A Generic Construction for Revocable Identity-Based Encryption with Subset Difference Methods

Kwangsu Lee[*]

Abstract

To deal with dynamically changing user's credentials in identity-based encryption (IBE), providing an efficient key revocation method is a very important issue. Recently, Ma and Lin proposed a generic method of designing a revocable IBE (RIBE) scheme that uses the complete subtree (CS) method by combining IBE and hierarchical IBE (HIBE) schemes. In this paper, we propose a new generic method for designing an RIBE scheme that uses the subset difference (SD) method instead of using the CS method. In order to use the SD method, we generically design an RIBE scheme by combining IBE, identity-based revocation (IBR), and two-level HIBE schemes. If the underlying IBE, IBR, and HIBE schemes are adaptively (or selectively) secure, then our RIBE scheme is also adaptively (or selectively) secure. In addition, we show that the layered SD (LSD) method can be applied to our RIBE scheme and a chosen-ciphertext secure RIBE scheme also can be designed generically.

Keywords: Revocable identity-based encryption, Subset difference method, Generic construction.

[*] Sejong University, Seoul, Korea. Email: kwangsu@sejong.ac.kr.

1 Introduction

Identity-based encryption (IBE) is a new type of public-key encryption (PKE) that solve the public-key management problem in PKE by using a user's identity as a public key [37]. Since the first IBE scheme in bilinear maps was proposed by Boneh and Franklin [5], research on new types of cryptographic encryption such as IBE, hierarchical IBE (HIBE), attribute-based encryption (ABE), and predicate encryption (PE) has been actively studied as an important research topic [5,7,13,15]. Despite the long history of research on IBE, the IBE schemes have not been widely deployed in real environments. One reason of this problem is that unlike PKE schemes, which uses a public-key infrastructure to handle certificate issuance and revocation, it is not simple to revoke the private key of a user in IBE. Therefore, an important additional feature of IBE schemes is to support the private key revocation flexibly and efficiently.

The method of revoking the private key of a user in IBE has been studied since the initial IBE scheme was designed, but this method is not suitable for handling a large number of users [5]. The first revocable IBE (RIBE) scheme to efficiently handle large numbers of users was proposed by Boldyreva et al. [3]. The key design principle of their RIBE scheme is that a trusted center periodically creates and broadcasts an update key on time T for non-revoked users, along with the generation of a user's private key. In this case, if the private key of a user ID is not revoked in the update key on time T, the user can decrypt a ciphertext for his identity ID and the corresponding time T. In other words, the RIBE scheme proposed by Boldyreva et al. can be seen as a method to support the indirect private key revocation, in which the center decides the revocation of private keys instead of the sender. Specifically, Boldyreva et al. designed their RIBE scheme by combining a tree-based broadcast method with a fuzzy identity-based encryption scheme. After the work of Boldyreva et al., various RIBE schemes and extension schemes have been proposed to enhance the efficiency, security, and functionality of RIBE [8,9,16,21,24,26,32,34–36,38].

Currently, to design an RIBE scheme, we redesign an RIBE scheme from the beginning by directly modifying an efficient IBE scheme proposed before. This is problematic in that a new RIBE scheme must be designed again whenever a new IBE scheme having a different mathematical structure is proposed. Ma and Lin recently overcome this problem by suggesting a generic method of designing an RIBE scheme by using an IBE scheme as a black-box [27]. In their generic RIBE scheme with the complete subtree (CS) method, an update key consists of $O(r \cdot n)$ IBE private keys and a ciphertext consists of $O(n)$ IBE ciphertexts where r is the number of revoked users and n is the bit length of an identity. In tree-based broadcast encryption, there exists the subset difference (SD) method proposed by Naor et al. [29] which is more efficient than the CS method. Additionally, the layered SD (LSD) method which improved the SD method has also been proposed [14]. Therefore, we ask whether it is possible to design an RIBE scheme from an IBE scheme in a generic way, using the SD/LSD method instead of using the CS method. If the SD/LSD method can be applied to a generic RIBE scheme, the size of an update key can be reduced from $O(r \cdot n)$ key elements to $O(r)$ key elements.

1.1 Our Contributions

In this paper, we show that it is possible to design an RIBE scheme with the SD method in a generic way. As described above, the generic RIBE scheme with the CS method uses IBE and two-level HIBE schemes as basic building blocks [27]. On the contrary, our generic RIBE scheme with the SD method uses IBE, identity-based revocation (IBR), and two-level HIBE schemes as basic building blocks. The IBR scheme is a special type of identity-based broadcast encryption (IBBE) scheme in which a set R of revoked users is specified in an IBR ciphertext whereas a set S of receivers is specified in an IBBE ciphertext. The newly derived RIBE scheme with the SD method consists of $O(r)$ number of IBE and IBR private keys in an update key and $O(n^2)$ number of IBE and IBR ciphertexts in a ciphertext. Compared with the previous generic RIBE scheme with the CS method, the size of an update key is reduced but the size of a ciphertext is increased.

To analyze the security of our generic RIBE scheme with the SD method, we show that if the underlying IBE, IBR, and HIBE schemes are adaptively (or selectively) secure under chosen plaintext attacks, then the proposed generic RIBE scheme is also adaptively (or selectively) secure under chosen plaintext attacks. The key idea of our proof is to first divide the types of an attacker according to the queries of the attacker, and to isolate the attacker of a specific type to break the security of the underlying IBE, IBR, or HIBE scheme. However, this idea is not simple to apply since the SD method has a complicated subset cover structure unlike the CS method. To handle this complicated structure in a ciphertext, we introduce additional hybrid games in the security proof and handle each ciphertext element of the challenge ciphertext one by one.

In addition, we show that it is possible to reduce the size of a ciphertext by extending the our generic RIBE scheme to use the more efficient LSD method instead of using the SD method. We also show that our generic RIBE scheme which provides only chosen-plaintext attack (CPA) security can be extended to provide the security against the more powerful chosen-ciphertext attacker (CCA). To provide the CCA security of RIBE, the underlying IBE, IBR, and HIBE schemes should provide the CCA security and a one-time signature scheme with strong unforgeability should be used.

1.2 Our Techniques

In order to design a generic RIBE scheme with the SD method, we first analyze the generic RIBE scheme with the CS method proposed by Ma and Lin [27]. The key design principle of their RIBE scheme with the CS method is that the identity *ID* of a receiver can be fixed to the path of a binary tree and a ciphertext is associated with the path set of the receiver's identity *ID* where as the private key of a user is associated with the path set of a binary tree in directly constructed many RIBE schemes. Therefore, if the receiver's identity *ID* is not revoked in the CS method, there is a common node in the path set of the binary tree and a node in the cover set of an update key. Thus, the equality function of IBE can be used to handle this common node since the path can be related to IBE ciphertexts and the cover set can be related to IBE private keys.

However, this design method is difficult to apply to the SD method. The reason is that in the SD method, unlike the CS method, there are no common nodes in the path set and the cover set. To solve this problem, we use the new interpretation of the SD method which was used for an efficient public-key revocation (PKR) scheme and RIBE scheme by using the SD method [20, 21]. To design an efficient PKR scheme, Lee et al. [20] observed that the subset $S_{i,j}$ of the SD method can be interpreted as a set of single member revocation instead of the existing interpretation that the subset $S_{i,j}$ is a set of leaf nodes where each leaf node belongs to the subtree $\mathcal{T}_i$ but does not belong to the subtree $\mathcal{T}_j$. That is, if we consider a group set GL which consists of all nodes of the subtree $\mathcal{T}_i$ that has the same depth as the node v_j, the subset $S_{i,j}$ can be interpreted as the same as GL except that the node v_j is excluded from GL. Thus, $S_{i,j}$ can be interpreted as single member revocation because it revokes one node v_j in GL.

This interesting observation was also used to directly construct an RIBE scheme with the SD method by Lee et al. [21]. They used a degree-one polynomial in the exponent to implement single member revocation. In this work, we found that IBE and IBR schemes can be combined in a generic way to achieve single member revocation if an RIBE ciphertext is associated with a path set PV for a receiver's identity ID and an RIBE update key is associated with a cover set CV for a revoked set R. That is, given the subset $S_{i,j}$, if we set a group label $GL = L_i \| d_j$ and a member label $ML = L_j$ where L_i, L_j are identifiers of nodes v_i, v_j and d_j is the depth of v_j, then all members of the group GL can be represented by a label pair (GL, ML). In this case, a label pair (GL, ML) in a ciphertext and another label pair (GL', ML') in an update key can be matching pairs if the group labels are equal but the member labels are different such that $GL = GL' \wedge ML \neq ML'$. Thus, we can support the equality $GL = GL'$ by using an IBE scheme, and we can support the inequality $ML \neq ML'$ by using an IBR scheme. In addition, to provide security against collusion attacks in the black-box construction, we divided the message M of a ciphertext into several secret shares by using a simple secret sharing scheme, and then encrypt these shares by using IBE and IBR schemes. Additionally, we use an HIBE scheme to provide the decryption key exposure resistance.

1.3 Related Work

Certificate Revocation. The study of certificate revocation in public-key encryption has been the subject of much research. In reality, the most widely used certificate revocation method is to periodically issue a certificate revocation list (CRL) containing serial numbers of revoked user's certificates. In addition, a delta-CRL can be used to more efficiently issue the revocation information, and it is also possible to immediately check the state of a certificate by using the online certificate status protocol (OCSP) service. In the theoretical aspect, various certificate revocation methods which are more efficient than the traditional methods also have been proposed [2, 28, 30].

Broadcast Encryption. Public-key broadcast encryption (PKBE) provides the revocation of receivers because a sender can specify a receiver set S in a ciphertext directly [6]. Identity-based broadcast encryption (IBBE) can provide more powerful revocation than existing PKBE because the maximum number of users in the system can be exponential [10]. Identity-based revocation (IBR) can be viewed as a cryptographic scheme that implements direct user revocation because all system users except the revoked users can decrypt a ciphertext where a revoked set R is specified in the ciphertext [23, 25]. However, PKBE, IBBE, and IBR have the disadvantage that a user cannot be revoked after the creation of a ciphertext. Particularly, it is a critical problem in a cryptographic system in which ciphertexts are stored in cloud storage and a user accesses these ciphertexts later since the user cannot be revoked when his or her credential is expired.

Revocable IBE. Boneh and Franklin [5] proposed a revocation method for IBE such that a trusted center periodically issues a private key for a user by combining an identity and time as $ID \| T$, but this method is not scalable since a secure channel should be established for every time. The efficient and scalable RIBE scheme was proposed by Boldyreva et al. [3] by combining the complete subtree (CS) method and a fuzzy identity-based encryption scheme. In their RIBE scheme, a ciphertext is associated with a receiver's identity D and time T, and a trusted center periodically issues an update key one time T for non-revoked users to implement the indirect key revocation. A number of secure and efficient RIBE schemes using a broadcast method for key updates have been proposed [8, 16, 26, 32, 35, 38, 39]. Most of the RIBE schemes follow the CS method for update keys, but Lee et al. [21] showed that an RIBE scheme with the SD method can be designed to reduces the size of update keys. Recently, Ma and Lin [27] proposed a generic RIBE construction with the CS method by combining IBE and HIBE schemes.

Revocable HIBE. The first revocable HIBE (RHIBE) scheme, which provides the private key revocation in HIBE, was proposed by Seo and Emura [34]. They proposed an RHIBE scheme by applying the design principle of previous RIBE schemes to an HIBE scheme. To improve the initially proposed RHIBE scheme, Seo and Emura later introduced a history-free update method to reduce the size of private keys and update keys [36]. After that, Lee and Park have introduced a new RHIBE scheme with short private keys and short updated keys by introducing an intermediate private key in HIBE and using a modular design method [24]. In order to enhance the selective security of previous RHIBE schemes, Lee [18] proposed an adaptively secure RHIBE scheme by applying the dual system encryption method of Waters [40], which was successfully used in adaptively secure IBE and HIBE schemes.

Revocable ABE. ABE is an extension of IBE in which a ciphertext is associated with attributes and a private key is associated with an access structure, and the ciphertext of ABE can be decrypted by the private key of ABE if the attributes satisfies the access structure [13]. An revocable ABE (RABE) scheme was proposed by Boldyreva et al. [3] by following the design principle of their RIBE scheme. ABE is well-suited for environments such as cloud storage where multiple users access different ciphertexts since it can provide flexible access control. For such an environment, Sahai et al. [33] proposed a revocable-storage ABE (RS-ABE) scheme that supports ciphertext updates as well as user key revocation. Lee et al. [18, 19] proposed an improved RS-ABE scheme by using a self-updatable encryption scheme, and they also proposed an RS-ABE scheme that provides the CCA security [22]. A generic construction of ABE with direct revocation in which a revoked set is attached in a ciphertext was proposed by Yamada et al. [41].

2 Preliminaries

In this section, we first review the definition and security model of IBE, IBR, and HIBE. Next, we review the definition and security model of RIBE.

2.1 Identity-Based Encryption

Identity-based encryption (IBE) is a kind of public key encryption (PKE) that can use a receiver's identity as a public key [5]. In IBE, a sender generates a ciphertext by encryption a message for the receiver's identity ID. A receiver retrieves a private key corresponding to his identity ID from a trusted center and then decrypts the ciphertext if the identity of the ciphertext is equal to the identity of the private key. The detailed syntax of IBE is given as follows.

Definition 2.1 (Identity-Based Encryption, IBE)**.** Let $\mathcal{I}$ be an identity space and $\mathcal{M}$ be a message space. An IBE scheme consists of four algorithms **Setup**, **GenKey**, **Encrypt**, and **Decrypt**, which are defined as follows:

Setup(1^{λ}): The setup algorithm takes as input a security parameter 1^{λ}. It outputs a master key MK and public parameters PP.

GenKey(ID, MK, PP): The private key generation algorithm takes as input an identity $ID \in \mathcal{I}$, the master key MK, and public parameters PP. It outputs a private key SK_{ID}.

Encrypt(ID, M, PP): The encryption algorithm takes as input an identity $ID \in \mathcal{I}$, a message $M \in \mathcal{M}$, and public parameters PP. It outputs a ciphertext CT_{ID}.

Decrypt$(CT_{ID}, SK_{ID'}, PP)$: The decryption algorithm takes as input a ciphertext CT_{ID}, a private key $SK_{ID'}$, and public parameters PP. It outputs a message M.

The correctness of IBE is defined as follows: For all MK and PP generated by **Setup**(1^{λ}), SK_{ID} generated by **GenKey**(ID, MK, PP) for any ID, and any ID and M, it is required that

- **Decrypt**$($**Encrypt**$(ID, M, PP), SK_{ID}, PP) = M$.

The security model of IBE is defined by extending the IND-CPA security model of PKE to allow additional private key queries [5]. In this model, an attacker can request a private key of an identity ID. In the challenge stage, the attacker submits a challenge identity ID^* and challenge messages M_0^*, M_1^*, and then receives a challenge ciphertext CT^*. The attacker further queries private keys and finally guesses the message hidden in CT^*. The detailed description of the security model of IBE is given as follows.

Definition 2.2 (IND-CPA Security)**.** The IND-CPA security of IBE is defined in terms of the following game between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$:

1. **Setup**: $\mathcal{C}$ generates a master key MK and public parameters PP by running **Setup**(1^{λ}). It keeps MK to itself and gives PP to $\mathcal{A}$.
2. **Phase 1**: $\mathcal{A}$ may adaptively request private keys for identities $ID_1, \dots, ID_{q_1}$. In response, $\mathcal{C}$ gives the corresponding private keys $SK_{ID_1}, \dots, SK_{ID_{q_1}}$ to $\mathcal{A}$ by running **GenKey**(ID_i, MK, PP).
3. **Challenge**: $\mathcal{A}$ submits a challenge identity ID^* and two messages M_0^*, M_1^* with the equal length subject to the restriction: for all ID_i of private key queries, $ID_i \neq ID^*$. $\mathcal{C}$ flips a random coin $\mu \in \{0,1\}$ and gives the challenge ciphertext CT^* to $\mathcal{A}$ by running **Encrypt**(ID^*, M_μ^*, PP).
4. **Phase 2**: $\mathcal{A}$ may continue to request private keys for $ID_{q_1+1}, \dots, ID_q$.
5. **Guess**: $\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$ of μ, and wins the game if $\mu = \mu'$.

The advantage of $\mathcal{A}$ is defined as $\mathrm{Adv}_{\mathcal{A}}^{IBE}(\lambda) = \left|\Pr[\mu = \mu'] - \frac{1}{2}\right|$ where the probability is taken over all the randomness of the game. An IBE scheme is IND-CPA secure if for all PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in the security parameter λ.

2.2 Identity-Based Revocation

Identity-based revocation (IBR) is a kind of public-key broadcast encryption (PKBE) [25], in which a large number of users with identities can participate to the system and a sender can specify the set R of revoked users in a ciphertext instead of the set S of receivers. In IBR, a sender generates a ciphertext CT by using a revoked set R and a message M, and then broadcasts the ciphertext. A receiver retrieves a private key for his or her identity from a trusted central and decrypt the ciphertext if his or her identity is not included in the set R. The detailed syntax of IBR is given as follows.

Definition 2.3 (Identity-Based Revocation, IBR)**.** An IBR scheme consists of four algorithms **Setup**, **GenKey**, **Encrypt**, and **Decrypt**, which are defined as follows:

Setup(1^{λ}): The setup algorithm takes as input a security parameter 1^{λ}. It outputs a master key MK and public parameters PP.

GenKey(ID, MK, PP): The private key generation algorithm takes as input an identity $ID \in \mathcal{I}$, the master key MK, and public parameters PP. It outputs a private key SK_{ID}.

Encrypt(R, M, PP): The encryption algorithm takes as input revoked identities $R \subset \mathcal{I}$, a message $M \in \mathcal{M}$, and public parameters PP. It outputs a ciphertext CT_R.

Decrypt(CT_R, SK_{ID}, PP): The decryption algorithm takes as input a ciphertext CT_R, a private key SK_{ID}, and public parameters PP. It outputs a message M.

The correctness of IBR is defined as follows: For all MK and PP generated by **Setup**(1^{λ}), SK_{ID} generated by **GenKey**(ID, MK, PP) for any ID, and any R such that $ID \notin R$ and any M, it is required that

- **Decrypt**$($**Encrypt**$(R, M, PP), SK_{ID}, PP) = M$.

The security model of IBR is defined by extending the IND-CPA security model of PKBE to account for the revoked set R [25]. In this model, an attacker requests private key queries on identities. In the challenge step, the attacker submits a challenge revoked set R^* and the challenge message M_0^*, M_1^* and receives a challenge ciphertext CT^*. The attacker additionally requests private key queries and finally guesses the hidden message in CT^*. In this game, all identities of private keys must belong to the revoked set R^*. The detailed description of the security model is given as follows.

Definition 2.4 (IND-CPA Security)**.** The IND-CPA security of IBR is defined in terms of the following game between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$:

1. **Setup**: $\mathcal{C}$ generates a master key MK and public parameters PP by running **Setup**(1^λ). It keeps MK to itself and gives PP to $\mathcal{A}$.

2. **Phase 1**: $\mathcal{A}$ may adaptively request private keys for identities $ID_1, \ldots, ID_{q_1}$. In response, $\mathcal{C}$ gives the corresponding private keys $SK_{ID_1}, \ldots, SK_{ID_{q_1}}$ to $\mathcal{A}$ by running **GenKey**(ID_i, MK, PP).

3. **Challenge**: $\mathcal{A}$ submits a challenge revoked set R^* of users and two messages M_0^*, M_1^* with the equal length subject to the restriction: for all ID_i of private key queries, $ID_i \in R^*$. $\mathcal{C}$ flips a random coin $\mu \in \{0,1\}$ and gives the challenge ciphertext CT^* to $\mathcal{A}$ by running **Encrypt**(R^*, M_μ^*, PP).

4. **Phase 2**: $\mathcal{A}$ may continue to request private keys for $ID_{q_1+1}, \ldots, ID_q$.

5. **Guess**: $\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$ of μ, and wins the game if $\mu = \mu'$.

The advantage of $\mathcal{A}$ is defined as $\mathrm{Adv}_{\mathcal{A}}^{IBR}(\lambda) = \left|\Pr[\mu = \mu'] - \frac{1}{2}\right|$ where the probability is taken over all the randomness of the game. An IBR scheme is IND-CPA secure if for all PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in the security parameter λ.

2.3 Hierarchical Identity-Based Encryption

Hierarchical identity-based encryption (HIBE) is an extension of IBE in which a hierarchical identity is used to represent a user's identity and the delegation of private keys is provided [12,15]. In HIBE, a user receives a private key for his hierarchical identity from a trusted center, or receives a delegated private key from another user. If a sender creates a ciphertext for a hierarchical identity $ID|_\ell$ and transmits it to a receiver, then the receiver can decrypt the ciphertext by using his private key if the hierarchical identity of the private key is a prefix of $ID|_\ell$. The detailed syntax of HIBE is given as follows.

Definition 2.5 (Hierarchical Identity-Based Encryption, HIBE)**.** An HIBE scheme consists of five algorithms **Setup**, **GenKey**, **Delegate**, **Encrypt**, and **Decrypt**, which are defined as follows:

Setup$(1^\lambda, L_{max})$. The setup algorithm takes as input a security parameter 1^λ and maximum hierarchical depth L_{max}. It outputs a master key MK and public parameters PP.

GenKey$(ID|_k, MK, PP)$. The key generation algorithm takes as input a hierarchical identity $ID|_k = (I_1, \ldots, I_k) \in \mathcal{I}^k$ where $k \leq L_{max}$, the master key MK, and the public parameters PP. It outputs a private key $SK_{ID|_k}$ for $ID|_k$.

Delegate$(ID|_k, SK_{ID|_{k-1}}, PP)$. The delegation algorithm takes as input a hierarchical identity $ID|_k$, a private key $SK_{ID|_{k-1}}$ for $ID|_{k-1}$, and the public parameters PP. It outputs a delegated private key $SK_{ID|_k}$ for $ID|_k$.

Encrypt$(ID|_\ell, M, PP)$. The encryption algorithm takes as input a hierarchical identity $ID|_\ell = (I_1, \ldots, I_\ell) \in \mathcal{I}^\ell$ where $\ell \leq L_{max}$, a message M, and public parameters PP. It outputs a ciphertext $CT_{ID|_\ell}$.

Decrypt$(CT_{ID|_\ell}, SK_{ID'|_k}, PP)$. The decryption algorithm takes as input a ciphertext $CT_{ID|_\ell}$, a private key $SK_{ID'_k}$, and public parameters PP. It outputs a message M.

The correctness of HIBE is defined as follows: For all MK, PP generated by **Setup**$(1^\lambda, L_{max})$, all $ID|_\ell, ID'|_k$, any $SK_{ID'|_k}$ generated by **GenKey**$(ID'|_k, MK, PP)$ such that $ID'|_k \in$ **Prefix**$(ID|_\ell)$, it is required that

- **Decrypt**$($**Encrypt**$(ID|_\ell, M, PP), SK_{ID'|_k}, PP) = M$.

The security model of HIBE is defined by extending the security model of IBE to include additional private key delegations [12, 15]. That is, an attacker can request delegated private key queries together with general private key queries. In this case, if the distribution of general private keys and the distribution of delegate private keys are the same, then we can only consider general private key queries to simplify the security model. The detailed security model of HIBE is given as follows.

Definition 2.6 (IND-CPA Security)**.** The IND-CPA security of HIBE is defined in terms of the following game between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$:

1. **Setup**: $\mathcal{C}$ generates a master key MK and public parameters PP by running **Setup**$(1^\lambda, L_{max})$. It keeps MK to itself and gives PP to $\mathcal{A}$.
2. **Phase 1**: $\mathcal{A}$ may adaptively request a polynomial number of private key queries. In response, $\mathcal{C}$ gives a corresponding private key $SK_{ID|_k}$ to $\mathcal{A}$ by running **GenKey**(ID_i, MK, PP) for each query.
3. **Challenge**: $\mathcal{A}$ submits a challenge hierarchical identity $ID^*|_\ell$ and two messages M_0^*, M_1^* with the equal length subject to the restriction: for each $ID|_k$ of private key queries, $ID|_k \notin$ **Prefix**$(ID^*|_\ell)$. $\mathcal{C}$ flips a random coin $\mu \in \{0,1\}$ and gives a challenge ciphertext CT^* to $\mathcal{A}$ by running **Encrypt**$(ID^*|_\ell, M_\mu^*, PP)$.
4. **Phase 2**: $\mathcal{A}$ may continue to request private key queries.
5. **Guess**: $\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$ of μ, and wins the game if $\mu = \mu'$.

The advantage of $\mathcal{A}$ is defined as $\mathrm{Adv}_{\mathcal{A}}^{HIBE}(\lambda) = \big|\Pr[\mu = \mu'] - \frac{1}{2}\big|$ where the probability is taken over all the randomness of the game. An HIBE scheme is IND-CPA secure if for all PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in the security parameter λ.

2.4 Revocable Identity-Based Encryption

Revocable identity-based encryption (RIBE) is an extension of existing identity-based encryption (IBE) to support private key revocation [3]. In RIBE, each user receives a private key for his or her identity ID from a trusted center. The trusted center then periodically generates an update key which is associated with time T and a non-revoked user set, and then it broadcasts the update key through the public channel. In this case, if the private key of a user is not revoked in the update key, the user can derive a decryption key for ID and T by combining the private key and the update key, and this decryption key can be used to decrypt a ciphertext which is related with ID and T. The syntax of RIBE is given as follows.

Definition 2.7 (Revocable IBE, RIBE)**.** An RIBE scheme consists of seven algorithms **Setup**, **GenKey**, **UpdateKey**, **DeriveKey**, **Encrypt**, **Decrypt**, and **Revoke**, which are defined as follows:

Setup(1^λ): The setup algorithm takes as input a security parameter 1^λ. It outputs a master key MK, an (empty) revocation list RL, and public parameters PP.

GenKey(ID, MK, PP): The private key generation algorithm takes as input an identity $ID \in \mathcal{I}$, the master key MK, and public parameters PP. It outputs a private key SK_{ID}.

UpdateKey(T, RL, MK, PP): The update key generation algorithm takes as input update time $T \in \mathcal{T}$, the revocation list RL, the master key MK, and public parameters PP. It outputs an update key UK_T.

DeriveKey(SK_{ID}, UK_T, PP): The decryption key derivation algorithm takes as input a private key SK_{ID}, an update key UK_T, and public parameters PP. It outputs a decryption key $DK_{ID,T}$.

Encrypt(ID, T, M, PP): The encryption algorithm takes as input an identity $ID \in \mathcal{I}$, time T, a message $M \in \mathcal{M}$, and public parameters PP. It outputs a ciphertext $CT_{ID,T}$.

Decrypt$(CT_{ID,T}, DK_{ID',T'}, PP)$: The decryption algorithm takes as input a ciphertext $CT_{ID,T}$, a decryption key $DK_{ID',T'}$, and public parameters PP. It outputs a message M.

Revoke(ID, T, RL): The revocation algorithm takes as input an identity ID to be revoked and revocation time T, and a revocation list RL. It outputs an updated revocation list RL.

The correctness of RIBE is defined as follows: For all MK, RL, and PP generated by **Setup**(1^λ), SK_{ID} generated by **GenKey**(ID, MK, PP) for any ID, UK_T generated by **UpdateKey**(T, RL, MK, PP) for any T and RL such that $(ID, T_j) \notin RL$ for all $T_j \leq T$, $CT_{ID,T}$ generated by **Encrypt**(ID, T, M, PP) for any ID, T, and M, it is required that

- **Decrypt**$(CT_{ID,T}, $ **DeriveKey**$(SK_{ID}, UK_T, PP), PP) = M$.

The security model of RIBE was first defined by Boldyreva et al. [3], and then this security model was extended by Seo and Emura [35] to support decryption key exposure resistance. In the security model of RIBE, an attacker can request a private key query for an identity ID, an update key query for time T, a decryption key query for ID and T, and a revocation query. In the challenge step, the attacker submits a challenge identity ID^*, challenge time T^*, and challenge messages M_0^*, M_1^*, and receives a challenge ciphertext CT^*. Note that the private key query for ID^* is not allowed in the IBE security model, but this private key query for ID^* is allowed in the RIBE security model. At this time, if the private key for ID^* is queried, then the private key for ID^* must be revoked in the update key on the challenge time T^*. The detailed definition of the RIBE security model is given as follows.

Definition 2.8 (IND-CPA Security)**.** The IND-CPA security of RIBE is defined in terms of the following experiment between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$:

1. **Setup**: $\mathcal{C}$ generates a master key MK, a revocation list RL, a state ST, and public parameters PP by running **Setup**(1^λ). It keeps MK, RL to itself and gives PP to $\mathcal{A}$.

2. **Phase 1**: $\mathcal{A}$ adaptively request a polynomial number of queries. These queries are processed as follows:

   - If this is a private key query for an identity ID, then it gives the corresponding private key SK_{ID} to $\mathcal{A}$ by running **GenKey**(ID, MK, PP).

- If this is an update key query for time T, then it gives the corresponding update key $UK_{T,R}$ to $\mathcal{A}$ by running **UpdateKey**(T, RL, MK, PP).
- If this is a decryption key query for an identity ID and time T, then it gives the corresponding decryption key $DK_{ID,T}$ to $\mathcal{A}$ by running **DeriveKey**(SK_{ID}, UK_T, PP).
- If this is a revocation query for an identity ID and revocation time T, then it updates the revocation list RL by running **Revoke**(ID, T, RL, ST) with the restriction: The revocation query for time T cannot be queried if the update key query for the time T was already requested.

Note that we assume that the update key queries and the revocation queries are requested in non-decreasing order of time.

3. **Challenge**: $\mathcal{A}$ submits a challenge identity ID^*, challenge time T^*, and two challenge messages M_0^*, M_1^* with equal length with the following restrictions:

   - If a private key query for an identity ID such that $ID = ID^*$ was requested, then the identity ID^* should be revoked at some time T such that $T \leq T^*$.
   - The decryption key query for ID^* and T^* was not requested.

   $\mathcal{C}$ flips random $\mu \in \{0,1\}$ and obtains a ciphertext CT^* by running **Encrypt**(ID^*, T^*, M_μ^*, PP). It gives CT^* to $\mathcal{A}$.

4. **Phase 2**: $\mathcal{A}$ may continue to request a polynomial number of additional queries subject to the same restrictions as before.

5. **Guess**: Finally, $\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$, and wins the game if $\mu = \mu'$.

The advantage of $\mathcal{A}$ is defined as $\text{Adv}_{\mathcal{A}}^{RIBE}(\lambda) = \left|\Pr[\mu = \mu'] - \frac{1}{2}\right|$ where the probability is taken over all the randomness of the experiment. An RIBE scheme is IND-CPA secure if for all PPT adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in the security parameter λ.

3 Revocable IBE with SD

In this section, we first review the perfect binary tree and the subset difference method, and then we propose a generic construction for RIBE by combining subset difference, IBE, IBR, and HIBE schemes.

3.1 Binary Tree

A perfect binary tree $\mathcal{BT}$ is a tree data structure in which all internal nodes have two child nodes and all leaf nodes have the same depth. Let $N = 2^n$ be the number of leaf nodes in $\mathcal{BT}$. The number of all nodes in $\mathcal{BT}$ is $2N-1$ and we denote v_i as a node in $\mathcal{BT}$ for any $1 \leq i \leq 2N-1$. The depth d_i of a node v_i is the length of the path from a root node to the node. The root node of a tree has depth zero. The depth of $\mathcal{BT}$ is the length of the path from the root node to a leaf node. A level of $\mathcal{BT}$ is a set of all nodes at given depth.

Each node $v_i \in \mathcal{BT}$ has an identifier $L_i \in \{0,1\}^*$ which is a fixed and unique string. An identifier of each node is assigned as follows: Each edge in the tree is assigned with 0 or 1 depending on whether it is connected to the left or right child node. The identifier L_i of a node v_i is obtained by reading all labels of edges in a path from the root node to the node v_i. The root node has an empty identifier ε. For a node v_i, we define **Label**(v_i) be the identifier of v_i and **Depth**(v_i) be the depth d_i of v_i.

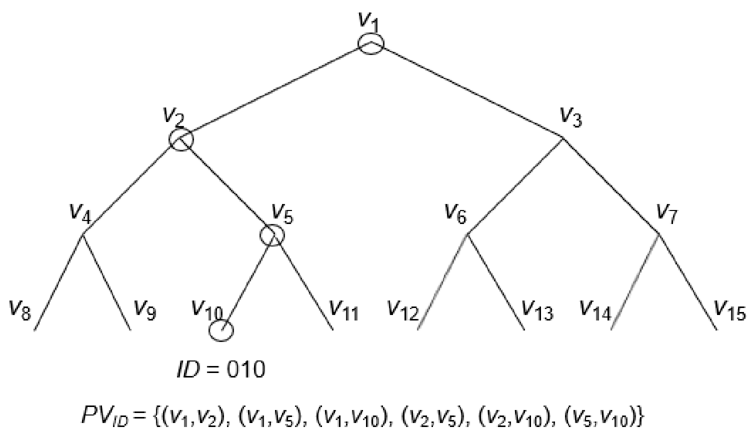

Figure 1: A path set for $ID = 010$ in the SD method

A subtree $\mathcal{T}_i$ in $\mathcal{BT}$ is defined as a tree that is rooted at a node $v_i \in \mathcal{BT}$. A subset S_i is defined as a set of all leaf nodes in $\mathcal{T}_i$. For any two nodes $v_i, v_j \in \mathcal{BT}$ where v_j is a descendant of v_i, $\mathcal{T}_{i,j}$ is defined as a subtree $\mathcal{T}_i - \mathcal{T}_j$, that is, all nodes that are descendants of v_i but not v_j. A subset $S_{i,j}$ is defined as the set of leaf nodes in $\mathcal{T}_{i,j}$, that is, $S_{i,j} = S_i \setminus S_j$.

For a perfect binary tree $\mathcal{BT}$ and a subset R of leaf nodes, $ST(\mathcal{BT}, R)$ is defined as the Steiner Tree induced by the set R and the root node, that is, the minimal subtree of $\mathcal{BT}$ that connects all the leaf nodes in R and the root node.

3.2 Subset Difference Method

The subset difference (SD) method is one instance of the subset cover (SC) framework proposed by Naor et al. [29] which was used for efficient symmetric key broadcast encryption. The SD method is more efficient than the complete subtree (CS) method because the size of the cover set representing the non-revoked users is smaller than that of the CS method. We follow the SD definition of Lee et al. [20]. The SD method uses a perfect binary tree and each user is located at a leaf node in the binary tree. The **Assign** algorithm computes a path set PV, which is consists of subsets associated with the path from the root node to a user's leaf node. The **Cover** algorithm derives a cover set CV that can effectively cover non-revoked leaf nodes. The **Match** algorithm can derive two related subsets if a user's leaf node is not revoked in the cover set. A simple example of the SD method is given in Figure 1 and 2. A detailed description of the SD method is given as follows.

SD.Setup(N**):** Let $N = 2^n$ be the number of leaf nodes. It sets a perfect binary tree $\mathcal{BT}$ of depth n and outputs $\mathcal{BT}$. Note that a user is assigned to a leaf node in $\mathcal{BT}$ and the collection $\mathcal{S}$ of SD is the set of all subsets $\{S_{i,j}\}$ where $v_i, v_j \in \mathcal{BT}$ and v_j is a descendant of v_i.

SD.Assign($\mathcal{BT}, v$**):** Let v be the leaf node of $\mathcal{BT}$ that is assigned to a user ID. Let $(v_{k_0}, v_{k_1}, \ldots, v_{k_n})$ be a path from the root node v_{k_0} to the leaf node $v_{k_n} = v$. It initializes a path set PV as an empty one. For all $i, j \in \{k_0, \ldots, k_n\}$ such that v_j is a descendant of v_i, it adds a subset $S_{i,j}$ defined by two nodes v_i and v_j in the path into PV. It outputs the path set $PV = \{S_{i,j}\}$.

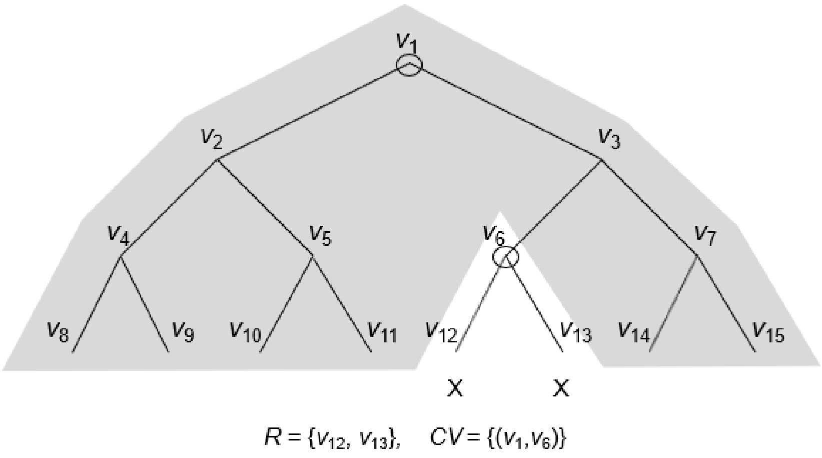

Figure 2: A cover set for $R = \{v_{12}, v_{13}\}$ in the SD method

SD.Cover($\mathcal{BT}, R$): Let R be a revoked set of leaf nodes (or users). It first sets a subtree $\mathcal{T}$ as $ST(\mathcal{BT}, R)$, and then it builds a cover set CV iteratively by removing nodes from $\mathcal{T}$ until $\mathcal{T}$ consists of just a single node as follows:

1. It finds two leaf nodes v_i and v_j in $\mathcal{T}$ such that the least-common-ancestor v of v_i and v_j does not contain any other leaf nodes of $\mathcal{T}$ in its subtree. Let v_l and v_k be the two child nodes of v such that v_i is a descendant of v_l and v_j is a descendant of v_k. If there is only one leaf node left, it makes $v_i = v_j$ to the leaf node, v to be the root of $\mathcal{T}$ and $v_l = v_k = v$.
2. If $v_l \neq v_i$, then it adds the subset $S_{l,i}$ to CV; likewise, if $v_k \neq v_j$, it adds the subset $S_{k,j}$ to CV_R.
3. It removes from $\mathcal{T}$ all the descendants of v and makes v a leaf node.

It outputs the cover set $CV = \{S_{i,j}\}$.

SD.Match(CV, PV): Let $CV = \{S_{i,j}\}$ and $PV = \{S_{i,j}\}$. It finds two subsets $S_{i,j} \in CV$ and $S_{i',j'} \in PV$ such that $(v_i = v_{i'}) \wedge (d_j = d_{j'}) \wedge (v_j \neq v_{j'})$ where d_j is the depth of v_j. If two subsets exist, then it outputs $(S_{i,j}, S_{i',j'})$. Otherwise, it outputs $\perp$.

The correctness of the SD scheme requires that if $v \notin R$, then **SD.Match**$(CV, PV) = (S_{i,j}, S_{i',j'})$ such that $(v_i = v_{i'}) \wedge (d_j = d_{j'}) \wedge (v_j \neq v_{j'})$ where $S_{i,j}$ is defined by two nodes v_i and v_j.

3.3 Generic Construction

Let **IBE** = (**Setup**, **GenKey**, **Encrypt**, **Decrypt**) be an IBE scheme, **IBR** = (**Setup**, **GenKey**, **Encrypt**, **Decrypt**) be an IBR scheme that supports a single revoked identity, and **HIBE** = (**Setup**, **GenKey**, **Delegate**, **Encrypt**, **Decrypt**) be a two-level HIBE scheme. We define **GMLabels**$(S_{i,j}) = (GL = \textbf{Label}(v_i) \| \textbf{Depth}(v_j), ML = \textbf{Label}(v_j))$ where GL is a group label and ML is a member label. A simple example of a group of nodes derived from a subset $S_{i,j}$ is given in Figure 3. A generic RIBE scheme using the SD method is described as follows.

RIBE.Setup(1^λ): Let $\mathcal{I} = \{0,1\}^n$ be the identity space.

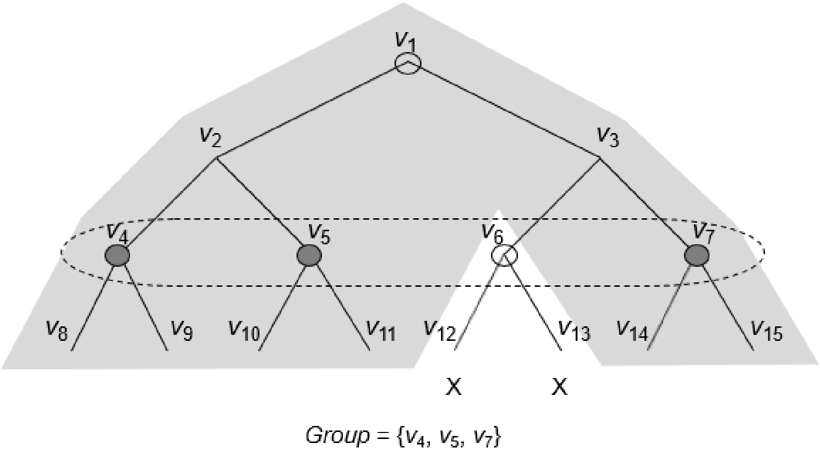

Figure 3: A single member revoked group from the subset $S_{1,6} = (v_1, v_6)$

1. It first obtains MK_{IBE}, PP_{IBE} by running **IBE.Setup**(1^λ). It obtains MK_{IBR}, PP_{IBR} by running **IBR.Setup**(1^λ). It also obtains MK_{HIBE}, PP_{HIBE} by running **HIBE.Setup**$(1^\lambda, 2)$.
2. It defines a binary tree $\mathcal{BT}$ by running **SD.Setup**(2^n) where an identity $ID \in \mathcal{I}$ is uniquely assigned to a leaf node v such that **Label**$(v) = ID$.
3. It outputs a master key $MK = (MK_{IBE}, MK_{IBR}, MK_{HIBE})$, a revocation list $RL = \emptyset$, and public parameters $PP = (PP_{IBE}, PP_{IBR}, PP_{HIBE}, \mathcal{BT})$.

RIBE.GenKey(ID, MK, PP**):** To generate a private key for ID, it proceeds as follows:

1. It obtains SK_{HIBE} by running **HIBE.GenKey**$((ID), MK_{HIBE}, PP_{HIBE})$.
2. Finally, it outputs a private key $SK_{ID} = SK_{HIBE}$.

RIBE.UpdateKey(T, RL, MK, PP**):** To generate an update key for T, it proceeds as follows:

1. It initializes $RV = \emptyset$. For each $(ID_j, T_j) \in RL$, it adds a leaf node $v_j \in \mathcal{BT}$ which is associated with ID_j into RV if $T_j \leq T$. It obtains CV_T by running **SD.Cover**$(\mathcal{BT}, RV)$.
2. For each $S_{i,j} \in CV_T$, it sets labels $(GL, ML) =$ **GMLabels**$(S_{i,j})$ and performs: It obtains $SK_{IBE,S_{i,j}}$ by running **IBE.GenKey**$(GL\|T, MK_{IBE}, PP_{IBE})$ and $SK_{IBR,S_{i,j}}$ by running **IBR.GenKey**$(ML\|T, MK_{IBR}, PP_{IBR})$.
3. Finally, it outputs an update key $UK_T = \big(CV_T, \{(SK_{IBE,S_{i,j}}, SK_{IBR,S_{i,j}})\}_{S_{i,j} \in CV_T}\big)$.

RIBE.DeriveKey(SK_{ID}, UK_T, PP**):** Let $SK_{ID} = SK_{HIBE}$. To derive a decryption key for ID and T, it proceeds as follows:

1. It obtains DK_{HIBE} by running **HIBE.Delegate**$((ID, T), SK_{HIBE}, PP_{HIBE})$.
2. Finally, it outputs a decryption key $DK_{ID,T} = (UK_T, DK_{HIBE})$.

RIBE.Encrypt(ID, T, M, PP**):** To generate a ciphertext for ID and T, it proceeds as follows:

1. It selects random R_1 and sets $R_2 = M \oplus R_1$. It obtains CT_{HIBE} by running **HIBE.Encrypt**$((ID, T), R_2, PP_{HIBE})$.

2. Let v_{ID} be a leaf node associated with ID such that $ID = \textbf{Label}(v_{ID})$. It obtains PV_{ID} by running $\textbf{SD.Assign}(\mathcal{BT}, v_{ID})$.
3. For each $S_{i,j} \in PV_{ID}$, it sets labels $(GL, ML) = \textbf{GMLabels}(S_{i,j})$ and performs:
   (a) It selects random $R_{3,S_{i,j}}$ and sets $R_{4,S_{i,j}} = R_1 \oplus R_{3,S_{i,j}}$.
   (b) It obtains $CT_{IBE,S_{i,j}}$ by running $\textbf{IBE.Encrypt}(GL \| T, R_{3,S_{i,j}}, PP_{IBE})$ and obtains $CT_{IBR,S_{i,j}}$ by running $\textbf{IBR.Encrypt}(ML \| T, R_{4,S_{i,j}}, PP_{IBR})$.

   It creates $CT_{PV} = \big(PV_{ID}, \{(CT_{IBE,S_{i,j}}, CT_{IBR,S_{i,j}})\}_{S_{i,j} \in PV_{ID}}\big)$.
4. Finally, it outputs a ciphertext $CT_{ID,T} = (CT_{PV}, CT_{HIBE})$.

RIBE.Decrypt($CT_{ID,T}, DK_{ID',T'}, PP$): Let $CT_{ID,T} = (CT_{PV}, CT_{HIBE})$ and $DK_{ID',T'} = (UK_T, DK_{HIBE})$. It proceeds as follows:

1. It first obtains R_2 by running $\textbf{HIBE.Decrypt}(CT_{HIBE}, DK_{HIBE}, PP_{HIBE})$.
2. It finds $(S_{i,j}, S_{i',j'}) = \textbf{SD.Match}(PV_{ID}, CV_T)$. It retrieves $CT_{IBE,S_{i,j}}, CT_{IBR,S_{i,j}}$ from CT_{PV} and $SK_{IBE,S_{i',j'}}, SK_{IBR,S_{i',j'}}$ from UK_T. Next, it obtains R_3 by running $\textbf{IBE.Decrypt}(CT_{IBE,S_{i,j}}, SK_{IBE,S_{i',j'}}, PP_{IBE})$ and obtains R_4 by running $\textbf{IBR.Decrypt}(CT_{IBR,S_{i,j}}, SK_{IBR,S_{i',j'}}, PP_{IBR})$.
3. Finally, it outputs a message $M = R_3 \oplus R_4 \oplus R_2$.

RIBE.Revoke(ID, T, RL): If $(ID, *)$ already exists in RL, it outputs RL. Otherwise, it adds (ID, T) to RL and outputs the updated RL.

3.4 Correctness

The correctness of the above RIBE scheme can be easily seen by using the correctness of the underlying IBE, IBR, HIBE and SD schemes. Let $CT_{ID,T} = (CT_{PV}, CT_{HIBE})$ be a ciphertext associated with ID and T, and $DK_{ID',T'} = (UK_T, DK_{HIBE})$ be a decryption key is associated with ID' and T'. In this case, if the condition $ID = ID' \wedge T = T'$ is satisfied, then the random R_2 is correctly decrypted by running $\textbf{HIBE.Decrypt}(CT_{HIBE}, SK_{HIBE}, PP_{HIBE})$ because of the correctness of HIBE.

Now we show that random R_1 can be correctly decrypted from CT_{PV} and UK_T if the identity ID of the ciphertext is not revoked in the update key UK_T. Recall that the ciphertext CT_{PV} is associated with PV_{ID} and the update key UK_T is associated with CV_T. By the correctness of the SD scheme, the **SD.Match** algorithm outputs two subsets of $S_{i,j}, S_{i',j'}$ such that $(v_i = v_{i'}) \wedge (d_j = d_{j'}) \wedge (v_j \neq v_{j'})$ if the leaf node v_{ID} is not included in the revoked set RV. Let $(CT_{IBE,S_{i,j}}, CT_{IBR,S_{i,j}}) \in CT_{PV}$ and $(SK_{IBE,S_{i',j'}}, SK_{IBR,S_{i',j'}}) \in UK_T$ be corresponding tuples of $S_{i,j}$ and $S_{i',j'}$ respectively. From the definition of **GMLabels**, labels $(GL, ML) = \textbf{GMLabels}(S_{i,j})$ and $(GL', ML') = \textbf{GMLabels}(S_{i',j'})$ are obtained and they satisfy $GL = GL' \wedge ML \neq ML'$. Therefore, if the time T of the ciphertext is the same as the time T' of the update key, then random R_3 can be decrypted by running $\textbf{IBE.Decrypt}(CT_{IBE,S_{i,j}}, SK_{IBE,S_{i',j'}}, PP_{IBE})$ because of $GL \| T = GL' \| T'$ and random R_4 can be decrypted by running $\textbf{IBR.Decrypt}(CT_{IBR,S_{i,j}}, SK_{IBR,S_{i',j'}}, PP_{IBR})$ because of $ML \| T \neq ML' \| T'$. Therefore, random R_1 is obtained from $R_3 \oplus R_4$.

3.5 Discussions

Layered Subset Difference. Since our generic RIBE scheme uses the SD method, the size of a ciphertext depends on the size of the PV set and the size of an update key depends on the size of the CV set in the SD method. Thus, the ciphertext and update key of generic RIBE consists of approximately $O(n^2)$ IBE ciphertexts and $2r$ IBE private keys respectively where n is the bit length of identity and r is the number of revoked users. In order to reduce the size of ciphertexts in this generic RIBE scheme, we can apply the layered subset difference (LSD) method of Halevy and Shamir [14]. If the LSD method is used instead of the SD method, the ciphertext and the update key of this general RIBE scheme consists of $O(n^{1.5})$ IBE ciphertexts and $4r$ IBE private keys, respectively.

Chosen-Ciphertext Security. The CCA security model, which is stronger than the CPA security model, allows an adversary to request decryption queries on ciphertexts. The above generic RIBE construction only can derive a CPA secure RIBE scheme by using CPA secure IBE, IBR, and HIBE schemes as building blocks. To derive a CCA secure RIBE scheme, we may try to use CCA secure encryption primitives as building blocks. However, this simple construction can not be CCA secure because it allows ciphertext elements reordering attacks. To solve this problem, we apply the CCA methodology for multiple encryption proposed by Dodis and Katz [11]. That is, a CCA secure RIBE scheme can be constructed by combining CCA secure IBE, IBR, HIBE schemes with a one-time signature (OTS) scheme with strong unforgeability. At this time, the underlying IBE, IBR, and HIBE schemes should be modified to receive additional labels as inputs since the public key of OTS should be tied with ciphertexts. This approach also provides the decryption key exposure resistance (DKER) property since a decryption key is generated by using the delegation property of HIBE.

4 Security Analysis

In this section, we prove the IND-CPA security of the generic RIBE construction proposed in the previous section. The basic idea of this proof is to show that if there is an attacker that breaks the IND-CPA security of the RIBE scheme, then we can construct an algorithm that breaks the IND-CPA security of underlying IBE, IBR, or HIBE schemes. In order to simplify the security proof, we try to prove the security by separating the attacker into two types. That is, the Type-I attacker does not request a private key query on the challenge identity ID^*, and the Type-II attacker requests a private key query on the identity ID^*.

First, since the Type-I attacker does not query the private key for the identity ID^*, we perform the proof that relates the security of the underlying HIBE scheme with the security of the RIBE scheme. Next, since the Type-II attacker queries the private key for ID^*, we perform the proof that relates the security of the underlying IBE or IBR scheme and the security of the RIBE scheme.

Theorem 4.1. *The generic RIBE scheme is IND-CPA secure if the underlying IBE, IBR, and HIBE schemes are IND-CPA secure.*

Proof. Let ID^* be the challenge identity and T^* be the challenge time. We divide the behavior of an adversary as two types: Type-I and Type-II, which are defined as follows:

Type-I. An adversary is Type-I if it requests a private key for $ID \neq ID^*$ for all private key queries. In this case, the adversary can request a decryption key for ID and T such that $ID \neq ID^*$ or $ID = ID^* \wedge T \neq T^*$.

Type-II. An adversary is Type-II if it requests a private key for $ID = ID^*$ for some private key query. In this case, the private key for ID^* should be revoked at some time T such that $T \leq T^*$ by the restriction of the security model.

Let E_i be the event that $\mathcal{A}$ behaves like Type-i adversary. From Lemmas 4.2 and 4.3, we obtain the following result

$$\begin{aligned}\mathrm{Adv}_{\mathcal{A}}^{RIBE}(\lambda) &\leq \Pr[E_I] \cdot \mathrm{Adv}_{\mathcal{A}}^{RIBE}(\lambda) + \Pr[E_{II}] \cdot \mathrm{Adv}_{\mathcal{A}}^{RIBE}(\lambda) \\ &\leq \mathrm{Adv}_{\mathcal{B}}^{HIBE}(\lambda) + O(n^2)\big(\mathrm{Adv}_{\mathcal{B}}^{IBE}(\lambda) + \mathrm{Adv}_{\mathcal{B}}^{IBR}(\lambda)\big).\end{aligned}$$

This completes our proof. □

4.1 Type-I Adversary

The Type-I attacker does not request a private key query on the challenge ID^*, but can request decryption key queries such that $ID = ID^*$ and $T \neq T^*$. To deal with this attacker, we build a reduction algorithm that attacks the HIBE scheme and selects the other IBE and IBR schemes by itself. In this case, this algorithm will be able to handle all queries of the Type-I attacker by using the queries for the HIBE scheme. The detailed proof is as follows.

Lemma 4.2. *For the Type-I adversary, the generic RIBE scheme is IND-CPA secure if the HIBE scheme is IND-CPA secure.*

Proof. Suppose there exists an adversary $\mathcal{A}$ that attacks the RIBE scheme with a non-negligible advantage. An algorithm $\mathcal{B}$ that attacks the HIBE scheme is initially given public parameters PP_{HIBE} by a challenger $\mathcal{C}$. Then $\mathcal{B}$ that interacts with $\mathcal{A}$ is described as follows:

Setup: $\mathcal{B}$ generates MK_{IBE}, PP_{IBE} by running the **IBE.Setup** algorithm, generates MK_{IBR}, PP_{IBR} by running the **IBR.Setup** algorithm. It initializes $RL = \emptyset$ and gives $PP = (PP_{IBE}, PP_{IBR}, PP_{HIBE})$ to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ adaptively requests a polynomial number of private key, update key, decryption key, and revocation queries.

- For a private key query with an identity ID, $\mathcal{B}$ proceeds as follows: It receives SK_{HIBE} from $\mathcal{C}$ by querying a private key for ID since $ID \neq ID^*$ by the restriction of the Type-I adversary. It gives $SK_{ID} = SK_{HIBE}$ to $\mathcal{A}$.

- For an update key query with time T, $\mathcal{B}$ proceeds as follows: It simply generates UK_T by running the **RIBE.UpdateKey** algorithm since it knows MK_{IBE} and MK_{IBR}. It gives UK_T to $\mathcal{A}$.

- For a decryption key query with an identity ID and time T, $\mathcal{B}$ proceeds as follows:

  1. It generates UK_T by running the **RIBE.UpdateKey** algorithm since it knows MK_{IBE} and MK_{IBR}.
  2. It receives DK_{HIBE} from $\mathcal{C}$ by querying a private key for ID and T since $ID \neq ID^*$ or $ID = ID^* \wedge T \neq T^*$ by the restriction of the Type-I adversary.
  3. It gives $DK_{ID,T} = (UK_T, DK_{HIBE})$ to $\mathcal{A}$.

- For a revocation query with an identity ID and time T, $\mathcal{B}$ proceeds as follows: It adds (ID, T) to RL if ID was not revoked before.

Challenge: $\mathcal{A}$ submits a challenge identity ID^*, challenge time T^*, and two challenge messages M_0^*, M_1^*. $\mathcal{B}$ proceeds as follows:

1. It first select random R_1 and sets $R_{2,0} = M_0^* \oplus R_1, R_{2,1} = M_1^* \oplus R_1$.

2. Next, it receives CT^*_{HIBE} from $\mathcal{C}$ by submitting ID^*, T^*, and two challenge messages $R_{2,0}, R_{2,1}$.
3. To creates CT^*_{PV} for ID^* and T^*, it simply follows the procedures in the **RIBE.Encrypt** algorithm with the random R_1 input.
4. It gives a challenge ciphertext $CT^* = (CT^*_{PV}, CT^*_{HIBE})$ to $\mathcal{A}$.

Phase 2: Same as Phase 1.
Guess: Finally, $\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$. $\mathcal{B}$ also outputs μ'. □

4.2 Type-II Adversary

Since the Type-II attacker requests a private key query on the challenge ID^*, we can not handle the private key queries of the RIBE scheme by using the private key queries of the HIBE scheme in the proof. Therefore, we prove the security by relating the security of the IBE and IBR schemes with the security of the RIBE scheme against the Type-II attacker.

The main idea of the proof is to take advantage of the restriction of the RIBE security model such that if the attacker queries the private key for the challenge identity ID^*, then the corresponding private key for ID^* must be revoked from the update key on the challenge time T^*. Thus, the ciphertext CT^*_{PV} in the challenge ciphertext consists of the IBE and IBR ciphertexts associated with the subset $S_{i,j}$ belonging to the path set PV_{ID^*}, but the IBE and IBR private keys that can decrypt the corresponding ciphertext elements in CT^*_{PV} are not included in the update key for T^* because of the restriction. Using this fact, we can prove the security of the RIBE scheme against the Type-II attacker by using the security of the IBE or IBR scheme.

We prove the security by using hybrid games consisting of multiple sub-games because the ciphertext CT^*_{PV} is composed of many IBE and IBR ciphertexts. That is, in the hybrid games, a ciphertext which encrypts a random value related to M^*_0 is changed to another ciphertext which encrypts a random value related to M^*_1. In this hybrid steps, since the number of IBE and IBR ciphertext pairs in CT^*_{PV} is maximum $O(n^2)$, the proof can be completed by performing $O(n^2)$ hybrid games. The detailed proof is described as follows.

Lemma 4.3. *For the Type-II adversary, the generic RIBE scheme is IND-CPA secure if the IBE and IBR schemes are IND-CPA secure.*

Proof. Let ID^* be the challenge identity and PV_{ID^*} be the path set of ID^* where the number of subsets in PV_{ID^*} is $\ell = n(n-1)/2$. The challenge ciphertext is formed as $CT^* = (CT^*_{PV}, CT^*_{HIBE})$ where $CT^*_{PV} = (PV_{ID^*}, \{(CT^*_{IBE,S_{i_k,j_k}}, CT^*_{IBR,S_{i_k,j_k}})\}_{k=1}^{\ell})$. For the security proof, we define hybrid games $\mathbf{G}_0, \mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3$ as follows:

Game $\mathbf{G}_0$. This game is the original security game defined in the security model except that the challenge bit μ is fixed to 0.

Game $\mathbf{G}_1$. This game is the same as the game $\mathbf{G}_0$ except that the settings of random R_1 and R_2 in the challenge ciphertext are changed. That is, R_2 are randomly chosen and R_1 is set as $M^*_0 \oplus R_2$.

Game $\mathbf{G}_2$ In this game, the generation of CT^*_{PV} in the challenge ciphertext CT^* is changed. That is, a random $R'_1 = M^*_1 \oplus R_2$ is encrypted instead of $R_1 = M^*_0 \oplus R_2$ to generate CT^*_{PV}.

For the analysis of security, we define additional sub-games $\mathbf{H}_0, \ldots, \mathbf{H}_\rho, \ldots, \mathbf{H}_\ell$ where $\mathbf{H}_0 = \mathbf{G}_1$ and $\mathbf{H}_\ell = \mathbf{G}_2$. The game $\mathbf{H}_\rho$ is similar to the game $\mathbf{H}_{\rho-1}$ except that the tuple $(CT^*_{IBE,S_{i_\rho,j_\rho}}, CT^*_{IBR,S_{i_\rho,j_\rho}})$ is an encryption on the random $R'_1 = M^*_1 \oplus R_2$. Specifically, each tuple $(CT^*_{IBE,S_{i_k,j_k}}, CT^*_{IBR,S_{i_k,j_k}})$ for $k \leq \rho$ is an encryption on the random $R'_1 = M^*_1 \oplus R_2$ and each tuple $(CT^*_{IBE,S_{i_k,j_k}}, CT^*_{IBR,S_{i_k,j_k}})$ for $k > \rho$ is an encryption on the random $R_1 = M^*_0 \oplus R_2$.

In the game $\mathbf{H}_\rho$, we let $(GL^*, ML^*) = \mathbf{GMLabels}(S_{i_\rho,j_\rho})$ of $S_{i_\rho,j_\rho} \in PV_{ID^*}$ where CT^*_{PV} is related with PV_{ID^*}. We divide the adversary as the following sub-types:

- An adversary is **Type-II-A** if it requests an update key for time T^* such that $GL \neq GL^*$ for all labels $(GL, ML) = \mathbf{GMLabels}(S_{i,j})$ of $S_{i,j} \in CV_R$ where UK_{T^*} is related with CV_R.

- An adversary is **Type-II-B** if it requests an update key for time T^* such that $GL = GL^*$ for some labels $(GL, ML) = \mathbf{GMLabels}(S_{i,j})$ of $S_{i,j} \in CV_R$ where UK_{T^*} is related with CV_R. In this case, we have that $ML \neq ML^*$ since the identity ID^* should be revoked in UK_{T^*} by the restriction of the security model.

Game $\mathbf{G}_3$ This game is the same as the game $\mathbf{G}_2$ except that the settings of random R'_1 and R_2 in the challenge ciphertext are changed. That is, R'_1 is randomly chosen and R_2 is set as $M^*_1 \oplus R'_1$. This game is the original security game in the security model except that the challenge bit μ is fixed to 1.

Let $S^{G_i}_{\mathcal{A}}$ be the event that $\mathcal{A}$ outputs 0 in a game $\mathbf{G}_i$. From Lemmas 4.4 and 4.5, we obtain the following result

$$\begin{aligned}\mathrm{Adv}^{RIBE}_{\mathcal{A}}(\lambda) &\leq \frac{1}{2}\left|\Pr[S^{G_0}_{\mathcal{A}}] - \Pr[S^{G_3}_{\mathcal{A}}]\right| \leq \frac{1}{2}\left|\Pr[S^{G_1}_{\mathcal{A}}] - \Pr[S^{G_2}_{\mathcal{A}}]\right| \\ &\leq \frac{1}{2}\Big(\sum_{\rho=1}^{\ell}\left|\Pr[S^{H_{\rho-1}}_{\mathcal{A}}] - \Pr[S^{H_\rho}_{\mathcal{A}}]\right|\Big) \leq O(n^2)\big(\mathrm{Adv}^{IBE}_{\mathcal{B}}(\lambda) + \mathrm{Adv}^{IBR}_{\mathcal{B}}(\lambda)\big).\end{aligned}$$

This completes our proof. □

Lemma 4.4. *If the IBE scheme is IND-CPA secure, then no polynomial-time Type-II-A adversary can distinguish between $\mathbf{H}_{\rho-1}$ and $\mathbf{H}_\rho$ with a non-negligible advantage.*

Proof. Suppose there exists an adversary $\mathcal{A}$ that attacks the RIBE scheme with a non-negligible advantage. An algorithm $\mathcal{B}$ that attacks the IBE scheme is initially given public parameters PP_{IBE} by a challenger $\mathcal{C}$. Then $\mathcal{B}$ that interacts with $\mathcal{A}$ is described as follows:

Setup: $\mathcal{B}$ generates MK_{IBR}, PP_{IBR} by running the **IBR.Setup** algorithm and generates MK_{HIBE}, PP_{HIBE} by running the **HIBE.Setup** algorithm. It initializes $RL = \emptyset$ and gives $PP = (PP_{IBE}, PP_{IBR}, PP_{HIBE})$ to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ adaptively requests a polynomial number of private key, update key, decryption key, and revocation queries.

- For a private key query with an identity ID, $\mathcal{B}$ proceeds as follows: It generates SK_{ID} by running the **RIBE.GenKey** algorithm since it knows MK_{HIBE}. It gives SK_{ID} to $\mathcal{A}$.

- For an update key query with time T, $\mathcal{B}$ proceeds as follows:

  1. It initializes $RV = \emptyset$. For each $(ID_j, T_j) \in RL$, it adds a leaf node $v_j \in \mathcal{BT}$ into RV if $T_j \leq T$. It obtains CV_T by running $\mathbf{SD.Cover}(\mathcal{BT}, RV)$.
  2. For each $S_{i,j} \in CV_T$, it sets $(GL_k, ML_k) = \mathbf{GMLabels}(S_{i,j})$ and performs: It receives $SK_{IBE,S_{i,j}}$ from $\mathcal{C}$ by submitting an identity $GL_k \| T$. It generates $SK_{IBR,S_{i,j}}$ by running $\mathbf{IBR.GenKey}(ML_k \| T, MK_{IBR}, PP_{IBR})$.

3. It creates $UK_T = \big(CV_T, \{(SK_{IBE,S_{i,j}}, SK_{IBR,S_{i,j}})\}_{S_{i,j} \in CV_T}\big)$ and gives UK_T to $\mathcal{A}$.

- For a decryption key query with an identity ID and time T, $\mathcal{B}$ proceeds as follows:
  1. It retrieves $SK_{ID} = SK_{HIBE}$ by querying a private key to its own oracle. It also retrieves UK_T by querying an update key to its own oracle.
  2. Next, it generates a delegated key DK_{HIBE} of SK_{HIBE} by running **HIBE.DelegateKey** for ID and T.
  3. It gives $DK_{ID,T} = (UK_T, DK_{HIBE})$ to $\mathcal{A}$.
- For a revocation query with an identity ID and time T, $\mathcal{B}$ proceeds as follows: It adds (ID, T) to RL if ID was not revoked before.

Challenge: $\mathcal{A}$ submits a challenge identity ID^*, challenge time T^*, and two challenge messages M_0^*, M_1^*. $\mathcal{B}$ proceeds as follows:

1. It first selects random R_2 and sets $R_{1,M_0} = M_0^* \oplus R_2, R_{1,M_1} = M_1^* \oplus R_2$.
2. Next, it generates CT_{HIBE}^* by running **HIBE.Encrypt**$((ID^*, T^*), R_2, PP_{HIBE})$.
3. It obtains PV_{ID^*} by running **SD.Assign**$(\mathcal{BT}, v_{ID^*})$ where a leaf node v_{ID^*} is associated with ID^*. For each $S_{i,j} \in PV_{ID^*}$, it obtains $(GL_k, ML_k) =$ **GMLabels**$(S_{i,j})$ and proceeds as follows:
   - If $k < \rho$, then it selects random $R_{3,k}$ and sets $R_{4,k} = R_{1,M_1} \oplus R_{3,k}$, and then generates $CT_{IBE,S_{i,j}}^*$ by running **IBE.Encrypt**$(GL_k \| T^*, R_{3,k}, PP_{IBE})$ and $CT_{IBR,S_{i,j}}^*$ by running **IBR.Encrypt**$(ML_k \| T^*, R_{4,k}, PP_{IBR})$.
   - If $k = \rho$, then it performs the follows:
     (a) It selects random $R_{4,k}$ and sets $R_{3,k,M_0} = R_{1,M_0} \oplus R_{4,k}$, $R_{3,k,M_1} = R_{1,M_1} \oplus R_{4,k}$.
     (b) It receives $CT_{IBE,S_{i,j}}^*$ from $\mathcal{C}$ by submitting a challenge identity $GL_k \| T^*$ and challenge messages R_{3,k,M_0}, R_{3,k,M_1}.
     (c) It generates $CT_{IBR,S_{i,j}}^*$ by running **IBR.Encrypt**$(ML_k \| T^*, R_{4,k}, PP_{IBR})$.
   - If $k > \rho$, then it selects random $R_{3,k}$ and sets $R_{4,k} = R_{1,M_0} \oplus R_{3,k}$, and then generates $CT_{IBE,S_{i,j}}^*$ by running **IBE.Encrypt**$(GL_k \| T^*, R_{3,k}, PP_{IBE})$ and $CT_{IBR,S_{i,j}}^*$ by running **IBR.Encrypt**$(ML_k \| T^*, R_{4,k}, PP_{IBR})$.

   It creates $CT_{PV}^* = \big(PV_{ID^*}, \{(CT_{IBE,S_{i,j}}^*, CT_{IBR,S_{i,j}}^*)\}_{S_{i,j} \in PV_{ID^*}}\big)$.
4. It gives a challenge ciphertext $CT^* = (CT_{PV}^*, CT_{HIBE}^*)$ to $\mathcal{A}$.

Phase 2: Same as Phase 1.
Guess: Finally, $\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$. $\mathcal{B}$ also outputs μ'. □

Lemma 4.5. *If the IBR scheme is IND-CPA secure, then no polynomial-time Type-II-B adversary can distinguish between $\mathbf{H}_{\rho-1}$ and $\mathbf{H}_\rho$ with a non-negligible advantage.*

Proof. Suppose there exists an adversary $\mathcal{A}$ that attacks the RIBE scheme with a non-negligible advantage. An algorithm $\mathcal{B}$ that attacks the IBR scheme is initially given public parameters PP_{IBR} by a challenger $\mathcal{C}$. Then $\mathcal{B}$ that interacts with $\mathcal{A}$ is described as follows:

Setup: $\mathcal{B}$ generates MK_{IBE}, PP_{IBE} by running the **IBE.Setup** algorithm and generates MK_{HIBE}, PP_{HIBE} by running the **HIBE.Setup** algorithm. It initializes $RL = \emptyset$ and gives $PP = (PP_{IBE}, PP_{IBR}, PP_{HIBE})$ to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ adaptively requests a polynomial number of private key, update key, decryption key, and revocation queries.

- For a private key query with an identity ID, $\mathcal{B}$ proceeds as follows: It generates SK_{ID} by running **RIBE.GenKey** algorithm since it knows MK_{HIBE}. It gives SK_{ID} to $\mathcal{A}$.

- For an update key query with time T, $\mathcal{B}$ proceeds as follows:

  1. It initializes $RV = \emptyset$. For each $(ID_j, T_j) \in RL$, it adds a leaf node $v_j \in \mathcal{BT}$ into RV if $T_j \leq T$. It obtains CV_T by running **SD.Cover**$(\mathcal{BT}, RV)$.
  2. For each $S_{i,j} \in CV_T$, it sets $(GL_k, ML_k) =$ **GMLabels**$(S_{i,j})$ and performs: It generates $SK_{IBE,S_{i,j}}$ by running **IBE.GenKey**$(GL_k \| T, MK_{IBE}, PP_{IBE})$. It receives $SK_{IBR,S_{i,j}}$ from $\mathcal{C}$ by submitting an identity $ML_k \| T$.
  3. It creates $UK_T = \big(CV_T, \{(SK_{IBE,S_{i,j}}, SK_{IBR,S_{i,j}})\}_{S_{i,j} \in CV_T}\big)$ and gives UK_T to $\mathcal{A}$.

- For a decryption key query with an identity ID and time T, $\mathcal{B}$ proceeds as follows:

  1. It retrieves $SK_{ID} = SK_{HIBE}$ by querying a private key to its own oracle. It also retrieves UK_T by querying an update key to its own oracle.
  2. Next, it generates a delegated key DK_{HIBE} of SK_{HIBE} by running **HIBE.DelegateKey** for ID and T.
  3. It gives $DK_{ID,T} = (UK_T, DK_{HIBE})$ to $\mathcal{A}$.

- For a revocation query with an identity ID and time T, $\mathcal{B}$ proceeds as follows: It adds (ID, T) to RL if ID was not revoked before.

Challenge: $\mathcal{A}$ submits a challenge identity ID^*, challenge time T^*, and two challenge messages M_0^*, M_1^*. $\mathcal{B}$ proceeds as follows:

1. It first select random R_2 and sets $R_{1,M_0} = M_0^* \oplus R_2, R_{1,M_1} = M_1^* \oplus R_2$.

2. Next, it generates CT_{HIBE}^* by running **HIBE.Encrypt**$((ID^*, T^*), R_2, PP_{HIBE})$.

3. It obtains PV_{ID^*} by running **SD.Assign**$(\mathcal{BT}, v_{ID^*})$ where a leaf node v_{ID^*} is associated with ID^*. For each $S_{i,j} \in PV_{ID^*}$, it obtains $(GL_k, ML_k) =$ **GMLabels**$(S_{i,j})$ and proceeds as follows:

   - If $k < \rho$, then it selects random $R_{3,k}$ and sets $R_{4,k} = R_{1,M_1} \oplus R_{3,k}$, and then generates $CT_{IBE,S_{i,j}}^*$ by running **IBE.Encrypt**$(GL_k \| T^*, R_{3,k}, PP_{IBE})$ and $CT_{IBR,S_{i,j}}^*$ by running **IBR.Encrypt**$(ML_k \| T^*, R_{4,k}, PP_{IBR})$.
   - If $k = \rho$, then it performs the follows:
     (a) It selects random $R_{3,k}$ and sets $R_{4,k,M_0} = R_{1,M_0} \oplus R_{3,k}$, $R_{4,k,M_1} = R_{1,M_1} \oplus R_{3,k}$.
     (b) It generates $CT_{IBE,S_{i,j}}^*$ by running **IBE.Encrypt**$(GL_k \| T^*, R_{3,k}, PP_{IBE})$.

(c) It receives $CT^*_{IBR,S_{i,j}}$ from $\mathcal{C}$ by submitting a challenge identity $ML_k \| T^*$ and challenge messages R_{4,k,M_0}, R_{4,k,M_1}.

- If $k > \rho$, then it selects random $R_{3,k}$ and sets $R_{4,k} = R_{1,M_0} \oplus R_{3,k}$, and then generates $CT^*_{IBE,S_{i,j}}$ by running **IBE.Encrypt**$(GL_k \| T^*, R_{3,k}, PP_{IBE})$ and $CT^*_{IBR,S_{i,j}}$ by running **IBR.Encrypt**$(ML_k \| T^*, R_{4,k}, PP_{IBR})$.

It creates $CT^*_{PV} = \big(PV_{ID^*}, \{(CT^*_{IBE,S_{i,j}}, CT^*_{IBR,S_{i,j}})\}_{S_{i,j} \in PV_{ID^*}}\big)$.

4. It gives a challenge ciphertext $CT^* = (CT^*_{PV}, CT^*_{HIBE})$ to $\mathcal{A}$.

Phase 2: Same as Phase 1.

Guess: Finally, $\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$. $\mathcal{B}$ also outputs μ'. □

5 Instantiations

In this section, we show that our generic RIBE construction can be instantiated as real RIBE schemes by using bilinear maps or lattices.

5.1 RIBE from Bilinear Maps

Previously, many RIBE schemes using the CS method were directly constructed on bilinear maps [3,26,35]. In addition, an RIBE scheme using the SD method was also directly constructed on bilinear maps [21]. Recently, a generic construction for RIBE using the CS method was proposed by Ma and Lin [27]. Nonetheless, different generic construction for RIBE using the SD method is still an interesting method because it allows different RIBE instantiations by changing the underlying cryptographic schemes and allows RIBE schemes with shorter update keys. Here, we will look at different instantiations of RIBE using the SD method that provide selective security or adaptive security.

First, we instantiate an efficient RIBE scheme that provides selective security by following the generic construction. To do this, we choose the BB-IBE scheme of Boneh and Boyen [4] as the underlying IBE scheme, which provides selective security in the DBDH assumption. For underlying IBR scheme, we may choose the efficient LSW-IBR scheme of Lewko et al. [25]. However, the IBR scheme for our generic construction only requires that the revoked set R of ciphertexts is just consists of a single revoked identity ID. Thus, we can derive a simplified LSW-IBR scheme which supports a single revoked identity, and this simplified IBR scheme provides selective security in the DBDH assumption [23]. Finally, we choose the two-level BB-HIBE scheme of Boneh and Boyen [4] that provides selective security in the DBDH assumption. The resulting RIBE scheme that uses the SD method provides selective security under the DBDH assumption.

Next, we instantiate an RIBE scheme that provides adaptive security. To this security, we use the IBE scheme of Waters [40] which provides adaptive security under the DBDH and DLIN assumptions, the IBR scheme of Okamoto and Takashima [31] which is derived from an NIPE scheme that provides adaptive security, and the two-level HIBE scheme of Waters [40] that provides adaptive security under the DBDH and DLIN assumptions. The resulting RIBE scheme provides adaptive security under these standard assumptions in prime-order bilinear groups. The previous adaptively secure RIBE scheme of Lee et al. [21] is built in composite-order bilinear groups, but this generic RIBE scheme is built in prime-order bilinear groups. However, this generic RIBE scheme has a small size of private keys and a large size of ciphertexts, whereas the RIBE scheme of Lee et al. has a small size of ciphertexts and a large size of private keys.

5.2 RIBE from Lattices

A number of RIBE schemes in lattices have been previously proposed [8,9,16,38]. Although the first lattice based RIBE scheme using the CS method did not provide decryption key exposure resistance (DKER), the new RIBE scheme using the CS method that allows DKER was recently proposed by using the delegation property of HIBE [8, 16]. In addition, a lattice based RIBE scheme using the SD method also has been proposed, but this scheme has a serious limitation such that the identity space is restricted to be small universe because the Lagrange interpolation technique is directly applied to lattices [9].

We use the previously proposed efficient lattice based IBE, IBR, and two-level HIBE schemes to instantiate a lattice based RIBE scheme using the SD method. For the underlying IBE and HIBE schemes, we choose efficient IBE and HIBE schemes of Agrawal et al. [1] that provide selective security in the LWE assumption. For the underlying simple IBR scheme, we choose the NIPE scheme of Katsumata and Yamada [17] which is derived from a linear functional encryption scheme. Note that an NIPE scheme is easily transformed into a simplified IBR scheme with a single revoked identity and this resulting IBR scheme provides selective security in the LWE assumption.

We compare our RIBE scheme with the SD method and the RIBE scheme directly designed by Cheng and Zhang [9]. Cheng and Zhang derived their RIBE scheme in lattices by applying the design principle of the RIBE scheme of Lee et al. [21] in bilinear maps. To use the technique of Lee et al., it is necessary to use the Lagrange interpolation to recover a polynomial value in decryption. In lattices, if Lagrange coefficients and noise values in ciphertexts are multiplied, then a large noise value is obtained in the decryption process, which should be removed to obtain a message. Since the resulting noise value is exponentially increased as the size of the identity space increases, their RIBE scheme has a serious problem that only a small universe of identity can be accepted. Therefore, our RIBE scheme with the SD method is the first lattice based RIBE scheme using the SD method that supports a large universe of identity and provides the DKER property.

6 Conclusion

In this paper, we proposed a new generic RIBE construction with the SD method. Our generic construction uses an IBE scheme, an IBR scheme with single revoked identity, and a two-level HIBE scheme as building blocks. The generic RIBE construction can be instantiated by bilinear maps or lattices, and the private key consists of constant IBE and HIBE private keys, the update key consists of $O(r)$ number of IBE and IBR private keys, and the ciphertext mainly consists of $O(n^2)$ number of IBE and IBR ciphertexts. If our generic RIBE construction is extended to use the more efficient LSD method instead of the SD method, the ciphertext is reduced to $O(n^{1.5})$ number of IBE and IBR ciphertexts. In addition, if the underlying IBE, IBR, and HIBE schemes provide the CCA security and a one-time signature is used, then a CCA secure RIBE scheme can be generically constructed.

There are some interesting open problems. The first problem is to reduce the size of a ciphertext in our generic RIBE scheme with the SD method. In the previous generic RIBE scheme with the CS method, the size of a ciphertext can be reduced by using an IBBE scheme. In our generic RIBE scheme with the SD method, it is difficult to reduce the size of a ciphertext since it uses an IBR scheme. The second problem is to design a generic RHIBE scheme with the SD method. To design a generic RHIBE scheme, the private key delegation is needed. It is possible to extend the IBE scheme to support key delegation by using an HIBE scheme, but it is unclear how to extend the IBR scheme to support key delegation.

References

[1] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer, 2010.

[2] William Aiello, Sachin Lodha, and Rafail Ostrovsky. Fast digital identity revocation (extended abstract). In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 137–152. Springer, 1998.

[3] Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar. Identity-based encryption with efficient revocation. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM Conference on Computer and Communications Security - CCS 2008*, pages 417–426. ACM, 2008.

[4] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 2004.

[5] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[6] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 258–275. Springer, 2005.

[7] Dan Boneh and Brent Waters. Conjunctive, subset, and range queries on encrypted data. In Salil P. Vadhan, editor, *Theory of Cryptography - TCC 2007*, volume 4392 of *Lecture Notes in Computer Science*, pages 535–554. Springer, 2007.

[8] Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Khoa Nguyen. Revocable identity-based encryption from lattices. In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, *Information Security and Privacy - ACISP 2012*, volume 7372 of *Lecture Notes in Computer Science*, pages 390–403. Springer, 2012.

[9] Shantian Cheng and Juanyang Zhang. Adaptive-id secure revocable identity-based encryption from lattices via subset difference method. In Javier López and Yongdong Wu, editors, *Information Security Practice and Experience - ISPEC 2015*, volume 9065 of *Lecture Notes in Computer Science*, pages 283–297. Springer, 2015.

[10] Cécile Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In Kaoru Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 200–215. Springer, 2007.

[11] Yevgeniy Dodis and Jonathan Katz. Chosen-ciphertext security of multiple encryption. In Joe Kilian, editor, *Theory of Cryptography - TCC 2005*, volume 3378 of *Lecture Notes in Computer Science*, pages 188–209. Springer, 2005.

[12] Craig Gentry and Alice Silverberg. Hierarchical id-based cryptography. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, 2002.

[13] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM Conference on Computer and Communications Security - CCS 2006*, pages 89–98. ACM, 2006.

[14] Dani Halevy and Adi Shamir. The LSD broadcast encryption scheme. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 47–60. Springer, 2002.

[15] Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-based encryption. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 466–481. Springer, 2002.

[16] Shuichi Katsumata, Takahiro Matsuda, and Atsushi Takayasu. Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. In Dongdai Lin and Kazue Sako, editors, *Public-Key Cryptography - PKC 2019*, volume 11443 of *Lecture Notes in Computer Science*, pages 441–471. Springer, 2019.

[17] Shuichi Katsumata and Shota Yamada. Non-zero inner product encryption schemes from various assumptions: LWE, DDH and DCR. In Dongdai Lin and Kazue Sako, editors, *Public-Key Cryptography - PKC 2019*, volume 11443 of *Lecture Notes in Computer Science*, pages 158–188. Springer, 2019.

[18] Kwangsu Lee. Self-updatable encryption with short public parameters and its extensions. *Des. Codes Cryptogr.*, 79(1):121–161, 2016.

[19] Kwangsu Lee, Seung Geol Choi, Dong Hoon Lee, Jong Hwan Park, and Moti Yung. Self-updatable encryption: Time constrained access control with hidden attributes and better efficiency. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013*, volume 8269 of *Lecture Notes in Computer Science*, pages 235–254. Springer, 2013.

[20] Kwangsu Lee, Woo Kwon Koo, Dong Hoon Lee, and Jong Hwan Park. Public-key revocation and tracing schemes with subset difference methods revisited. In Miroslaw Kutylowski and Jaideep Vaidya, editors, *Computer Security - ESORICS 2014*, volume 8713 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2014.

[21] Kwangsu Lee, Dong Hoon Lee, and Jong Hwan Park. Efficient revocable identity-based encryption via subset difference methods. *Des. Codes Cryptogr.*, 85(1):39–76, 2017.

[22] Kwangsu Lee, Dong Hoon Lee, Jong Hwan Park, and Moti Yung. CCA security for self-updatable encryption: Protecting cloud data when clients read/write ciphertexts. *Computer Journal*, 62(4):545–562, 2019.

[23] Kwangsu Lee and Jong Hwan Park. Identity-based revocation from subset difference methods under simple assumptions. *IEEE Access*, 7:60333–60347, 2019.

[24] Kwangsu Lee and Seunghwan Park. Revocable hierarchical identity-based encryption with shorter private keys and update keys. *Des. Codes Cryptogr.*, 86(10):2407–2440, 2018.

[25] Allison B. Lewko, Amit Sahai, and Brent Waters. Revocation systems with very small private keys. In *IEEE Symposium on Security and Privacy*, pages 273–285. IEEE Computer Society, 2010.

[26] Benoît Libert and Damien Vergnaud. Adaptive-id secure revocable identity-based encryption. In Marc Fischlin, editor, *Topics in Cryptology - CT-RSA 2009*, volume 5473 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2009.

[27] Xuecheng Ma and Dongdai Lin. A generic construction of revocable identity-based encryption. Cryptology ePrint Archive, Report 2019/299, 2019. `http://eprint.iacr.org/2019/299`.

[28] Silvio Micali. Efficient certificate revocation. Technical Report Technical Report TM-542b, 1996.

[29] Dalit Naor, Moni Naor, and Jeffery Lotspiech. Revocation and tracing schemes for stateless receivers. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 41–62. Springer, 2001.

[30] Moni Naor and Kobbi Nissim. Certificate revocation and certificate update. *IEEE J. Sel. Areas Commun.*, 18(4):561–570, 2000.

[31] Tatsuaki Okamoto and Katsuyuki Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, editors, *CANS 2011*, volume 7092 of *Lecture Notes in Computer Science*, pages 138–159. Springer, 2011.

[32] Seunghwan Park, Kwangsu Lee, and Dong Hoon Lee. New constructions of revocable identity-based encryption from multilinear maps. *IEEE Trans. Inf. Forensic Secur.*, 10(8):1564–1577, 2015.

[33] Amit Sahai, Hakan Seyalioglu, and Brent Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 199–217. Springer, 2012.

[34] Jae Hong Seo and Keita Emura. Efficient delegation of key generation and revocation functionalities in identity-based encryption. In Ed Dawson, editor, *Topics in Cryptology - CT-RSA 2013*, volume 7779 of *Lecture Notes in Computer Science*, pages 343–358. Springer, 2013.

[35] Jae Hong Seo and Keita Emura. Revocable identity-based encryption revisited: Security model and construction. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography - PKC 2013*, volume 7778 of *Lecture Notes in Computer Science*, pages 216–234. Springer, 2013.

[36] Jae Hong Seo and Keita Emura. Revocable hierarchical identity-based encryption: History-free update, security against insiders, and short ciphertexts. In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015*, volume 9048 of *Lecture Notes in Computer Science*, pages 106–123. Springer, 2015.

[37] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology - CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.

[38] Atsushi Takayasu and Yohei Watanabe. Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance. In Josef Pieprzyk and Suriadi Suriadi, editors, *Information Security and Privacy - ACISP 2017*, volume 10342 of *Lecture Notes in Computer Science*, pages 184–204. Springer, 2017.

[39] Yohei Watanabe, Keita Emura, and Jae Hong Seo. New revocable IBE in prime-order groups: Adaptively secure, decryption key exposure resistant, and with short public parameters. In Helena Handschuh, editor, *Topics in Cryptology - CT-RSA 2017*, volume 10159 of *Lecture Notes in Computer Science*, pages 432–449. Springer, 2017.

[40] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636. Springer, 2009.

[41] Kotoko Yamada, Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Keisuke Tanaka. Generic constructions for fully secure revocable attribute-based encryption. In Simon N. Foley, Dieter Gollmann, and Einar Snekkenes, editors, *Computer Security - ESORICS 2017*, volume 10493 of *Lecture Notes in Computer Science*, pages 532–551. Springer, 2017.