsf{IND\text{-}ID\text{-}CCA}$ *secure, if for any* t*-time algorithm* $\mathcal{A}$ *who makes in all* q_e *Extraction,* q_{rk} *RKGeneration,* q_{re} *ReEncryption, and* q_d *Decryption queries, we have that* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IBPRE}(\lambda)}$ *is at most* ϵ.

The master secret security (MSS) property that we imported to IBPRE, which is not necessarily implied by the above $\mathsf{IND\text{-}ID\text{-}CCA}$ security, is defined with the following game between an attack algorithm $\mathcal{A}$ and a challenger.

Setup. The challenger runs $\mathsf{Setup}(\lambda)$ to obtain a public key PK and gives it to the adversary.

Query Phase. The adversary $\mathcal{A}$ adaptively issues:

- Extraction query, on input an identity ID: the challenger forwards the corresponding private key d_{ID} to the adversary.
- RKGeneration query, on input two identities $\mathsf{ID}_1, \mathsf{ID}_2$: the challenger runs the RKGen algorithm to obtain the re-encryption key $d_{\mathsf{ID}_1 \to \mathsf{ID}_2}$ and sends it to the adversary.

Output. The adversary $\mathcal{A}$ outputs an identity ID^* and a working private key d_{ID^*}. The adversary *succeeds* if he has made no Extraction query on ID^*.

The advantage of the adversary $\mathcal{A}$ in the above game is defined as

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IBPRE-MSS}} = \mathsf{Pr}[\mathcal{A}\ \textit{succeeds}].$$

Definition 5. *An identity-based unidirectional proxy re-encryption scheme* IBPRE *is $(t, q_e, q_{rk}, \epsilon)$-master secret secure, if for any t-time algorithm $\mathcal{A}$ who makes in all q_e Extraction and q_{rk} RKGeneration queries, we have that $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IBPRE-MSS}}$ is at most ϵ.*

3 General Framework for Mutual Conversion

Our general framework for mutual IBmE-IBPRE conversion transforms a secure identity-based unidirectional PRE scheme into a secure identity-based mediated encryption scheme, and vice versa. We now present the two conversions respectively.

3.1 From IBPRE to IBmE

Suppose that Π^{IBPRE} is an IBPRE scheme with algorithms Setup, Extract, Encrypt, RKGen, ReEncrypt and Decrypt. We can construct an IBmE scheme Π^{IBmE} by defining the corresponding IBmE algorithms as specified in Subsection 2.4.

$\mathsf{IBmE.Setup}(\lambda)$. For security parameter λ, run $(\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{IBPRE.Setup}(\lambda)$. Let PK be the public key and MSK be the master secret key.

$\mathsf{IBmE.Extract}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID})$. Given PK, MSK, and an identity ID, run

$$d_{\mathsf{ID}\|0} \leftarrow \mathsf{IBPRE.Extract}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID}\|0),$$
$$d_{\mathsf{ID}\|1} \leftarrow \mathsf{IBPRE.Extract}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID}\|1).$$

Set the private key $d_{\mathsf{ID}} = (d_{\mathsf{ID}\|0}, d_{\mathsf{ID}\|1})$.

$\mathsf{IBmE.DistributeKey}(\mathsf{PK}, \mathsf{ID}, d_{\mathsf{ID}})$. Given PK, an identity ID and the private key $d_{\mathsf{ID}} = (d_{\mathsf{ID}\|0}, d_{\mathsf{ID}\|1})$, run

$$d_{\mathsf{ID}\|0\to\mathsf{ID}\|1} \leftarrow \mathsf{IBPRE.RKGen}(\mathsf{PK}, \mathsf{ID}\|0, d_{\mathsf{ID}\|0}, \mathsf{ID}\|1).$$

Set the SEM's and user's private keys $d_{\mathsf{ID},\text{sem}} = d_{\mathsf{ID}\|0\to\mathsf{ID}\|1}$, $d_{\mathsf{ID},\text{user}} = d_{\mathsf{ID}\|1}$.

$\mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}, m)$. Given PK, an identity ID, and a message m, generate the ciphertext $C \leftarrow \mathsf{IBPRE.Encrypt}(\mathsf{PK}, \mathsf{ID}\|0, m)$.

$\mathsf{IBmE.SEMDecrypt}(\mathsf{PK}, C, \mathsf{ID}, d_{\mathsf{ID},\text{sem}})$. Given PK, a ciphertext C, an identity ID, and the SEM's private key $d_{\mathsf{ID},\text{sem}} = d_{\mathsf{ID}\|0\to\mathsf{ID}\|1}$, run

$$C_{\mathsf{ID}\|1} \leftarrow \mathsf{IBPRE.ReEncrypt}(\mathsf{PK}, d_{\mathsf{ID}\|0\to\mathsf{ID}\|1}, C).$$

Set the SEM's decryption share $\delta_{C,\mathsf{ID},\text{sem}} = C_{\mathsf{ID}\|1}$.

$\mathsf{IBmE.UserDecrypt}(\mathsf{PK}, C, \mathsf{ID}, d_{\mathsf{ID},\text{user}}, \delta_{C,\mathsf{ID},\text{sem}})$. Given PK, a ciphertext C, an identity ID, the user's private key $d_{\mathsf{ID},\text{user}} = d_{\mathsf{ID}\|1}$, and the SEM's decryption share $\delta_{C,\mathsf{ID},\text{sem}} = C_{\mathsf{ID}\|1}$, set

$$m \leftarrow \mathsf{IBPRE.Decrypt}(\mathsf{PK}, C_{\mathsf{ID}\|1}, \mathsf{ID}\|1, d_{\mathsf{ID}\|1}).$$

$\mathsf{IBmE.Decrypt}(\mathsf{PK}, C, \mathsf{ID}, d_{\mathsf{ID}})$. Given PK, a ciphertext C, an identity ID, and the private key $d_{\mathsf{ID}} = (d_{\mathsf{ID}\|0}, d_{\mathsf{ID}\|1})$, set

$$m \leftarrow \mathsf{IBPRE.Decrypt}(\mathsf{PK}, C, \mathsf{ID}\|0, d_{\mathsf{ID}\|0}).$$

Clearly, the scheme constructed above satisfies the correctness condition. We now prove its security.

Theorem 1. *Suppose that Π^{IBPRE} is an* IND-ID-CCA *secure IBPRE scheme, then Π^{IBmE} is also an* IND-ID-CCA *secure IBmE scheme.*

Proof. Let $\mathcal{A}$ be an IND-ID-CCA adversary against Π^{IBmE} with advantage ϵ. We show it is feasible to construct from $\mathcal{A}$ an IND-ID-CCA adversary $\mathcal{B}$ against Π^{IBPRE} also with advantage ϵ. Let $\mathcal{C}$ denote a challenger of Π^{IBPRE}. $\mathcal{C}$ begins by supplying $\mathcal{B}$ with the public key PK of Π^{IBPRE}. $\mathcal{B}$ mounts an IND-ID-CCA attack against Π^{IBPRE} with certain help from $\mathcal{A}$ as follows.

Setup. $\mathcal{B}$ gives PK to the adversary $\mathcal{A}$.

Query Phase 1. The adversary $\mathcal{A}$ adaptively issues:

- Extraction query on ID: $\mathcal{B}$ makes the Extraction query to $\mathcal{C}$ for the identity $\mathsf{ID}\|0$ and $\mathsf{ID}\|1$, gets the private keys $d_{\mathsf{ID}\|0}$ and $d_{\mathsf{ID}\|1}$, and sends $d_{\mathsf{ID}} = (d_{\mathsf{ID}\|0}, d_{\mathsf{ID}\|1})$ to $\mathcal{A}$.
- UserKeyExtraction query on ID: $\mathcal{B}$ makes the Extraction query to $\mathcal{C}$ for the identity $\mathsf{ID}\|1$ and returns the result to $\mathcal{A}$.
- SEMKeyExtraction query on ID: $\mathcal{B}$ makes the RKGeneration query to $\mathcal{C}$ for $(\mathsf{ID}\|0, \mathsf{ID}\|1)$ and returns the result to $\mathcal{A}$.
- UserDecryption query on $(\mathsf{ID}, C, \delta_{C,\mathsf{ID},\text{sem}})$: $\mathcal{B}$ makes the Decryption query to $\mathcal{C}$ for $(\mathsf{ID}\|1, C_{\mathsf{ID}\|1} = \delta_{C,\mathsf{ID},\text{sem}})$ and returns the result to $\mathcal{A}$.
- SEMDecryption query on (ID, C): $\mathcal{B}$ makes the ReEncryption query to $\mathcal{C}$ for $(\mathsf{ID}\|0, \mathsf{ID}\|1, C)$ and returns the result to $\mathcal{A}$.
- Decryption query on (ID, C): $\mathcal{B}$ makes the Decryption query to $\mathcal{C}$ for $(\mathsf{ID}\|0, C)$ and returns the result to $\mathcal{A}$.

Challenge. The adversary $\mathcal{A}$ selects two plaintexts (m_0, m_1) of equal length, as well as the target identity ID^*. Then $\mathcal{B}$ sends $(m_0, m_1, \mathsf{ID}^*\|0)$ to $\mathcal{C}$. The challenger $\mathcal{C}$ responds with a challenge ciphertext C^* which is the encryption of message m_β with respect to the identity $\mathsf{ID}^*\|0$ in the scheme Π^{IBPRE}. Last, $\mathcal{B}$ forwards C^* to $\mathcal{A}$ as the response to $\mathcal{A}$.

Query Phase 2. $\mathcal{A}$ continues to adaptively issue queries as in Phase 1, and $\mathcal{B}$ responds as in Query Phase 1.

Guess. The adversary $\mathcal{A}$ outputs a bit β'. Then $\mathcal{B}$ also takes β' as its guess.

Analysis. It is obvious that the simulation is perfect. Thus we have shown that an IND-ID-CCA IBmE adversary against Π^{IBmE} with advantage ϵ can be employed to construct an IND-ID-CCA IBPRE adversary against Π^{IBPRE} with an identical advantage ϵ. □

3.2 From IBmE to IBPRE

Suppose that Π^{IBmE} is an IBmE scheme with algorithms Setup, Extract, DistributeKey, Encrypt, SEMDecrypt, UserDecrypt and Decrypt. We can construct an IBPRE scheme Π^{IBPRE} by defining the corresponding IBPRE algorithms as specified in Subsection 2.5.

$\mathsf{IBPRE.Setup}(\lambda)$. For security parameter λ, run $(\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{IBmE.Setup}(\lambda)$. Let PK be the public key and MSK be the master secret key.

$\mathsf{IBPRE.Extract}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID})$. Given PK, MSK, and a user identity ID, set the user's private key $d_{\mathsf{ID}} \leftarrow \mathsf{IBmE.Extract}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID})$.

$\mathsf{IBPRE.Encrypt}(\mathsf{PK}, \mathsf{ID}, m)$. Given PK, an identity ID, and a message m, generate the ciphertext $C \leftarrow \mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}, m\|0)$.

$\mathsf{IBPRE.RKGen}(\mathsf{PK}, \mathsf{ID}_1, d_{\mathsf{ID}_1}, \mathsf{ID}_2)$. Given PK, two identities $\mathsf{ID}_1, \mathsf{ID}_2$, and the private key d_{ID_1} of ID_1, run $(d_{\mathsf{ID}_1,\text{sem}}, d_{\mathsf{ID}_1,\text{user}}) \leftarrow \mathsf{IBmE.DistributeKey}$ $(\mathsf{PK}, \mathsf{ID}_1, d_{\mathsf{ID}_1})$. Set the re-encryption key

$$\begin{aligned} &d_{\mathsf{ID}_1 \to \mathsf{ID}_2} = (d_{\mathsf{ID}_1,\text{sem}}, C_K), \quad \text{where} \\ &C_K \leftarrow \mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}_2, d_{\mathsf{ID}_1,\text{user}}\|1). \end{aligned}$$

$\mathsf{IBPRE.ReEncrypt}(\mathsf{PK}, d_{\mathsf{ID}_1 \to \mathsf{ID}_2}, C_{\mathsf{ID}_1})$. Given PK, a re-encryption key $d_{\mathsf{ID}_1 \to \mathsf{ID}_2} = (d_{\mathsf{ID}_1,\text{sem}}, C_K)$ and a ciphertext C_{ID_1}, run $\delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}} \leftarrow \mathsf{IBmE.SEMDecrypt}(\mathsf{PK}, C_{\mathsf{ID}_1}, \mathsf{ID}_1, d_{\mathsf{ID}_1,\text{sem}})$, $C_\delta \leftarrow \mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}_2, \delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}}\|1)$.

Set the re-encrypted ciphertext $C_{\mathsf{ID}_2} = (C_{\mathsf{ID}_1}, C_\delta, C_K)$.

$\mathsf{IBPRE.Decrypt}(\mathsf{PK}, C_{\mathsf{ID}_2}, \mathsf{ID}_2, d_{\mathsf{ID}_2})$. Given PK, a ciphertext C_{ID_2}, an identity ID_2, and the private key d_{ID_2} of ID_2, if C_{ID_2} is a regular ciphertext, output $m\|0 \leftarrow \mathsf{IBmE.Decrypt}(\mathsf{PK}, C_{\mathsf{ID}_2}, \mathsf{ID}_2, d_{\mathsf{ID}_2})$; if C_{ID_2} is a re-encrypted ciphertext, let $C_{\mathsf{ID}_2} = (C_{\mathsf{ID}_1}, C_\delta, C_K)$, and run $d_{\mathsf{ID}_1,\text{user}}\|1 \leftarrow \mathsf{IBmE.Decryt}(\mathsf{PK}, C_K, \mathsf{ID}_2, d_{\mathsf{ID}_2})$, $\delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}}\|1 \leftarrow \mathsf{IBmE.Decryt}(\mathsf{PK}, C_\delta, \mathsf{ID}_2, d_{\mathsf{ID}_2})$. Output $m\|0 \leftarrow \mathsf{IBmE.UserDecrypt}(\mathsf{PK}, C_{\mathsf{ID}_1}, \mathsf{ID}_1, d_{\mathsf{ID}_1,\text{user}}, \delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}})$.

Note that an extra bit is appended to the message in order to distinguish between the encryption in IBPRE.Encrypt and the encryption in IBPRE.RKGen and IBPRE.ReEncrypt. To map $m\|0, d_{\mathsf{ID}_1,\text{user}}\|1$ and $\delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}}\|1$ to the message space of Π^{IBmE}, an efficient encoding algorithm and the corresponding decoding algorithm may be required.

Clearly, the scheme constructed above satisfies the correctness condition. We now prove its security.

Theorem 2. *Suppose that* Π^{IBmE} *is an* IND-ID-CCA *secure IBmE scheme, then* Π^{IBPRE} *is also an* IND-ID-CCA *secure IBPRE scheme.*

Proof. Let $\mathcal{A}$ be an IND-ID-CCA adversary against Π^{IBPRE} with advantage ϵ. We show it is feasible to construct from $\mathcal{A}$ an IND-ID-CCA adversary $\mathcal{B}$ against Π^{IBmE} with advantage $\epsilon/2$. Let $\mathcal{C}$ denote a challenger of Π^{IBmE}. $\mathcal{C}$ begins by supplying $\mathcal{B}$ with the public key PK of Π^{IBmE}. $\mathcal{B}$ mounts an IND-ID-CCA attack against Π^{IBmE} with certain help from $\mathcal{A}$ as follows.

Setup. $\mathcal{B}$ gives PK to the adversary $\mathcal{A}$. $\mathcal{B}$ also maintains a CHK-list. Initially the list is empty.

Query Phase 1. The adversary $\mathcal{A}$ adaptively issues:

- Extraction query on ID: $\mathcal{B}$ makes the Extraction query to $\mathcal{C}$ concerning the identity ID, gets the private key d_{ID}, and sends it to $\mathcal{A}$.

- RKGeneration query on $(\mathsf{ID}_1, \mathsf{ID}_2)$: If $\mathsf{ID}_1 = \mathsf{ID}^*$, $\mathcal{B}$ makes the SEMKeyExtraction query to $\mathcal{C}$ for the identity ID_1, gets $d_{\mathsf{ID}_1,\text{sem}}$, and sends $d_{\mathsf{ID}_1 \to \mathsf{ID}_2} = (d_{\mathsf{ID}_1,\text{sem}}, C_K)$ to $\mathcal{A}$, where $C_K \leftarrow \mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}_2, K\|1)$ and K is a random element; else $\mathcal{B}$ makes UserKeyExtraction and SEMKeyExtraction queries to $\mathcal{C}$ for the identity ID_1, gets $d_{\mathsf{ID}_1,\text{user}}, d_{\mathsf{ID}_1,\text{sem}}$, and sends $d_{\mathsf{ID}_1 \to \mathsf{ID}_2} = (d_{\mathsf{ID}_1,\text{sem}}, C_K)$ to $\mathcal{A}$, where $C_K \leftarrow \mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}_2, d_{\mathsf{ID}_1,\text{user}}\|1)$.

- ReEncryption query on $(\mathsf{ID}_1, \mathsf{ID}_2, C_{\mathsf{ID}_1})$: If $\mathsf{ID}_1 = \mathsf{ID}^*$, $\mathcal{B}$ makes the SEMDecryption query to $\mathcal{C}$ for $(\mathsf{ID}_1, C_{\mathsf{ID}_1})$, gets $\delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}}$, sends $C_{\mathsf{ID}_2} = (C_{\mathsf{ID}_1}, C_\delta, C_K)$ to $\mathcal{A}$, where

$$\begin{aligned} &C_\delta \leftarrow \mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}_2, \delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}}\|1), \\ &C_K \leftarrow \mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}_2, K\|1), \end{aligned}$$

and K is a random element, and adds the record $(\mathsf{ID}_1 = \mathsf{ID}^*, C_{\mathsf{ID}_1}, K)$ into the CHK-list; else $\mathcal{B}$ makes the UserKeyExtraction query to $\mathcal{C}$ for the identity ID_1, gets $d_{\mathsf{ID}_1,\text{user}}$, makes the SEMDecryption query to $\mathcal{C}$ for $(\mathsf{ID}_1, C_{\mathsf{ID}_1})$ to get $\delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}}$, and sends $C_{\mathsf{ID}_2} = (C_{\mathsf{ID}_1}, \delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}}, C_K)$ to $\mathcal{A}$, where $C_K \leftarrow \mathsf{IBmE.Encrypt}(\mathsf{PK}, \mathsf{ID}_2, d_{\mathsf{ID}_1,\text{user}}\|1)$.

- Decryption query on $(\mathsf{ID}_2, C_{\mathsf{ID}_2})$:

1) If C_{ID_2} is a regular encryption, $\mathcal{B}$ makes the Decryption query to $\mathcal{C}$ for $(\mathsf{ID}_2, C_{\mathsf{ID}_2})$ and gets $m_{\mathsf{ID}_2}\|b$. If $b = 1$, $\mathcal{B}$ outputs $\perp$, else $\mathcal{B}$ sends m_{ID_2} to $\mathcal{A}$.

2) If C_{ID_2} is a re-encrypted ciphertext, let $C_{\mathsf{ID}_2} = (C_{\mathsf{ID}_1}, C_\delta, C_K)$. $\mathcal{B}$ makes the Decryption query to $\mathcal{C}$ for $(\mathsf{ID}_2, C_\delta)$ and (ID_2, C_K), gets $\delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\text{sem}}\|b_\delta$ and $K\|b_k$. If $b_\delta = 0$ or $b_k = 0$, $\mathcal{B}$ outputs $\perp$; else:

a) If $\mathsf{ID}_1 = \mathsf{ID}^*$, $\mathcal{B}$ checks whether a record $(\mathsf{ID}_1 = \mathsf{ID}^*, C_{\mathsf{ID}_1}, K)$ exists in the CHK-list. If not, $\mathcal{B}$ outputs

$\perp$, else $\mathcal{B}$ makes the UserDecryption query to $\mathcal{C}$ for $(\mathsf{ID}_1, C_{\mathsf{ID}_1}, \delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\mathrm{sem}})$ and returns the result to $\mathcal{A}$.

b) Else, $\mathcal{B}$ runs $\mathsf{IBmE.UserDecrypt}$ $(\mathsf{PK}, C_{\mathsf{ID}_1}, \mathsf{ID}_1, K, \delta_{C_{\mathsf{ID}_1},\mathsf{ID}_1,\mathrm{sem}})$ and returns the result to $\mathcal{A}$.

Challenge. The adversary $\mathcal{A}$ selects two plaintexts (m_0, m_1) of equal length, as well as a target identity ID^*. Then $\mathcal{B}$ sends $(m_0\|0, m_1\|0, \mathsf{ID}^*)$ to $\mathcal{C}$. The challenger $\mathcal{C}$ responds with a ciphertext C^* which is the encryption of message $m_\beta\|0$ with respect to the identity ID^* in the scheme $\mathit{\Pi}^{\mathsf{IBmE}}$. Finally, $\mathcal{B}$ forwards C^* to $\mathcal{A}$ as the response to $\mathcal{A}$.

Query Phase 2. $\mathcal{A}$ continues to adaptively issue queries as in Phase 1, and $\mathcal{B}$ responds as in Query Phase 1.

Guess. The adversary $\mathcal{A}$ outputs a bit β', which is then employed by $\mathcal{B}$.

Analysis. It is obvious that the simulation is perfect. Thus we have shown that an IND-ID-CCA IBPRE adversary against $\mathit{\Pi}^{\mathsf{IBPRE}}$ with advantage ϵ can be employed to construct an IND-ID-CCA IBmE adversary against $\mathit{\Pi}^{\mathsf{IBmE}}$ with advantage $\epsilon/2$. □

4 CCA-Secure IBPRE Scheme with MSS

In this section, based on Waters' IBE scheme[5] which is only CPA-secure, we propose a concrete IBPRE scheme that is IND-ID-CCA secure in the standard model. This security is achieved owning to employing the "direct chosen-ciphertext secure" technique from [22]. At the same time, inspired by [23-24], we construct the scheme in a particular manner that the favorable master secret security (MSS) is also achieved.

4.1 Protocol Description

As introduced in Subsection 2.5, our IBPRE scheme consists of six algorithms.

$\mathsf{Setup}(\lambda)$. Given the security parameter λ, we choose an appropriate pairing group system $\langle p, \mathbb{G}, \mathbb{G}_T, e\rangle$. Let g be a generator of $\mathbb{G}$. Randomly select $\alpha \in \mathbb{Z}_p$ and let $g_1 = g^\alpha$. Assume all entity identities are represented as bit strings of length n, a separate parameter independent of p. Then, choose random elements $g_2, u'_1, u_{1,1}, \ldots, u_{1,n}, u'_2, u_{2,1}, \ldots, u_{2,n}, u'_3, u_{3,1}, \ldots, u_{3,n} \in \mathbb{G}$. Let $H : \{0,1\}^* \to \{0,1\}^n$ be a secure one-way hash function and $E : \{0,1\}^* \to \mathbb{G}_T$ be an encoding algorithm. The system master secret key is defined as $\mathsf{MSK} = g_2^\alpha$. Let the following tuple be the public key PK:

$$(p, \mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, H, u'_1, u_{1,1}, \ldots,\\ u_{1,n}, u'_2, u_{2,1}, \ldots, u_{2,n}, u'_3, u_{3,1}, \ldots, u_{3,n}).$$

Considering an n-bit string ID, let $\mathcal{V}$ be the set of all i's for which the i-th bit of ID is 1, respectively, and then define three products

$$F_1(\mathsf{ID}) = u'_1 \prod_{i\in\mathcal{V}} u_{1,i},\ F_2(\mathsf{ID}) = u'_2 \prod_{i\in\mathcal{V}} u_{2,i},\\ F_3(\mathsf{ID}) = u'_3 \prod_{i\in\mathcal{V}} u_{3,i}.$$

$\mathsf{Extract}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID})$. For an identity ID, randomly choose $r_{\mathsf{ID}} \in \mathbb{Z}_p$ and set the user's private key

$$d_{\mathsf{ID}} = (d^1_{\mathsf{ID}}, d^2_{\mathsf{ID}}) = (g_2^\alpha F_1(\mathsf{ID})^{r_{\mathsf{ID}}}, g^{r_{\mathsf{ID}}}).$$

$\mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}, m, b = 0)$. Given PK, an identity ID, and a message $m \in \{0,1\}^*$, randomly choose $s \in \mathbb{Z}_p$. First compute two n-bit strings $\mathsf{W}_1 = H(C_1, C_2, C_3)$ and $\mathsf{W}_2 = H(C_1, C_2, C_3, C_4)$, and then compute

$$C_1 = g^s,\quad C_2 = F_1(\mathsf{ID})^s,\quad C_3 = e(g_1, g_2)^s E(m\|b),\\ C_4 = F_2(\mathsf{W}_1)^s,\quad C_5 = F_3(\mathsf{W}_2)^s.$$

Output the ciphertext $C = (C_1, C_2, C_3, C_4, C_5)$.

$\mathsf{RKGen}(\mathsf{PK}, \mathsf{ID}_1, d_{\mathsf{ID}_1}, \mathsf{ID}_2)$. Given PK, two identities $\mathsf{ID}_1, \mathsf{ID}_2$, and the private key $d_{\mathsf{ID}_1} = (g_2^\alpha F_1(\mathsf{ID}_1)^{r_{\mathsf{ID}_1}}, g^{r_{\mathsf{ID}_1}})$ of ID_1, randomly choose $g_3 \in \mathbb{G}$ and $z \in \mathbb{Z}_p$. Let $\tilde{C} \leftarrow \mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}_2, g_3^{-z}, 1)$, and set the re-encryption key

$$d_{\mathsf{ID}_1\to\mathsf{ID}_2} = (g_2^\alpha F_1(\mathsf{ID}_1)^{r_{\mathsf{ID}_1}} g_3^z {u'_2}^r, u^r_{2,1}, \ldots,\\ u^r_{2,n}, g^r,\ g^{r_{\mathsf{ID}_1}}, \tilde{C}),$$

$\mathsf{ReEncrypt}(\mathsf{PK}, d_{\mathsf{ID}_1\to\mathsf{ID}_2}, C_{\mathsf{ID}_1})$. Given PK, a re-encryption key $d_{\mathsf{ID}_1\to\mathsf{ID}_2} = (g_2^\alpha \cdot F_1(\mathsf{ID}_1)^{r_{\mathsf{ID}_1}} g_3^z {u'_2}^r, u^r_{2,1}, \ldots, u^r_{2,n}, g^r, g^{r_{\mathsf{ID}_1}}, \tilde{C})$, and a ciphertext C_{ID_1}, parse C_{ID_1} as $(C_1, C_2, C_3, C_4, C_5)$. Check whether

$$e(C_1, F_1(\mathsf{ID}_1)) = e(g, C_2),\\ e(C_1, F_2(\mathsf{W}_1)) = e(g, C_4),\\ e(C_1, F_3(\mathsf{W}_2)) = e(g, C_5),$$

where $\mathsf{W}_1 = H(C_1, C_2, C_3)$ and $\mathsf{W}_2 = H(C_1, C_2, C_3, C_4)$. If not, outputs $\perp$, else randomly choose $t \in \mathbb{Z}_p$ and compute

$$C_6 = g^r,\ C_7 = g^{r_{\mathsf{ID}_1}},\ C_8 = g^t,\\ C_9 = g_2^\alpha F_1(\mathsf{ID}_1)^{r_{\mathsf{ID}_1}} g_3^z F_2(\mathsf{W}_1)^r F_3(\mathsf{W}_2)^t,\\ C_{10} = F_3(\mathsf{W}_3)^t,\quad \text{where}\\ \mathsf{W}_3 = H(C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, \tilde{C}).$$

Then output the re-encrypted ciphertext $C_{\mathsf{ID}_2} = (C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, \tilde{C}, C_{10})$.

$\mathsf{Decrypt}(\mathsf{PK}, C_{\mathsf{ID}_2}, \mathsf{ID}_2, d_{\mathsf{ID}_2})$. Given PK, a ciphertext C_{ID_2}, an identity ID_2, and his private key $d_{\mathsf{ID}_2} = (d^1_{\mathsf{ID}_2}, d^2_{\mathsf{ID}_2})$, there are two possibilities for the decryption. First, if C_{ID_2} is a regular ciphertext, let $C_{\mathsf{ID}_2} =$

$(C_1, C_2, C_3, C_4, C_5)$, $\mathsf{W}_1 = H(C_1, C_2, C_3)$, and $\mathsf{W}_2 = H(C_1, C_2, C_3, C_4)$. Check whether

$$\begin{aligned} e(C_1, F_1(\mathsf{ID}_2)) &= e(g, C_2),\\ e(C_1, F_2(\mathsf{W}_1)) &= e(g, C_4),\\ e(C_1, F_3(\mathsf{W}_2)) &= e(g, C_5).\end{aligned}$$

If not, output $\perp$, else compute

$$M = C_3 \cdot \frac{e(C_2, d^2_{\mathsf{ID}_2})}{e(C_1, d^1_{\mathsf{ID}_2})}.$$

Let $m \| b = E^{-1}(M)$. If $b = 0$, output m; else, output $\perp$.

Second, if C_{ID_2} is a re-encrypted ciphertext from ID_1 to ID_2, let $C_{\mathsf{ID}_2} = (C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, \tilde{C}, C_{10})$, $\mathsf{W}_1 = H(C_1, C_2, C_3)$, and $\mathsf{W}_2 = H(C_1, C_2, C_3, C_4)$. Check whether

$$\begin{aligned} e(C_1, F_1(\mathsf{ID}_1)) &= e(g, C_2),\\ e(C_1, F_2(\mathsf{W}_1)) &= e(g, C_4),\\ e(C_1, F_3(\mathsf{W}_1)) &= e(g, C_5).\end{aligned}$$

If not, output $\perp$, else compute

$$\begin{aligned} g_3^{-z} \| b &= E^{-1}(\mathsf{Decrypt}(\mathsf{PK}, \tilde{C}, \mathsf{ID}_2, d_{\mathsf{ID}_2})),\\ d^1_\delta &= C_9 g_3^{-z}\\ &= g_2^\alpha F_1(\mathsf{ID}_1)^{r_{\mathsf{ID}_1}} g_3^z F_2(\mathsf{W}_1)^r F_3(\mathsf{W}_2)^t g_3^{-z}\\ &= g_2^\alpha F_1(\mathsf{ID}_1)^{r_{\mathsf{ID}_1}} F_2(\mathsf{W}_1)^r F_3(\mathsf{W}_2)^t,\\ d^2_\delta &= C_7 = g^{r_{\mathsf{ID}_1}},\ d^3_\delta = C_6 = g^r,\ d^4_\delta = C_8 = g^t.\end{aligned}$$

Check whether $b = 1$ and

$$\begin{aligned} e(g, d^1_\delta) &= e(g_1, g_2) e(d^2_\delta, F_1(\mathsf{ID}_1))\\ &\qquad e(d^3_\delta, F_2(\mathsf{W}_1)) e(d^4_\delta, F_3(\mathsf{W}_2)),\\ e(g, C_{10}) &= e(C_8, F_3(\mathsf{W}_3)),\end{aligned}$$

where

$$\mathsf{W}_3 = H(C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, \tilde{C}).$$

If not, output $\perp$, else compute

$$M = C_3 \cdot \frac{e(d^2_\delta, C_2) e(d^3_\delta, C_4) e(d^4_\delta, C_5)}{e(C_1, d^1_\delta)}.$$

Let $m \| b = E^{-1}(M)$. If $b = 0$, output m, else output $\perp$.

Correctness. If C_{ID_2} is a well-formed regular ciphertext for ID_2, we have

$$\begin{aligned} \frac{e(C_2, d^2_{\mathsf{ID}_2})}{e(C_1, d^1_{\mathsf{ID}_2})} &= \frac{e(F_1(\mathsf{ID}_2)^s, g^{r_{\mathsf{ID}_2}})}{e(g^s, g_2^\alpha F_1(\mathsf{ID}_2)^{r_{\mathsf{ID}_2}})}\\ &= \frac{1}{e(g^s, g_2^\alpha)} = e(g_1, g_2)^{-s},\end{aligned}$$

as required.

If C_{ID_2} is a well-formed re-encrypted ciphertext from ID_1 to ID_2, we have

$$\begin{aligned} &\frac{e(d^2_\delta, C_2) e(d^3_\delta, C_4) e(d^4_\delta, C_5)}{e(C_1, d^1_\delta)}\\ &= \frac{e(g^{r_{\mathsf{ID}_1}}, F_1(\mathsf{ID}_1)^s) e(g^r, F_2(\mathsf{W}_1)^s) e(g^t, F_3(\mathsf{W}_2)^s)}{e(g^s, g_2^\alpha F_1(\mathsf{ID}_1)^{r_{\mathsf{ID}_1}} F_2(\mathsf{W}_1)^r F_3(\mathsf{W}_2)^t)}\\ &= \frac{1}{e(g^s, g_2^\alpha)} = e(g_1, g_2)^{-s},\end{aligned}$$

also as required.

We have noticed that our scheme involves long public keys. This is due to the fact that the scheme is based on Waters' IBE scheme[5]. Nevertheless, [25-26] independently suggested a modification to Waters' scheme to reduce the size of the public parameters, which is also applicable to our IBPRE scheme. In addition, the size of the public parameters can be further reduced by adopting the method introduced by Chatterjee and Sarkar[27]. We do not dwell on the reduction due to space concerns.

4.2 Security Proofs

The following two theorems show that our scheme is $\mathsf{IND\text{-}ID\text{-}CCA}$ secure in the standard model and achieves master secret security at the same time.

Theorem 3. *The proposed IBPRE scheme is* $(t, q_e, q_{rk}, q_{re}, q_d, \epsilon)$ $\mathsf{IND\text{-}ID\text{-}CCA}$ *secure, assuming the* (t', ϵ')*-DBDH assumption holds, where*

$$\begin{aligned} &t' = t + \mathcal{O}(\epsilon^{-2} \ln(\epsilon^{-1}) \lambda^{-1} \ln(\lambda^{-1})),\\ &\epsilon' \geqslant \frac{\epsilon}{2\lambda}\lambda = \frac{1}{512 q_1 q_2 q_3 (n+1)^3},\\ &q_1 = q_e + q_{rk} + q_{re} + q_d, \quad \textit{and} \quad q_2 = q_3 = q_d.\end{aligned}$$

Proof. Suppose there exists a $(t, q_e, q_{rk}, q_{re}, q_d, \epsilon)$-$\mathsf{IND\text{-}ID\text{-}CCA}$ adversary $\mathcal{A}$ against the proposed IBPRE scheme. Then we show it is feasible to construct another probabilistic polynomial-time $\mathcal{B}$ that employs $\mathcal{A}$ to solve the DBDH problem with a probability of at least ϵ' and in the time of at most t'. The input for algorithm $\mathcal{B}$ is a random 5-tuple (g, g^a, g^b, g^c, Z), which is either sampled from $\mathcal{T}_{\beta=1}$ (where $Z = e(g, g)^{abc}$, recall Subsection 2.2) or from $\mathcal{T}_{\beta=0}$ (where $Z \in_R \mathbb{G}_T$). The output is 1 if $Z = e(g, g)^{abc}$, otherwise 0. Algorithm $\mathcal{B}$ employs $\mathcal{A}$ to execute the following.

Setup. $\mathcal{B}$ assigns $q_1 = q_e + q_{rk} + q_{re} + q_d$ and $q_2 = q_3 = q_d$. For $1 \leqslant i \leqslant 3$, $\mathcal{B}$ sets $m_i = 4q_i$, randomly chooses integer k_i between 0 and n, randomly chooses x_i and $x_{i,1}, \ldots, x_{i,n}$ from $\mathbb{Z}_{m_i}$, and randomly chooses y_i and $y_{i,1}, \ldots, y_{i,n}$ from $\mathbb{Z}_p$. We assume that $m_i(n+1) < p$, for $1 \leqslant i \leqslant 3$.

Let ID be an n-bit string and $\mathcal{V}$ be the set of all i's for which the i-th bit of ID is 1. For $1 \leqslant j \leqslant 3$, we define

$$L_j(\mathsf{ID}) = p - m_j k_j + x_j + \sum_{i \in \mathcal{V}} x_{j,i},$$

$$T_j(\mathsf{ID}) = y_j + \sum_{i \in \mathcal{V}} y_{j,i},$$

$$K_j(\mathsf{ID}) = \begin{cases} 0, & \text{if } x_j + \sum\limits_{i \in \mathcal{V}} x_{j,i} \equiv 0 \pmod{m_j}, \\ 1, & \text{otherwise.} \end{cases}$$

$\mathcal{B}$ assigns $g_1 = g^a$, $g_2 = g^b$. It then assigns the public parameters $u'_j = g_2^{p - m_j k_j + x_j} g^{y_j}$ and $u_{j,i} = g_2^{x_{j,i}} g^{y_{j,i}}$ for $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant 3$. Apparently, we have

$$g_2^{L_j(\mathsf{ID})} g^{T_j(\mathsf{ID})} = u'_j \prod_{i \in \mathcal{V}} u_{j,i}.$$

From the perspective of the adversary, the distribution of the public parameters is identical to the real construction. The master secret is $g_2^{\alpha} = g_2^a = g^{ab}$ which is unknown to $\mathcal{B}$. All public parameters are then passed to $\mathcal{A}$. $\mathcal{B}$ also maintains a CHK-list to validate the re-encrypted ciphertext. Initially the list is empty.

Query Phase 1. The adversary $\mathcal{A}$ adaptively issues:

• Extraction query on ID: if $K_1(\mathsf{ID}) = 0$, $\mathcal{B}$ aborts and randomly outputs a bit. Otherwise, $\mathcal{B}$ chooses a random $r \in \mathbb{Z}_p$. Using the technique described by Boneh and Boyen[3], it constructs the private key

$$\begin{aligned} d_{\mathsf{ID}} &= (d^1_{\mathsf{ID}}, d^2_{\mathsf{ID}}) \\ &= (g_1^{\frac{-T_1(\mathsf{ID})}{L_1(\mathsf{ID})}} (u'_1 \prod_{i \in \mathcal{V}} u_{1,i})^r, g_1^{\frac{-1}{L_1(\mathsf{ID})}} g^r). \end{aligned}$$

Let $\tilde{r} = r - \frac{a}{L_1(\mathsf{ID})}$. Then we have

$$\begin{aligned} d^1_{\mathsf{ID}} &= g_1^{\frac{-T_1(\mathsf{ID})}{L_1(\mathsf{ID})}} \Big(u'_1 \prod_{i \in \mathcal{V}} u_{1,i}\Big)^r \\ &= g_1^{\frac{-T_1(\mathsf{ID})}{L_1(\mathsf{ID})}} (g_2^{L_1(\mathsf{ID})} g^{T_1(\mathsf{ID})})^r \\ &= g_2^a (g_2^{L_1(\mathsf{ID})} g^{T_1(\mathsf{ID})})^{-\frac{a}{L_1(\mathsf{ID})}} (g_2^{L_1(\mathsf{ID})} g^{T_1(\mathsf{ID})})^r \\ &= g_2^a \Big(u'_1 \prod_{i \in \mathcal{V}} u_{1,i}\Big)^{r - \frac{a}{L_1(\mathsf{ID})}} \\ &= g_2^a \Big(u'_1 \prod_{i \in \mathcal{V}} u_{1,i}\Big)^{\tilde{r}}. \end{aligned}$$

We also have $d^2_{\mathsf{ID}} = g_1^{\frac{-1}{L_1(\mathsf{ID})}} g^r = g^{r - \frac{a}{L_1(\mathsf{ID})}} = g^{\tilde{r}}$. Hence for the adversary, all private keys computed by $\mathcal{B}$ will be indistinguishable from the keys generated by a true challenger.

• RKGeneration query on $(\mathsf{ID}_1, \mathsf{ID}_2)$:

1) If $\mathsf{ID}_1 = \mathsf{ID}^*$, $\mathcal{B}$ chooses x, y, r_1, r_2, z_1, z_2 at random from $\mathbb{Z}_p$ and sets $g_3 = g_2^x g^y$. Note that we require $L_1(\mathsf{ID}^*) \equiv 0 \pmod{p}$. Let $\mathcal{V}^*$ be the set of all i's for which the i-th bit of ID^* is 1. $\mathcal{B}$ computes

$$\begin{aligned} d_{\mathsf{ID}_1 \to \mathsf{ID}_2} &= (g^{r_1 T_1(\mathsf{ID}_1)} g_1^{-y/x} g_3^{z_1} {u'_2}^{r_2}, \\ &\qquad u_{2,1}^{r_2}, \ldots, u_{2,n}^{r_2},\ g^{r_2}, g^{r_1}, \tilde{C}), \\ vk_{\mathsf{ID}_1 \to \mathsf{ID}_2} &= g_1^{-1/x} g^{z_1} = g^{-a/x + z_1}, \end{aligned}$$

where $\tilde{C} \leftarrow \mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}_2, g_3^{z_2}, 1)$, and sends $d_{\mathsf{ID}_1 \to \mathsf{ID}_2}$ to $\mathcal{A}$. Then the record $(\mathsf{ID}_1, \mathsf{ID}_2, vk_{\mathsf{ID}_1 \to \mathsf{ID}_2}, \tilde{C})$ is added in the CHK-list.

Let $z = -a/x + z_1$, we have

$$\begin{aligned} d_{\mathsf{ID}_1 \to \mathsf{ID}_2} &= \Big(g_2^a \Big(u'_1 \prod_{i \in \mathcal{V}*} u_{1,i}\Big)^{r_1} g_3^z {u'_2}^{r_2}, \\ &\qquad u_{2,1}^{r_2}, \ldots, u_{2,n}^{r_2},\ g^{r_2}, g^{r_1}, \tilde{C}\Big), \\ vk_{\mathsf{ID}_1 \to \mathsf{ID}_2} &= g^z. \end{aligned}$$

2) Else if $L_1(\mathsf{ID}_1) \bmod p \neq 0$, $\mathcal{B}$ uses the same method in Extraction query to get the private key of ID, runs RKGen algorithm, and returns the result to $\mathcal{A}$. Last, $\mathcal{B}$ computes $vk_{\mathsf{ID}_1 \to \mathsf{ID}_2}$ and adds the record $(\mathsf{ID}_1, \mathsf{ID}_2, vk_{\mathsf{ID}_1 \to \mathsf{ID}_2}, \tilde{C})$ to the CHK-list.

3) Else, $\mathcal{B}$ aborts and randomly outputs a bit.

• ReEncryption query on $(\mathsf{ID}_1, \mathsf{ID}_2, C_{\mathsf{ID}_1})$: $\mathcal{B}$ uses the same method in RKGeneration query to get $d_{\mathsf{ID}_1 \to \mathsf{ID}_2}$, runs $\mathsf{ReEncrypt}$ algorithm, and returns the result to $\mathcal{A}$.

• Decryption query on $(\mathsf{ID}_2, C_{\mathsf{ID}_2})$:

1) If C_{ID_2} is a regular ciphertext, let $C_{\mathsf{ID}_2} = (C_1, C_2, C_3, C_4, C_5)$. $\mathcal{B}$ lets $\mathsf{W}_1 = H(C_1, C_2, C_3)$ and $\mathsf{W}_2 = H(C_1, C_2, C_3, C_4)$, and checks whether

$$\begin{aligned} e(C_1, F_1(\mathsf{ID}_2)) &= e(g, C_2), \\ e(C_1, F_2(\mathsf{W}_1)) &= e(g, C_4), \\ e(C_1, F_3(\mathsf{W}_2)) &= e(g, C_5), \end{aligned}$$

If not, $\mathcal{B}$ outputs $\perp$. Then,

– if $L_1(\mathsf{ID}_2) \equiv L_2(\mathsf{W}_1) \equiv L_3(\mathsf{W}_2) \equiv 0 \pmod{p}$, $\mathcal{B}$ aborts and randomly outputs a bit;

– else $\mathcal{B}$ uses the same method in Extraction query to get

$$\begin{aligned} d^1_{\delta} &= g_2^{\alpha} F_1(\mathsf{ID}_2)^{r_{\mathsf{ID}_2}} F_2(\mathsf{W}_1)^r F_3(\mathsf{W}_2)^t, \\ d^2_{\delta} &= g^{r_{\mathsf{ID}_2}},\ d^3_{\delta} = g^r,\ d^4_{\delta} = g^t. \end{aligned}$$

Then, $\mathcal{B}$ computes $M = C_3 \cdot \frac{e(d^2_{\delta}, C_2) e(d^3_{\delta}, C_4) e(d^4_{\delta}, C_5)}{e(C_1, d^1_{\delta})}$. Let $m \| b = E^{-1}(M)$. If $b = 0$, $\mathcal{B}$ returns m to $\mathcal{A}$; else, $\mathcal{B}$ outputs $\perp$.

2) If C_{ID_2} is a re-encrypted ciphertext from ID_1 to ID_2, let $C_{\mathsf{ID}_2} = (C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, \tilde{C}, C_{10})$.

$\mathcal{B}$ first checks whether

$$\begin{aligned} &e(C_1, F_1(\mathsf{ID}_1)) = e(g, C_2),\\ &e(C_1, F_2(\mathsf{W}_1)) = e(g, C_4),\\ &e(C_1, F_3(\mathsf{W}_1)) = e(g, C_5),\\ &e(g, C_{10}) = e(C_8, F_3(\mathsf{W}_3)),\end{aligned}$$

where $\mathsf{W}_1 = H(C_1, C_2, C_3)$, $\mathsf{W}_2 = H(C_1, C_2, C_3, C_4)$, and $\mathsf{W}_3 = H(C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, \tilde{C})$. If not, $\mathcal{B}$ outputs $\perp$, else $\mathcal{B}$ checks whether the record $(\mathsf{ID}_1, \mathsf{ID}_2, vk_{\mathsf{ID}_1 \to \mathsf{ID}_2}, \tilde{C})$ is on the CHK-list and

$$\begin{aligned} e(g, C_9) = {}& e(g_1, g_2) e(C_7, F_1(\mathsf{ID}_1))\\ & e(vk_{\mathsf{ID}_1 \to \mathsf{ID}_2}, g_3)\\ & e(C_6, F_2(\mathsf{W}_1)) e(C_8, F_3(\mathsf{W}_2)).\end{aligned}$$

If not, $\mathcal{B}$ outputs $\perp$. Else $\mathcal{B}$ uses the same method in the first case to respond to $\mathcal{A}$'s query.

Indeed, for a well-formed re-encrypted ciphertext, we have

$$\begin{aligned} e(g, C_9) &= e(g, g_2^a F_1(\mathsf{ID}_1)^{r_{\mathsf{ID}_1}} g_3^z F_2(\mathsf{W}_1)^r F_3(\mathsf{W}_2)^t)\\ &= e(g_1, g_2) e(g^{r_{\mathsf{ID}_1}}, F_1(\mathsf{ID}_1)) e(g^z, g_3)\\ &\quad e(g^r, F_2(\mathsf{W}_1)) e(g^t, F_3(\mathsf{W}_2))\\ &= e(g_1, g_2) e(C_7, F_1(\mathsf{ID}_1)) e(vk_{\mathsf{ID}_1 \to \mathsf{ID}_2}, g_3)\\ &\quad e(C_6, F_2(\mathsf{W}_1)) e(C_8, F_3(\mathsf{W}_2)).\end{aligned}$$

Challenge. The adversary $\mathcal{A}$ selects two plaintexts (m_0, m_1) of equal length, as well as a target identity ID^*. If $L_1(\mathsf{ID}^*) \bmod p \neq 0$, $\mathcal{B}$ aborts and randomly outputs a bit. Otherwise, $\mathcal{B}$ flips a fair coin $\beta \in \{0, 1\}$ and constructs the ciphertext as follows:

1) $\mathcal{B}$ computes

$$\begin{aligned} C_1^* &= g^c, C_3^* = Z \cdot E(m_\beta \| 0),\\ C_2^* &= (g^c)^{T_1(\mathsf{ID}^*)} = (g_2^{L_1(\mathsf{ID}^*)} g^{T_1(\mathsf{ID}^*)})^c\\ &\quad (\because L_1(\mathsf{ID}^*) \equiv 0 \pmod p)\\ &= \Big(u_1' \prod_{i \in \mathcal{V}^*} u_{1,i}\Big)^c.\end{aligned}$$

(This shows that C_2^* is well-formed.)

2) $\mathcal{B}$ computes $\mathsf{W}_1^* = H(C_1^*, C_2^*, C_3^*)$. Let $\mathcal{W}_1^*$ be the set of all i's for which the i-th bit of W_1^* is 1. If $L_2(\mathsf{W}_1^*) \bmod p \neq 0$, $\mathcal{B}$ aborts and randomly outputs a bit. Otherwise, $\mathcal{B}$ computes

$$\begin{aligned} C_4^* &= (g^c)^{T_2(\mathsf{W}_1^*)} = (g_2^{L_2(\mathsf{W}_1^*)} g^{T_2(\mathsf{W}_1^*)})^c\\ &\quad (\because L_2(\mathsf{W}_1^*) \equiv 0 \pmod p)\\ &= \Big(u_2' \prod_{i \in \mathcal{W}_1^*} u_{2,i}\Big)^c.\end{aligned}$$

(This shows that C_4^* is well-formed.)

3) $\mathcal{B}$ computes $\mathsf{W}_2^* = H(C_1^*, C_2^*, C_3^*, C_4^*)$. Let $\mathcal{W}_2^*$ be the set of all i's for which the i-th bit of W_2^* is 1. If $L_3(\mathsf{W}_2^*) \bmod p \neq 0$, $\mathcal{B}$ aborts and randomly outputs a bit. Otherwise, $\mathcal{B}$ computes

$$\begin{aligned} C_5^* &= (g^c)^{T_3(\mathsf{W}_2^*)} = (g_2^{L_3(\mathsf{W}_2^*)} g^{T_3(\mathsf{W}_2^*)})^c\\ &\quad (\because L_3(\mathsf{W}_2^*) \equiv 0 \pmod p)\\ &= \Big(u_3' \prod_{i \in \mathcal{W}_2^*} u_{3,i}\Big)^c.\end{aligned}$$

(This shows that C_5^* is well-formed.)

4) Last, $\mathcal{B}$ returns the ciphertext $C^* = (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*)$. C^* is a valid encryption of m_β if $Z = e(g, g)^{abc}$. Otherwise, C^* exhibits no information on $\mathcal{B}$'s choice of β.

Query Phase 2. $\mathcal{A}$ continues to adaptively issue queries as in Phase 1, and $\mathcal{B}$ responds as in Query Phase 1.

Guess. The adversary $\mathcal{A}$ outputs a bit β'.

Artificial Abort. The probability that $\mathcal{B}$ aborts in the query or challenge phase depends on the adversary's input. $\mathcal{B}$ corrects for this by forcing all possible sets of queries of the adversary to cause $\mathcal{B}$ to abort with (almost) the same probability. This is done by sampling the transcript of adversary's query and in certain cases aborting. The sampling procedure introduces the extra component $\mathcal{O}(\epsilon^{-2} \ln(\epsilon^{-1}) \lambda^{-1} \ln(\lambda^{-1}))$[5,27] into the simulator's runtime. Here λ is a lower bound on the probability that $\mathcal{B}$ does not abort before entering the artificial abort stage.

Output. If $\mathcal{B}$ has not aborted up to this stage, then it outputs 1 if $\beta' = \beta$, else it outputs 0.

Analysis. It is obvious that the simulation is perfect. The probability of $\mathcal{B}$ not aborting before entering the artificial abort stage can be computed as in [5, 27]. □

Theorem 4. *The proposed identity-based unidirectional PRE scheme is $(t, q_e, q_{rk}, \epsilon)$ master secret secure, assuming the (t', ϵ')-CDH assumption holds, where*

$$t' = t + \mathcal{O}(\epsilon^{-2} \ln(\epsilon^{-1}) \lambda^{-1} \ln(\lambda^{-1})),\ \epsilon' \geqslant \frac{\epsilon}{2\lambda},$$

where $\lambda = \frac{1}{8q_e(n+1)}$.

Proof. Suppose there exists a $(t, q_e, q_{rk}, \epsilon)$ MSS adversary $\mathcal{A}$ against our identity-based unidirectional PRE scheme. Then we show it is feasible to construct another probabilistic polynomial-time $\mathcal{B}$ that employs $\mathcal{A}$ to solve the CDH problem with a probability of at least ϵ' and in the time of at most t'. The input information for algorithm $\mathcal{B}$ is a group $\mathbb{G}$, a generator g, and the elements g^a and g^b. The output is g^{ab}. Algorithm $\mathcal{B}$ employs $\mathcal{A}$ to execute the following.

Setup. $\mathcal{B}$ sets $m = 4q_e$, randomly chooses integer k between 0 and n, randomly chooses x_1 and

$x_{1,1}, \ldots, x_{1,n}$ from $\mathbb{Z}_m$, and randomly chooses y_1 and $y_{1,1}, \ldots, y_{1,n}$ from $\mathbb{Z}_p$. We assume that $m(n+1) < p$.

Let ID be an n-bit string and $\mathcal{V}$ be the set of all i's for which the i-th bit of ID is 1. We define

$$L_1(\mathsf{ID}) = p - mk + x_1 + \sum_{i \in \mathcal{V}} x_{1,i},$$

$$T_1(\mathsf{ID}) = y_1 + \sum_{i \in \mathcal{V}} y_{1,i},$$

$$K_1(\mathsf{ID}) = \begin{cases} 0, & \text{if } x_1 + \sum_{i \in \mathcal{V}} x_{1,i} \equiv 0 (\bmod m)), \\ 1, & \text{otherwise.} \end{cases}$$

$\mathcal{B}$ assigns $g_1 = g^a$, $g_2 = g^b$. It then assigns the public parameters $u_1' = g_2^{p-mk+x_1} g^{y_1}$, and $u_{1,i} = g_2^{x_{1,i}} g^{y_{1,i}}$ for $1 \leqslant i \leqslant n$. Apparently, we have

$$g_2^{L_1(\mathsf{ID})} g^{T_1(\mathsf{ID})} = u_1' \prod_{i \in \mathcal{V}} u_{1,i}.$$

$\mathcal{B}$ also randomly chooses $x, y, y_{2,1}, \ldots, y_{2,n}$ from $\mathbb{Z}_p$, and $u_3', u_{3,1}, \ldots, u_{3,n}$ from $\mathbb{G}$. $\mathcal{B}$ assigns $u_2' = g_2^x g^y$, $u_{2,1} = g^{y_{2,1}}, \ldots, u_{2,n} = g^{y_{2,n}}$. From the perspective of the adversary, the distribution of the public parameters is identical to the real construction. All public parameters are then passed to $\mathcal{A}$.

Query Phase. The adversary $\mathcal{A}$ adaptively issues:

- Extraction query on ID: If $K_1(\mathsf{ID}) = 0$, $\mathcal{B}$ aborts. Otherwise, $\mathcal{B}$ chooses a random $r \in \mathbb{Z}_p$. Using the technique described by Boneh and Boyen[3], $\mathcal{B}$ constructs the private key d_{ID} as

$$\begin{aligned} d_{\mathsf{ID}} &= (d^1_{\mathsf{ID}}, d^2_{\mathsf{ID}}) \\ &= \Big(g_1^{\frac{-T_1(\mathsf{ID})}{L_1(\mathsf{ID})}} \Big(u_1' \prod_{i \in \mathcal{V}} u_{1,i} \Big)^r, g_1^{\frac{-1}{L_1(\mathsf{ID})}} g^r \Big). \end{aligned}$$

Let $\tilde{r} = r - \frac{a}{L_1(\mathsf{ID})}$. Then we have

$$\begin{aligned} d^1_{\mathsf{ID}} &= g_1^{\frac{-T_1(\mathsf{ID})}{L_1(\mathsf{ID})}} \Big(u_1' \prod_{i \in \mathcal{V}} u_{1,i} \Big)^r \\ &= g_1^{\frac{-T_1(\mathsf{ID})}{L_1(\mathsf{ID})}} (g_2^{L_1(\mathsf{ID})} g^{T_1(\mathsf{ID})})^r \\ &= g_2^a (g_2^{L_1(\mathsf{ID})} g^{T_1(\mathsf{ID})})^{-\frac{a}{L_1(\mathsf{ID})}} (g_2^{L_1(\mathsf{ID})} g^{T_1(\mathsf{ID})})^r \\ &= g_2^a \Big(u_1' \prod_{i \in \mathcal{V}} u_{1,i} \Big)^{r - \frac{a}{L_1(\mathsf{ID})}} = g_2^a (u_1' \prod_{i \in \mathcal{V}} u_{1,i})^{\tilde{r}}. \end{aligned}$$

We also have $d^2_{\mathsf{ID}} = g_1^{\frac{-1}{L_1(\mathsf{ID})}} g^r = g^{r - \frac{a}{L_1(\mathsf{ID})}} = g^{\tilde{r}}$. Hence for the adversary, all private keys computed by $\mathcal{B}$ will be indistinguishable from the keys generated by a true challenger.

- *RKGeneration* query on $(\mathsf{ID}_1, \mathsf{ID}_2)$:

1) If $L_1(\mathsf{ID}_1) \bmod p \neq 0$, $\mathcal{B}$ uses the same method in Extraction query to get the private key of ID, runs RKGen algorithm, and returns the result to $\mathcal{A}$.

2) Else, $\mathcal{B}$ chooses r_1, r_2, z at random from $\mathbb{Z}_p$, and g_3 at random from $\mathbb{G}$. $\mathcal{B}$ computes

$$\begin{aligned} d_{\mathsf{ID}_1 \to \mathsf{ID}_2} = (& g^{r_1 T_1(\mathsf{ID}_1)} g_3^z g_1^{-y/x} u_2'^{\,r_2}, \\ & g_1^{-y_{2,1}/x} g^{r_2}, \ldots, g_1^{-y_{2,n}/x} g^{r_2}, \\ & g_1^{-1/x} g^{r_2}, g^{r_1}, \tilde{C}), \end{aligned}$$

where $\tilde{C} \leftarrow \mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}_2, g_3^{-z}, 1)$, and sends $d_{\mathsf{ID}_1 \to \mathsf{ID}_2}$ to $\mathcal{A}$.

Note that, $L_1(\mathsf{ID}_1) \equiv 0 \pmod p$. Let $\mathcal{V}_1$ be the set of all i's for which the i-th bit of ID_1 is 1, and $r_2' = -a/x + r_2$. We have

$$\begin{aligned} d_{\mathsf{ID}_1 \to \mathsf{ID}_2} = \Big(& g_2^a \Big(u_1' \prod_{i \in \mathcal{V}_1} u_{1,i} \Big)^{r_1} g_3^z u_2'^{\,r_2'}, u_{2,1}^{r_2'}, \\ & \ldots, u_{2,n}^{r_2'}, g^{r_2'}, g^{r_1}, \tilde{C} \Big). \end{aligned}$$

Output. The adversary $\mathcal{A}$ outputs an identity ID^* and the private key $d_{\mathsf{ID}^*} = (d^1_{\mathsf{ID}^*}, d^2_{\mathsf{ID}^*})$. Let $\mathcal{V}^*$ be the set of all i's for which the i-th bit of ID^* is 1. If $L_1(\mathsf{ID}^*) \bmod p \neq 0$, $\mathcal{B}$ aborts; else $\mathcal{B}$ computes and outputs

$$\frac{d^1_{\mathsf{ID}^*}}{(d^2_{\mathsf{ID}^*})^{T_1(\mathsf{ID}^*)}} = \frac{g_2^a (u_1' \prod_{i \in \mathcal{V}^*} u_{1,i})^r}{g^{r T_1(\mathsf{ID}^*)}} = g_2^a = g^{ab},$$

which is exactly the solution to the given CDH problem.

Analysis. It is obvious that the simulation is perfect. The probability of $\mathcal{B}$ not aborting can be computed as in [5]. □

5 Concluding Remarks

In this paper, we have presented two new constructions that are both provably secure in the standard model. First, we explored the relationship between identity-based mediated encryption (IBmE) and identity-based unidirectional proxy re-encryption (IBPRE), and demonstrated how a secure IBmE scheme can be constructed from any secure IBPRE scheme and vice versa. Second, we imported the notion of master secret security (MSS) to IBPRE and accordingly presented a concrete IBPRE scheme, which not only is CCA-secure but also achieves the MSS property.

Concerning future research on IBPRE, an interesting open problem may be posed as follows. Our IBPRE scheme is not resilient to the "transfer of delegation" attack in that the proxy can collude with a set of colluding delegatees to re-delegate the decryption rights. In real applications, such conspiracy may violate the intended security policy. The design of an IBPRE scheme further secure against the "transfer of delegation" attack still seems to be a challenging task.

Acknowledgement We thank anonymous reviewers for their review efforts.

References

[1] Shamir A. Identity-based cryptosystems and signature schemes. In *Proc. Crypto1984*, Santa Babara, USA, Aug. 19-22, 1984, pp.47-53.

[2] Boneh D, Franklin M. Identity based encryption from the Weil pairing. In *Proc. Crypto 2001*, Santa Barbara, USA, Aug. 19-23, 2001, pp.213-229.

[3] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In *Proc. Eurocrypt 2004*, Paris, France, April 9-11, 2004, pp.223-238.

[4] Boneh D, Boyen X. Secure identity based encryption without random oracles. In *Proc. Crypto 2004*, Santa Barbara, USA, Aug. 15-19, 2004, pp.443-459.

[5] Waters B. Efficient identity-based encryption without random oracles. In *Proc. Eurocrypt 2005*, Aarhus, Denmark, May 22-26, 2005, pp.114-127.

[6] Gentry C. Practical identity-based encryption without random oracles. In *Proc. Eurocrypt 2006*, St. Petersburg, Russia, May 28-June 1, 2006, pp.445-464.

[7] Boneh D, Gentry C, Hamburg M. Space-efficient identity based encryption without pairings. In *Proc. the 48th Annual IEEE Symposium on Foundations of Computer Science* (*FOCS 2007*), Rhode Island, USA, Oct. 20-23, 2007, pp.647-657.

[8] Boneh D, Ding X, Tsudik G, Wong C M. A method for fast revocation of public key certificates and security capabilities. In *Proc. the 10th USENIX Security Symposium*, Washington DC, USA, Aug. 13-17, 2001, pp.297-310.

[9] Ding X, Tsudik G. Simple identity-based cryptography with mediated RSA. In *Proc. CT-RSA 2003*, San Francisco, USA, April 13-17, 2003, pp.193-210.

[10] Libert B, Quisquater J J. Efficient revocation and threshold pairing based cryptosystems. In *Proc. the 22nd ACM Symposium on Principles of Distributed Computing* (*PODC 2003*), Boston, USA, July 13-16, 2003, pp.163-171.

[11] Baek J, Zheng Y. Identity-based threshold decryption. In *Proc. PKC 2004*, Singapore, March 1-4, 2004, pp.262-276.

[12] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. the 1st ACM Conference on Computer and Communications Security* (*CCS 1993*), Fairfax, USA, Nov. 3-5, 1993, pp.62-73.

[13] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. In *Proc. Eurocrypt 1998*, Espoo, Finland, May 31-June 4, 1998, pp.127-144.

[14] Ateniese G, Fu K, Green M, Hohenberger S. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security*, Feb. 2006, 9(1): 1-30.

[15] Canetti R, Hohenberger S. Chosen-ciphertext secure proxy re-encryption. In *Proc. the 14th ACM Conference on Computer and Communications Security* (*CCS 2007*), Singapore, March 20-22, 2007, pp.185-194.

[16] Libert B, Vergnaud D. Unidirectional chosen-ciphertext secure proxy re-encryption. In *Proc. PKC 2008*, Barcelona, Spain, March 9-12, 2008, pp.360-379.

[17] Deng R H, Weng J, Liu S, Chen K. Chosen-ciphertext secure proxy re-encryption without pairings. In *Proc. CANS 2008*, Hong Kong, China, Dec. 2-4, 2008, pp.1-17.

[18] Shao J, Cao Z. CCA-secure proxy re-encryption without pairings. In *Proc. PKC 2009*, Irvine, USA, March 18-20, 2009, pp.357-376.

[19] Green M, Ateniese G. Identity-based proxy re-encryption. In *Proc. ACNS 2007*, Zhuhai, China, June 5-8, 2007, pp.288-306.

[20] Chu C K, Tzeng W G. Identity-based proxy re-encryption without random oracles. In *Proc. ISC 2007*, Valparaiso, Chile, Oct. 9-12, 2007, pp.189-202.

[21] Shao J, Xing D, Cao Z. Identity-based proxy re-encryption schemes with multiuse, unidirection, and CCA security. Cryptology ePrint Archive, Report 2008/103, 2008.

[22] Boyen X, Mei Q, Waters B. Direct chosen ciphertext security from identity based techniques. In *Proc. the 12th ACM Conference on Computer and Communications Security* (*CCS 2005*), Taipei, China, March 21-24, 2005, pp.320-329.

[23] Abdalla M, Catalano D, Dent A W, Malone-Lee J, Neven G, Smart N P. Identity-based encryption gone wild. In *Proc. ICALP 2006*, Venice, Italy, July 9-16, 2006, pp.300-311.

[24] Abdalla M, Kiltz E, Neven G. Generalized key delegation for hierarchical identity-based encryption. In *Proc. ESORICS 2007*, Dresden, Germany, Sept. 24-26, 2007, pp.139-154.

[25] Naccache D. Secure and practical identity-based encryption. *IET Information Security*, June 2007, 1(2): 59-64.

[26] Chatterjee S, Sarkar P. Trading time for space: Towards an efficient IBE scheme with short(er) public parameters in the standard model. In *Proc. ICISC 2005*, Seoul, Korea, Dec. 1-2, 2005, pp.424-440.

[27] Chatterjee S, Sarkar P. HIBE with short public parameters without random oracle. In *Proc. ASIACRYPT 2006*, Shanghai, China, Dec. 3-7, 2006, pp.145-160.

Jun-Zuo Lai received the B.S. and M.S. degrees in computer science and technology from Jingdezhen Ceramic Institute in 2002 and 2005, respectively. He is currently a Ph.D. candidate in the Shanghai Jiao Tong University, Shanghai, China. His research interests include cryptography and information security.

Wen-Tao Zhu received his B.S. and Ph.D. degrees both from Department of Electronic Engineering and Information Science, University of Science and Technology of China. He has since 2004 been with State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, and is currently an associate research professor. His research interests include computer networking and information security. He is a member of IEEE and is a senior member of the China Institute of Communications.

Robert H. Deng received his Bachelor's degree from National University of Defense Technology, China, M.Sc. and Ph.D. degrees from the Illinois Institute of Technology, USA. He has been with the Singapore Management University since 2004, and is currently professor, associate dean for Faculty & Research, School of Information Systems. Prior to this, he was principal scientist and manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. He has 26 patents and more than 200 technical publications in international conferences and journals in the areas of computer networks, network security and information security. He has served as general chair, program committee chair and program committee member of numerous international conferences. He is an associate editor of the IEEE Transactions on Information Forensics and Security, associate editor of Security and Communication Networks Journal (John Wiley), and member of Editorial Board of Journal of Computer Science and Technology (the Chinese Academy of Sciences). He received the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006.

Sheng-Li Liu got her Bachelor's, Master's and Ph.D. degrees from Xidian University in 1995, 1998 and 2000 respectively. From 2000 till 2002, she continued her research on cryptography and got another Ph.D. degree at Technische Universiteit Eindhoven, the Netherlands. Since 2002, she joined the Department of Computer Science and Engineering, Shanghai Jiao Tong University. She is now a professor and her research interests include ID-based cryptography, pairing-based cryptosystems, and information-theoretic security.

Wei-Dong Kou received his B.S. and M.S. degrees from Beijing University of Posts and Telecommunications, his Ph.D. degree from Xidian University. He is currently chief architect and technical executive, IBM Software Group, Greater China Group. Before returning to IBM in 2004, He was on leave from IBM and served as Dean, the School of Computer Science at Xidian University, and Director of the National ISN Research Lab in China. He was associate director of E-business Institute at the University of Hong Kong.