A Generic Construction of Revocable Identity-Based Encryption

Xuecheng Ma[1,2] and Dongdai Lin[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
maxuecheng@iie.ac.cn

Abstract. Revocable identity-based encryption (RIBE) is an extension of IBE that supports a key revocation mechanism which is important when deployed an IBE system in practice. Boneh and Franklin presented the first generic construction of RIBE, however, their scheme is not scalable where the size of key updates is linear in the number of users in the system. Then, Boldyreva, Goyal and Kumar presented the first scalable RIBE where the size of key update is logarithmic in the number of users and linear in the number of revoked users.
In this paper, we present a generic construction of scalable RIBE from any IBE in a black-box way. Our construction has some merits both in theory and practice. We obtain the first RIBE scheme based on quadratic residuosity problem and the first adaptive-ID secure RIBE scheme based on lattices if we instantiate the underlying IBE with IBE schemes from quadratic residuosity assumption and adaptive-ID secure IBE from lattices, respectively. In addition, public parameters size and secret keys size are the same as that of the underlying IBE schemes. Our construction is natural to be server-aided where the overheads of communication and computation for receivers are the same as those of underlying IBE schemes. Finally, inspired by recent work of Katsumata et al., we present a generic construction of RIBE with decryption key exposure resilience using HIBE and IBE schemes.

Key words: Generic Construction, Revocable IBE, DKER

1 Introduction

Identity-Based Encryption (IBE) was introduced by Shamir [41], to eliminate the need for maintaining a certificate based Public Key Infrastructure (PKI) in the traditional Public Key Encryption (PKE) setting. The first IBE scheme was proposed by Boneh and Franklin [7] in the random oracle model [3]. Since then, there are many followup works [5, 6, 44, 20, 45, 14, 8, 1, 2, 9–11, 21, 46, 47, 18].

Revocation capability is very important and necessary for IBE setting as well as PKI setting. To address the challenge of key revocation, Boneh and Franklin [7] proposed a naive method for adding a simple revocation mechanism to any

IBE system as follows. A sender encrypts a message using a receiver's identity concatenated with the current time period, i.e., $\mathsf{id}||\mathsf{t}$ and the Key Generation Center (KGC) issues the private key $\mathsf{sk}_{\mathsf{id}||\mathsf{t}}$ for each non-revoked users in every time period. However, BF-RIBE scheme is inefficient. The number of private keys issued in every time period is linear in the number of all users in the system hence the scheme did not scale well if there are a large number of users.

Boldyreva, Goyal and Kumar [4] proposed the first scalable revocable IBE (RIBE) scheme in the selective-ID security model by combining the fuzzy IBE scheme of Sahai and Waters [38] with a subset cover framework called the complete subtree (CS) method [31]. The BGK-RIBE scheme significantly reduced the size of key updates from linear to logarithmic in the number of users. Each user holds a long-term private key associated with its identity but the private key is not allowed to decrypt the ciphertext in order to achieve the key revocation mechanism. KGC broadcasts key updates for every time period through a public channel. Specially, the non-revoked users can derive decryption key from their long-term private keys and key updates while revoked users can't. There are numerous followup works [24, 27, 29, 39, 43].

RIBE with DKER. In the definition of security in BGK-RIBE, the adversary is only allowed to be access to the key extraction oracle, the revocation oracle and the key update oracle. Considering leakage of decryption keys in realistic attacks, Seo and Emura [39, 40] introduced a security notion called decryption key exposure resistance (DKER). In the definition of DKER security experiment, an exposure of a user's decryption key at some time period will not compromise the confidentiality of ciphertexts that are encrypted for different time periods. It attracted many followup works concerning R(H)IBE schemes with DKER [19, 24, 26–28, 30, 33, 34, 37, 40, 43]. Recently, Katsumata et al. [25] presented a generic construction of RIBE with DKER from any RIBE without DKER and two-level HIBE. Combining the result of [17] that any IBE schemes can be converted to an HIBE scheme (in the selective-ID model) and any RIBE scheme without DKER implies an IBE scheme, their result also implies a generic conversion from any RIBE scheme without DKER into an RIBE scheme with DKER.

Lattice-Based RIBE. The first selective-ID secure lattice-based RIBE without DKER was proposed by Chen at al. [12]. Cheng and Zhang [13] claimed that their proposed RIBE scheme with the subset difference (SD) method is the first adaptive-ID secure lattice-based scheme. However, Takayasu and Watanabe [42] pointed out critical bugs in their security proof and presented a semi-adaptive-ID secure lattice-based RIBE scheme with bounded DKER which only allows a bounded number of decryption keys to be leaked. Recently, Katsumata et al. [25] proposed the first lattice-based R(H)IBE scheme with DKER secure under the learning with errors (LWE) assumption but their proposal was still selective-ID secure. Therefore, constructing an adaptive-ID secure RIBE scheme (even without DKER) based on lattices still remains an open problem.

Server-aided RIBE [35, 15, 32] is a variant of RIBE where almost all of the workload on the user side can be delegated to an untrusted third party server. The server is untrusted in the sense that it does not possess any secret information. Each user only need to store a short long-term private key without having to communicate with either KGC.

Our Contributions. In this paper, we propose a generic construction of RIBE from any IBE schemes in a black-box way. Our construction is scalable where the update key size of our construction is logarithmic in the number of users. The benefits of our generic construction are as follows:

- Practical Benefits.
  (a) Our RIBE scheme has the same size of public parameters and user's secret key as those of underlying IBE scheme. Although the size of ciphertext in our scheme is logarithmic in the number of users, fortunately, there is a tradeoff between the size of public parameter and size of the ciphertext if we replace the underlying IBE with appropriate Identity-Based Broadcast Encryption (IBBE).
  (b) Our scheme is naturally server-aided. The communication cost and decryption cost for the receiver is the same as the underlying IBE shceme in the server-aided model.

  If we instantiate our construction with appropriate concrete IBE schemes, our scheme is very efficient. An overview comparison with other revocable IBE schemes is given in Table 1.
- Theoretical Benefits. There have been a lot of works considering ad hoc methods to transform existing IBE schemes with revocation mechanism. However, as the only generic construction, BF-RIBE is not scalable. Our generic construction demonstrates a simple and clear picture about how revocation problems in IBE could be addressed.
  (a) We present a generic construction of RIBE that can convert any IBE schemes to RIBE schemes *without* DKER. Inspired by the work of [25], we propose a construction of RIBE with DKER from HIBE and IBE schemes.
  (b) Instantiating our generic construction of existing IBE schemes [14, 8], we can obtain the first RIBE scheme (with DKER) based on quadratic residues modulo composite.
  (c) Our construction inherent the security of the underlying IBE scheme. Hence, we can obtain the first adaptive-ID secure lattice-based RIBE scheme by instantiating our construction with adaptive-ID secure IBE from lattices [1, 2, 9–11, 21, 46, 47].

Related Work. The first revocable IBE scheme from any IBE was presented by Boneh and Franklin [7], however their proposal was not scalable. Boldyreva et al. [4] proposed the first scalable RIBE using a tree-based approach but their scheme was not a generic construction. Recently, Katsumata et al. [25] proposed a generic construction of RIBE with DKER which uses as building blocks any two-level standard HIBE scheme and RIBE scheme without DKER. However, our generic construction of RIBE with DKER uses two-level HIBE and IBE schemes.

Identity-Based Broadcast Encryption is a natural extension of IBE. Delerablée [16] presented the first IBBE scheme with constant size ciphertext and

Table 1. Comparison with other RIBE schemes

Schemes	BF	BGK	LV	SE	LLP	Ours-1	Ours-2
PP Size	$O(1)$	$O(1)$	$O(\lambda)$	$O(\lambda)$	$O(1)$	$O(1)$	$O(\log(N))$
SK Size	$O(1)$	$O(\log N)$	$O(\log N)$	$O(\log N)$	$O(\log^{1.5} N)$	$O(1)$	$O(1)$
CT Size	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(\log N)$	$O(1)$
KU Size	$O(N-r)$	$O(r \log \frac{N}{r})$	$O(r \log \frac{N}{r})$	$O(r \log \frac{N}{r})$	$O(r)$	$O(r \log \frac{N}{r})$	$O(r \log \frac{N}{r})$
DKER	Yes	No	No	Yes	Yes	Yes	Yes
Storage	$O(1)$	$O(N)$	$O(N)$	$O(N)$	$O(1)$	$O(1)$	$O(1)$
Model	Full	Selective	Full	Full	Full	Full	Full
Assumption	RO,BDH	DBDH	DBDH	DBDH	Static	RO,BDH	DBDH,Static

We let λ be a security parameter, N be the maximum number of users, r be the number of revoked users. For security model, we use symbols RO for random oracle model, Full for adaptive model, Selective for selective model. We instantiate the generic construction of RIBE with DKER with different underlying concrete schemes. In our-1, we instantiate the IBE scheme and HIBE scheme with [7] and [22] respectively. In our-2, we instantiate the IBBE scheme with constant-size ciphertext and secret key and two-level HIBE scheme with [48] and [44], respectively.

with weak selective security in the random oracle model. Gentry and Waters [23] were the first to propose adaptive-ID secure IBBE systems achieving linear and sub-linear sized ciphertexts. Zhang et al. [48] presented an adaptive-ID secure IBBE scheme with a constant-size ciphertext and private keys. Recently, Ramanna [36] proposed a novel IBBE scheme with constant size ciphertext that can achieve adaptive security in the standard model.

Organization. The rest of the paper is organized as follows. In Sect. 2 we describe some preliminaries. We give our generic construction of RIBE scheme without DKER from IBE schemes in Sect. 3. In Sect. 4, we present our generic construction of RIBE with DKER from HIBE and IBE schemes. Section 5 shows some optimization of our constructions. Section 6 concludes the paper.

2 Preliminaries

2.1 Notations

Throughout the paper we use the following notation: We use λ as the security parameter and write $\mathsf{negl}(\lambda)$ to denote that some function $f(\cdot)$ is negligible in λ. An algorithm is PPT if it is modeled as a probabilistic Turing machine whose running time is bounded by some function $\mathsf{poly}(\lambda)$. By $X \approx Y$, we denote that the random variable ensembles $\{X_\lambda\}_{\lambda \in \mathbb{N}}$ and $\{Y_\lambda\}_{\lambda \in \mathbb{N}}$ are computationally indistinguishable with error $\mathsf{negl}(\lambda)$. If S is a finite set, then $s \leftarrow S$ denotes the operation of picking an element s from S uniformly at random. If A is a probabilistic algorithm, then $y \leftarrow A(x)$ denotes the action of running $A(x)$ on input x with uniform coins and outputting y. Let $[n]$ denotes $\{1, ..., n\}$. Let $\{0,1\}^{[i,j]}$ denotes all binary strings with length in $[i, j]$. For a bit string $a = (a_1, ..., a_n) \in \{0,1\}^n$, and $i, j \in [n]$ with $i \leq j$, we write $a[i, j]$ to denote the substring $(a_i, ..., a_j)$ of a. For any two strings u and v, $|u|$ denote the length of u and $u||v$ denotes their concatenation. Let BT be a complete binary tree and $\mathsf{Path(v)}$ be a set of all nodes on the path between the root node and a leaf v. We also use $\mathsf{Path(id)}$ to denote the path from the corresponding node of id to the root node.

2.2 Identity-Based Encryption

An identity-based encryption scheme consists of four probabilistic polynomial-time (PPT) algorithms (Setup, KeyGen, Enc, Dec) defined as follows:

- $\mathsf{Setup}(1^\lambda)$: This algorithm takes as input the security parameter 1^λ, and outputs a public parameter PP and a master secret key MK.
- $\mathsf{KeyGen(MK,id)}$: This algorithm takes as input the master secret key MK and an identity $\mathsf{id} \in \{0,1\}^\ell$, it outputs the identity secret key $\mathsf{sk_{id}}$.
- $\mathsf{Enc}(\mathsf{PP},\mathsf{id},\mu)$: This algorithm takes as input the public parameter PP, an identity $\mathsf{id} \in \{0,1\}^\ell$, and a plaintext μ, it outputs a ciphertext c.
- $\mathsf{Dec}(\mathsf{sk_{id}}, \mathsf{c})$: This algorithm takes as input a secret key $\mathsf{sk_{id}}$ for identity id and a ciphertext c, it outputs a plaintext μ.

The following correctness and security properties must be satisfied:

– **Correctness:** For all security parameters 1^λ, identity $\mathsf{id} \in \{0,1\}^\ell$ and plaintext μ, the following holds:

$$\Pr[\mathsf{Dec}(\mathsf{sk_{id}}, \mathsf{Enc}(\mathsf{PP}, \mathsf{id}, \mu)) = \mu] = 1$$

where $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{Setup}(1^\lambda)$ and $\mathsf{sk_{id}} \leftarrow \mathsf{KeyGen}(\mathsf{MK}, \mathsf{id})$.

– **Adaptive Security:** For any PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, there is a negligible function $\mathsf{negl}(\cdot)$ such that the following holds:

$$Adv_{\mathcal{A}}^{\mathsf{IND\text{-}ID\text{-}CPA}} = |\Pr[\mathsf{IND\text{-}ID\text{-}CPA}(\mathcal{A}) = 1] - \tfrac{1}{2}| \leq \mathsf{negl}(\lambda)$$

where $\mathsf{IND\text{-}ID\text{-}CPA}(\mathcal{A})$ is shown in Figure 1.
In order to prove the security of our RIBE construction, we define a special security for IBE as follows:

– **Multi-Identity Adaptive Security:** For any PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, there is a negligible function $\mathsf{negl}(\cdot)$ such that the advantage of $\mathcal{A}$ satisfies:

$$Adv_{\mathcal{A}}^{\mathsf{IND\text{-}mID\text{-}CPA}} = |\Pr[\mathsf{IND\text{-}mID\text{-}CPA}(\mathcal{A}) = 1] - \tfrac{1}{2}| \leq \mathsf{negl}(\lambda)$$

where $\mathsf{IND\text{-}mID\text{-}CPA}(\mathcal{A})$ is shown in Figure 2.

It is obvious that adaptive (selective) security is a special case of multi-identity adaptive (selective) security when there is only one challenge identity.

Experiment $\mathsf{IND\text{-}ID\text{-}CPA}(\mathcal{A})$:

1. $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{Setup}(1^\lambda)$
2. $(\mu_0, \mu_1, \mathsf{id}^*) \leftarrow \mathcal{A}_2^{\mathsf{KeyGen}(\mathsf{MK},\cdot)}(\mathsf{PP})$ where $|\mu_0| = |\mu_1|$ and for each query id by $\mathcal{A}_2$ to $\mathsf{KeyGen}(\mathsf{MK},\cdot)$ we have that $\mathsf{id} \neq \mathsf{id}^*$.
3. $\beta \leftarrow \{0, 1\}$
4. $\mathsf{c}^* \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{id}^*, \mu_\beta)$
5. $\beta' \leftarrow \mathcal{A}_3^{\mathsf{KeyGen}(\mathsf{MK},\cdot)}(\mathsf{PP}, \mathsf{c}^*)$ and for each query id by $\mathcal{A}_3$ to $\mathsf{KeyGen}(\mathsf{MK},\cdot)$ we have that $\mathsf{id} \neq \mathsf{id}^*$.
6. Output 1 if $\beta = \beta'$ and 0 otherwise.

Fig. 1. The adaptive security experiment of IBE

Experiment $\mathsf{IND\text{-}mID\text{-}CPA}(\mathcal{A})$:

1. $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{Setup}(1^\lambda)$
2. $(\mu_0, \mu_1, \mathsf{id}_1^*, ..., \mathsf{id}_q^*) \leftarrow \mathcal{A}_2^{\mathsf{KeyGen}(\mathsf{MK},\cdot)}(\mathsf{PP})$ where q is a polynomial of λ, $|\mu_0| = |\mu_1|$ and for each query id by $\mathcal{A}_2$ to $\mathsf{KeyGen}(\mathsf{MK},\cdot)$ we have that $\mathsf{id} \notin \{\mathsf{id}_1^*, ..., \mathsf{id}_q^*\}$
3. $\beta \leftarrow \{0, 1\}$
4. $\{\mathsf{c}_i^* \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{id}_i^*, \mu_\beta)\}_{i\in[q]}$
5. $\beta' \leftarrow \mathcal{A}_3^{\mathsf{KeyGen}(\mathsf{MK},\cdot)}(\mathsf{PP}, \mathsf{c}_1^*, ..., \mathsf{c}_q^*)$ and for each query id by $\mathcal{A}_3$ to $\mathsf{KeyGen}(\mathsf{MK},\cdot)$ we have that $\mathsf{id} \notin \{\mathsf{id}_1^*, ..., \mathsf{id}_q^*\}$
6. Output 1 if $\beta = \beta'$ and 0 otherwise.

Fig. 2. The multi-identity adaptive security experiment of IBE

Adaptive Security Implies Multi-Identity Adaptive Security

Lemma 1 *If no PPT adversaries against the adaptive (selective) security then there exists no PPT adversaries can break the multi-identity adaptive (selective) security.*

Proof. Since the proof for the adaptive-ID security and that for selective-ID security are essentially the same, we only show the proof for the former.

We prove the lemma by hybrid argument. First, we define $q+1$ hybrid games $\mathcal{H}_0, ..., \mathcal{H}_q$ where $\mathcal{H}_0$ is the real game and for all $i \in [q]$, $\mathcal{H}_i$ is the same as $\mathcal{H}_{i-1}$ except the way that the challenger generates the challenge ciphertext. In $\mathcal{H}_i$, the challenger computes the challenge ciphertext as $\{\mathsf{c}_j^* \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{id}_j^*, \mathsf{0})\}_{j\in\{1,...,i\}}$ and $\{\mathsf{c}_j^* \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{id}_j^*, \mu_\beta)\}_{j\in\{i+1,...,q\}}$ where $\mathsf{0}$ is an all-zeros string with the same length of μ_0 and β is randomly chosen from $\{0,1\}$. Let S_i denote the event that the output of IND-mID-CPA game is 1 in $\mathcal{H}_i$. In $\mathcal{H}_q$, the challenge ciphertext is encryption of zeros so $\Pr[S_q] = \frac{1}{2}$. We will show that $|\Pr[S_{i-1}] - \Pr[S_i]| \leq \mathsf{negl}(\lambda)$ for all $i \in [q]$ and finish the proof. We construct a PPT algorithm $\mathcal{B}$ such that $|\Pr[S_{i-1}] - \Pr[S_i]|$ is equal to the probability that $\mathcal{B}$ breaks the adaptive-ID security of IBE. The detail of the algorithm $\mathcal{B}$ is as follows:

1. $\mathcal{B}$'s challenger sends the public parameter PP to $\mathcal{B}$ and $\mathcal{B}$ forwards it to $\mathcal{A}$.
2. When $\mathcal{A}$ queries secret key for identity id, $\mathcal{B}$ makes secret key query for id and sends $\mathsf{sk}_{\mathsf{id}}$ to $\mathcal{A}$. Then $\mathcal{A}$ sends q challenge identities $\mathsf{id}_1^*, ..., \mathsf{id}_q^*$ and two plaintexts (μ_0, μ_1) with the same length.
3. $\mathcal{B}$ randomly chooses a bit β and sends $(\mathsf{0}, \mu_\beta, \mathsf{id}_i^*)$to its challenger, where $|\mathsf{0}| = |\mu_0| = |\mu_1|$. The challenger randomly chooses a bit b and outputs $\mathsf{c}_i^* = \mathsf{Enc}(\mathsf{PP}, \mathsf{id}_i^*, \mathsf{0})$ if $b = 0$ and $\mathsf{c}_i^* = \mathsf{Enc}(\mathsf{PP}, \mathsf{id}_i^*, \mu_\beta)$ if $b = 1$. Then, $\mathcal{B}$ computes $\{\mathsf{c}_j^* \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{id}_j^*, \mathsf{0})\}_{j\in\{1,...,i-1\}}$ and $\{\mathsf{c}_j^* \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{id}_j^*, \mu_\beta)\}_{j\in\{i+1,...,q\}}$. Finally, it outputs $\mathsf{c}^* = (\mathsf{c}_1^*, ..., \mathsf{c}_q^*)$.
4. $\mathcal{B}$ answers the secret key queries as Step 3. $\mathcal{A}$ outputs a guess β' of β. $\mathcal{B}$ outputs $b' = 0$ if $\beta' = \beta$ and outputs $b' = 1$ otherwise.

Note that the identities $\mathcal{A}$ submits to secret key oracle can not in $\{\mathsf{id}_1^*, ..., \mathsf{id}_q^*\}$. If $b = 0$, $\mathcal{B}$ perfectly simulates the challenger in $\mathcal{H}_i$, and otherwise, it perfectly simulates that in $\mathcal{H}_{i-1}$. Moreover, the probability that $b' = b$ satisfies:

$$\begin{aligned}
\Pr[b' = b] &= \Pr[b' = b|b = 0]\Pr[b = 0] + \Pr[b' = b|b = 1]\Pr[b = 1] \\
&= \frac{1}{2}\Pr[b' = b|b = 0] + \frac{1}{2}\Pr[b' = b|b = 1] \\
&= \frac{1}{2}\Pr[b' = b|b = 0] + \frac{1}{2}(1 - \Pr[b' \neq b|b = 1]) \\
&= \frac{1}{2} + \frac{1}{2}(\Pr[\beta' = \beta|b = 0] - \Pr[\beta' = \beta|b = 1]) \\
&= \frac{1}{2} + \frac{1}{2}(\Pr[S_i] - \Pr[S_{i-1}])
\end{aligned}$$

The adaptive security of IBE guarantees that $|\Pr[b' = b] - \frac{1}{2}| \leq \mathsf{negl}(\lambda)$ so that $|\Pr[S_i] - \Pr[S_{i-1}]| \leq \mathsf{negl}(\lambda)$ for all $i \in [\ell]$. Hence, $|\Pr[S_0] - \Pr[S_q]| = |\Pr[S_0] - \frac{1}{2}| \leq \mathsf{negl}(\lambda)$. We complete the proof.

3 Generic Construction of Revocable Identity-Based Encryption

3.1 Definition and Security Model

A revocable IBE scheme has seven probabilistic polynomial-time (PPT) algorithms (Setup, KeyGen, KeyUpd, DkGen, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$, Revoke) with associated message space $\mathcal{M}$, identity space $\mathcal{ID}$, and time space $\mathcal{T}$.

- $\mathsf{Setup}(1^\lambda, \mathsf{N})$: This algorithm takes as input a security parameter λ and a maximal number of users N. It outputs a public parameter PP, a master secret key MK, a revocation list RL (initially empty), and a state st.
- $\mathsf{KeyGen}(\mathsf{PP}, \mathsf{MK}, \mathsf{id}, \mathsf{st})$: This algorithm takes as input the public parameter PP, the master secret key MK, an identity id, and the state st. It outputs a secret key $\mathsf{sk_{id}}$ and an update state st.
- $\mathsf{KeyUp}(\mathsf{PP}, \mathsf{MK}, \mathsf{t}, \mathsf{RL}, \mathsf{st})$: This algorithm takes as input the public parameter PP, the master secret key MK, a key update time $\mathsf{t} \in \mathcal{T}$, the revocation list RL, and the state st. It outputs a key update $\mathsf{ku_t}$.
- $\mathsf{DkGen}(\mathsf{sk_{id}}, \mathsf{ku_t})$: This algorithm takes as input a secret key $\mathsf{sk_{id}}$ and the key update $\mathsf{ku_t}$. It outputs a decryption $\mathsf{dk_{id,t}}$ or a special symbol $\perp$ indicating that id was revoked.
- $\mathsf{Encrypt}(\mathsf{PP}, \mathsf{id}, \mu)$: This algorithm takes as input the public parameter PP, an identity id, and a message $\mu \in \mathcal{M}$. It outputs a ciphertext c.
- $\mathsf{Decrypt}(\mathsf{PP}, \mathsf{dk_{id,t}}, \mathsf{c})$: This algorithm takes as input the public parameter PP, a decryption secret key $\mathsf{sk_{id,t}}$ and a ciphertext. It outputs a message $\mu \in \mathcal{M}$.
- $\mathsf{Revoke}(\mathsf{id}, \mathsf{t}, \mathsf{RL})$: This algorithm takes as input an identity id, a revocation time $\mathsf{t} \in \mathcal{T}$ and the revocation list RL. It outputs a revocation list RL

It satisfies the following conditions:

– **Correctness:** For all λ and polynomials (in λ) N, all PP and MK output by setup algorithm Setup, all $\mu \in \mathcal{M}$, $\mathsf{id} \in \mathcal{ID}$, $\mathsf{t} \in \mathcal{T}$ and all possible valid states st and revocation list RL, if identity id was not revoked before or, at time t then there exists a negligible function $\mathsf{negl}(\cdot)$ such that the following holds:

$$\Pr[\mathsf{Decrypt}(\mathsf{sk_{id,t}}, \mathsf{Encrypt}(\mathsf{PP}, \mathsf{id}, \mathsf{t}, \mu)) = \mu] \geq 1 - \mathsf{negl}(\lambda)$$

where $(\mathsf{sk_{id}}, \mathsf{st}) \leftarrow \mathsf{KeyGen}(\mathsf{PP}, \mathsf{MK}, \mathsf{id}, \mathsf{st})$, $\mathsf{ku_t} \leftarrow \mathsf{KeyUp}(\mathsf{PP}, \mathsf{MK}, \mathsf{t}, \mathsf{RL}, \mathsf{st})$ and $\mathsf{dk_{id,t}} \leftarrow \mathsf{DkGen}(\mathsf{sk_{id}}, \mathsf{ku_t})$.

– **Adaptive Security:** For any PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, there is a negligible function $\mathsf{negl}(\cdot)$ such that the advantage of $\mathcal{A}$ satisfies:

$$Adv_{\mathcal{A}}^{\mathsf{IND\text{-}RID\text{-}CPA}} = |\Pr[\mathsf{IND\text{-}RID\text{-}CPA}(\mathcal{A}) = 1] - \tfrac{1}{2}| \leq \mathsf{negl}(\lambda)$$

where $\mathsf{IND\text{-}RID\text{-}CPA}(\mathcal{A})$ is shown is Figure 3.

Experiment $\mathsf{IND\text{-}RID\text{-}CPA}(\mathcal{A})$:

1. $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{Setup}(1^\lambda)$
2. $(\mu_0, \mu_1, \mathsf{id}^*, \mathsf{t}^*) \leftarrow \mathcal{A}_2^{\mathsf{KeyGen}(\mathsf{MK},\cdot),\mathsf{KeyUp}(\mathsf{PP},\mathsf{MK},\cdot,\mathsf{RL},\mathsf{st}),\mathsf{Revoke}(\cdot,\cdot)}(\mathsf{PP})$ where $|\mu_0| = |\mu_1|$
3. $\beta \leftarrow \{0, 1\}$
4. $\mathsf{c}^* \leftarrow \mathsf{Encrypt}(\mathsf{PP}, \mathsf{id}^*, \mathsf{t}^*, \mu_\beta)$
5. $\beta' \leftarrow \mathcal{A}_3^{\mathsf{KeyGen}(\mathsf{MK},.),\mathsf{KeyUp}(\mathsf{PP},\mathsf{MK},\cdot,\mathsf{RL},\mathsf{st}),\mathsf{Revoke}(\cdot,\cdot)}(\mathsf{PP}, \mathsf{c}^*)$.
6. Output 1 if $\beta = \beta'$ and 0 otherwise.

The following restriction must hold:

– $\mathsf{KeyUp}(\mathsf{PP},\mathsf{MK},\cdot,\mathsf{RL},\mathsf{st})$ and $\mathsf{Revoke}(\cdot,\cdot)$ can be queried on time which is greater than or equal to the time of all previous queries, i.e., the adversary is allowed to query only in non-decreasing order of time. Also, the oracle $\mathsf{Revoke}(\cdot,\cdot)$ cannot be queried at time t if $\mathsf{KeyUp}(\mathsf{PP},\mathsf{MK},\cdot,\mathsf{RL},\mathsf{st})$ was queried on time t.
– If $\mathsf{KeyGen}(\mathsf{MK},\cdot)$ was queried on identity id^*, then $\mathsf{Revoke}(\cdot,\cdot)$ must be queried on time t for some $\mathsf{t} \leq \mathsf{t}^*$, i.e. $(\mathsf{id}^*, \mathsf{t})$ must be on revocation list RL when $\mathsf{KeyUp}(\mathsf{PP},\mathsf{MK},\cdot,\mathsf{RL},\mathsf{st})$ is queried on t^*.

Fig. 3. The adaptive security experiment of Revocable IBE

3.2 A Generic Construction from IBE

Basic Intuition. The key observation behind our construction is that BGK-RIBE utilized a tree-based approach which makes their scheme scalable. Recall that $\mathsf{Path}(\mathsf{id})$ denote the set of nodes on the path from id to root. KGC issues secret key for id the id-component decryption key for all nodes in $\mathsf{Path}(\mathsf{id})$. Moreover, there was a KUNode algorithm which outputs a minimal set S of nodes that contains an ancestor of all leaves corresponding to non-revoked users and the key update is the t-component decryption key for all nodes in S. In BGK-RIBE, only non-revoked users can derive decryption key $\mathsf{sk}_{\mathsf{id},\mathsf{t}}$ by combining the id-component decryption key and the t-component decryption key for one ancestor of id. Inspired by the idea of tree-based approach, we use secret key extractions to generate key updates. Specifically, we divide our message μ into (μ_0, μ_1) where μ_0 and μ_1 are random with the condition $\mu = \mu_0 + \mu_1$. So μ is information-hidden if only μ_0 or μ_1 is revealed. Our ciphertext can be divided into two parts, one part is the encryption of μ_0 under the receiver's identity id, the other part is encryption of μ_1 under identities $\mathsf{t}||\theta$ for all $\theta \in \mathsf{Path}(\mathsf{id})$. So μ_1 can be recovered by any one of secret keys of $\{\mathsf{sk}_{\mathsf{t}||\theta}\}_{\theta\in\mathsf{Path}(\mathsf{id})}$. Every user is issued a secret key $\mathsf{sk}_{\mathsf{id}}$ as the long term secret key. To generate the key update for time t, KGC extract secret keys for all identities $\mathsf{t}||\mathsf{v}$ where v is the node in $\mathsf{KUNode}(\mathsf{t}, \mathsf{RL}, \mathsf{BT})$. Hence, all users can obtain μ_0 by decrypting the first part of ciphertexts while only non-revoked users can obtain μ_1 by decrypting the second part of ciphertexts using $\mathsf{sk}_{\mathsf{t}||\theta}$ in ku_t where $\theta \in \mathsf{Path}(\mathsf{id})$.

Definition 1 (KUNode Algorithm [4]) *This algorithm takes as input a binary tree* BT*, revocation list* RL *and time* t*, and outputs a set of nodes. Let* θ_{left} *and* θ_{right} *denote the left and right child of node* θ*, where* θ *is a non-leaf node. The description of* KUNode *is as follows:*

$\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})$:
  $\mathsf{X}, \mathsf{Y} \leftarrow \emptyset$
  $\forall(\mathsf{id}_i, \mathsf{t}_i) \in \mathsf{RL}$
    if $\mathsf{t}_i \leq \mathsf{t}$ then add $\mathsf{Path}(\mathsf{id}_i)$ to X
  $\forall\theta \in \mathsf{X}$
    if $\theta_{left} \notin \mathsf{X}$ then add θ_{left} to Y
    if $\theta_{right} \notin \mathsf{X}$ then add θ_{right} to Y
  If $\mathsf{Y} = \emptyset$ then add root to Y
  Return Y

Figure 4 gives a simple example to help the readers easily understand $\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})$. In the example, identities $\mathsf{001}$ and $\mathsf{100}$ are revoked. $\mathsf{X} = \mathsf{Path}(001) \cup \mathsf{Path}(100) = \{\mathsf{root},0,00,001,1,10,100\}$, and $\mathsf{Y} = \{01,11,000,101\}$. Intuitively, for all non-revoked identities id such that $\mathsf{Path}(\mathsf{id}) \cap \mathsf{Y} \neq \emptyset$ while for revoked identities such that $\mathsf{Path}(001) \cap \mathsf{Y} = \emptyset$ and $\mathsf{Path}(100) \cap \mathsf{Y} = \emptyset$.

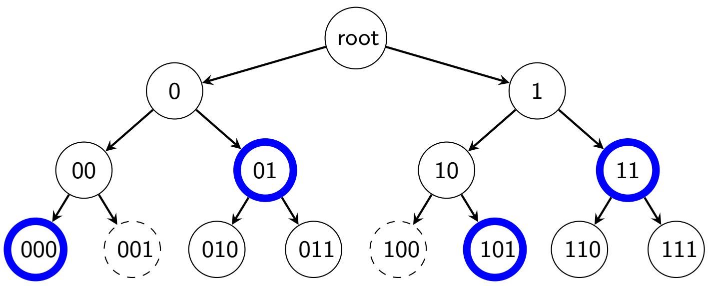

Fig. 4. An Example of KUNode

Detailed Construction. Let ($\mathsf{IBE.Setup}, \mathsf{IBE.Enc}, \mathsf{IBE.KeyGen}, \mathsf{IBE.Dec}$) be an IBE scheme that supports $\mathcal{ID} = \{0,1\}^{[\ell,2\ell]}$. There is a generic method to extend any IBE supporting identity space $\mathcal{ID}'$ to handle arbitrary identities $\mathsf{id} \in \{0,1\}^*$ by first hashing id using a collision resistant hash function $H : \{0,1\}^* \to \mathcal{ID}'$ prior to key generation and encryption [5]. Hence, any IBE schemes supporting identity space $\mathcal{ID}'$ with a collision resistant hash function $H : \{0,1\}^* \to \mathcal{ID}'$ can be applied for our construction. We assume IBE scheme has the plaintext space $\mathcal{M}$ which is finite and forms an abelian group with the group operation "+"

Utilizing the above IBE scheme, we will show how to construct a RIBE scheme Π = (Setup,KeyGen,KeyUp,DkGen,$\mathsf{Encrypt}$,$\mathsf{Decrypt}$,Revoke) as follows. In our RIBE scheme, the plaintext space is the same with the underlying IBE scheme and identity space is $\{0,1\}^\ell$. Moreover, we assume the time period space $\mathcal{T}$ is a subset of the identity space, i.e. $\mathcal{T} \subseteq \{0,1\}^\ell$.

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{PP}, \mathsf{MK})$: This algorithm takes the security parameter 1^λ as input and runs $(\mathsf{IBE.PP}, \mathsf{IBE.MK}) \leftarrow \mathsf{IBE.Setup}(1^\lambda)$. It sets the public parameter $\mathsf{PP} = \mathsf{IBE.PP}$, master secret key $\mathsf{MK} = \mathsf{IBE.MK}$ and secret state st $= \mathsf{IBE.MK}$. The following algorithms implicitly take PP as input.
- $\mathsf{KeyGen}(\mathsf{MK}, \mathsf{id}) \to \mathsf{sk_{id}}$: It runs $\mathsf{sk_{id}} \leftarrow \mathsf{IBE.KeyGen}(\mathsf{MK}, \mathsf{id})$.
- $\mathsf{KeyUp}(\mathsf{t}, \mathsf{RL}, \mathsf{st}) \to \mathsf{ku_t}$: Let BT be a complete binary tree of depth ℓ. Every identity id in the identity space $\{0,1\}^\ell$ can be viewed as a leaf node of BT. For each node $\theta \in \mathsf{KUNode}(\mathsf{BT}, \mathsf{RL}, \mathsf{t})$, compute $\mathsf{sk}_{\mathsf{t}||\theta} \leftarrow \mathsf{IBE.KeyGen}(\mathsf{IBE.MK}, \mathsf{t}||\theta)$. It outputs $\mathsf{ku_t} = \{(\theta, \mathsf{sk}_{\mathsf{t}||\theta})\}_{\theta \in \mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$.
- $\mathsf{DkGen}(\mathsf{sk_{id}}, \mathsf{ku_t}) \to \mathsf{sk_{id,t}}$: Parse $\mathsf{ku_t}$ as $\{(\theta, \mathsf{sk}_{\mathsf{t}||\theta})\}_{\theta \in \mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$. If no node $\theta \in \mathsf{Path}(\mathsf{id})$, return $\perp$. Otherwise, pick the node $\theta \in \mathsf{Path}(\mathsf{id})$ and output $\mathsf{sk_{id,t}} = (i, \mathsf{sk_{id}}, \mathsf{sk}_{\mathsf{t}||\theta})$ where $i = |\theta|$ is the length of θ.
- $\mathsf{Encrypt}(\mathsf{PP}, \mathsf{id}, \mathsf{t}, \mu) \to \mathsf{c}$: Randomly sample a pair of plaintexts $(\mu_0, \mu_1) \in \mathcal{M}^2$ with the condition that $\mu = \mu_0 + \mu_1$. Then it computes $\mathsf{c}_0 = \mathsf{IBE.Enc}(\mathsf{PP}, \mathsf{id}, \mu_0)$ and $\{\mathsf{c}_i = \mathsf{IBE.Enc}(\mathsf{PP}, \mathsf{t}||\mathsf{id}_{[1,i]}, \mu_1)\}_{i \in [\ell]}$. Finally, it outputs the ciphertext $\mathsf{c} = (\mathsf{c}_0, ..., \mathsf{c}_\ell)$.
- $\mathsf{Decrypt}(\mathsf{c}, \mathsf{sk_{id,t}}) \to \mu$: Parse c as $(\mathsf{c}_0, ..., \mathsf{c}_\ell)$ and $\mathsf{sk_{id,t}}$ as $(i, \mathsf{sk_{id}}, \mathsf{sk}_{\mathsf{t}||\theta})$. Then, compute $\mu_0 \leftarrow \mathsf{IBE.Dec}(\mathsf{sk_{id}}, \mathsf{c}_0)$ and $\mu_1 \leftarrow \mathsf{IBE.Dec}(\mathsf{sk}_{\mathsf{t}||\theta}, \mathsf{c}_i)$. Finally, output $\mu = \mu_0 + \mu_1$.
- $\mathsf{Revoke}(\mathsf{t}, \mathsf{RL}, \mathsf{id}) \to (\mathsf{RL})$: Add the pair $(\mathsf{id}, \mathsf{t})$ to the revocation list by $\mathsf{RL} \leftarrow \mathsf{RL} \cup \{(\mathsf{id}, \mathsf{t})\}$ and output RL.

3.3 Correctness

The correctness of the RIBE construction is guaranteed by the correctness of the underlying IBE.

3.4 Security Analysis

Theorem 1 *The revocable IBE is adaptive-ID (selective-ID) secure if the underlying IBE scheme is adaptive-ID (selective-ID) secure.*

Proof. We will prove the adaptive-ID security and the proof for selective-identity security are exactly the same. For any PPT adversary against the adaptive-ID security of revocable IBE, we can construct a PPT algorithm $\mathcal{B}$ against the adaptive-ID security of the underlying IBE scheme. $\mathcal{B}$ randomly guesses an adversarial type among the following two types which are mutually exclusive and cover all possibilities:

1. Type-1 adversary: $\mathcal{A}$ issues a secret key query for id^* hence id^* has been revoked before t^*.
2. Type-2 adversary: $\mathcal{A}$ does not issue a secret key query for id^*.

Note that $\mathcal{B}$'s guess is independent of the attack that $\mathcal{A}$ chooses, so the probability that $\mathcal{B}$ guesses right is $\frac{1}{2}$. We separately describe $\mathcal{B}$'s strategy by its guess.

Type-1 adversary: We will show that if adversary $\mathcal{A}_1$ makes a Type-1 attack successfully, there exists an adversary $\mathcal{B}_1$ breaking the multi-identity adaptive security of IBE defined in Figure 2. $\mathcal{B}_1$ proceeds as follows:

- Setup: $\mathcal{B}_1$ obtains a public parameter PP from its challenger and sends it to $\mathcal{A}_1$.
- KeyGen: When receiving a secret key query for id, $\mathcal{B}_1$ queries secret key extraction oracle for id.
- Revoke: $\mathcal{B}_1$ receives (id,t) from $\mathcal{A}_1$, and add (id,t) to RL.
- KeyUp: Upon receiving t, $\mathcal{B}_1$ makes secret key queries for identities $\{\mathsf{t}||\theta\}_{\theta\in\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$ and sends $\{(\theta,\mathsf{sk}_{\mathsf{t}||\theta})\}_{\theta\in\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$ to $\mathcal{A}_1$.
- $\mathsf{Challenge}$: $\mathcal{A}_1$ outputs an identity id^*, a time period t^* and two plaintexts μ_0, μ_1 with the same length. $\mathcal{B}_1$ randomly samples $\mu \leftarrow \mathcal{M}$ and sends $\{\mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}\}_{i\in[\ell]}$ as challenger identities and $\mu'_0 = \mu_0 - \mu$ and $\mu'_1 = \mu_1 - \mu$ as the challenge plaintexts. The challenger randomly chooses a challenge bit β and sends the challenge ciphertexts $\{\mathsf{c}^*_i = \mathsf{IBE.Enc}(\mathsf{PP},\mathsf{t}^*||\mathsf{id}^*_{[1,\,i]},\mu'_\beta)\}_{i\in[\ell]}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ then computes $\mathsf{c}^*_0 = \mathsf{IBE.Enc}(\mathsf{PP},\mathsf{id}^*,\mu)$ and sends $\mathsf{c}^* = (\mathsf{c}^*_0,...,\mathsf{c}^*_\ell)$ to $\mathcal{A}_1$.
- Guess: $\mathcal{A}_1$ outputs a guess bit β' and $\mathcal{B}_1$ set β' as its guess.

For the KeyGen oracle, since $|\mathsf{id}| = \ell$ and $|\mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}| \geq \ell+1$ for all $i \in [\ell]$, $\mathsf{id} \notin \{\mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}\}_{i\in[\ell]}$. For the KeyUp oracle, note that id^* has been revoked before t^* which means $\mathsf{id}^*_{[1,\,i]} \notin \mathsf{KUNode}(\mathsf{BT},\mathsf{RL}_{\mathsf{t}^*},\mathsf{t}^*)$ for all $i \in [\ell]$, so that $\mathcal{B}_1$ never queries secret keys for identities $\{\mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}\}_{i\in[\ell]}$ committed to its challenger. Hence $\mathcal{B}_1$ perfectly simulates $\mathcal{A}_1$'s view so that $\mathcal{B}_1$'s challenge bit is also $\mathcal{A}_1$'s challenge bit. $\mathcal{B}_1$ just forwards $\mathcal{A}_1$'s guess so the probability that $\mathcal{B}_1$ wins in $\mathsf{IND\text{-}mID\text{-}CPA}$ is equal to the probability that $\mathcal{A}_1$ wins in $\mathsf{IND\text{-}RID\text{-}CPA}$. Due to Lemma 1, the probability that $\mathcal{A}_1$ wins in $\mathsf{IND\text{-}RID\text{-}CPA}$ is negligible since the underlying IBE is adaptive-ID secure.

Type-2 adversary: If there exists an adversary $\mathcal{A}_2$ who makes a Type-2 attack successfully, we can construct an adversary $\mathcal{B}_2$ breaking adaptive-ID security of the underlying IBE. $\mathcal{B}_2$ proceeds as follows:

- Setup:$\mathcal{B}_2$ obtains a public parameter PP from its challenger and sends it to $\mathcal{A}_2$.
- KeyGen: When receiving a secret key query for id, $\mathcal{B}_2$ just forwards the secret key query to its challenger and sends the challenger's response to $\mathcal{A}_2$.
- Revoke: $\mathcal{B}_2$ receives (id,t) from $\mathcal{A}_2$, and adds (id,t) to RL.
- KeyUp: When $\mathcal{A}_2$ makes a key update query for time t, $\mathcal{B}_2$ makes secret key queries for all identities $\{\mathsf{t}||\theta\}_{\theta\in\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$ and sends the response $\{(\theta,\mathsf{sk}_{\mathsf{t}||\theta})\}_{\theta\in\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$ to $\mathcal{A}_2$.
- $\mathsf{Challenge}$: $\mathcal{A}_2$ outputs a challenge identity id^*, a time period t^* and two plaintexts μ_0 and μ_1 with the same length. $\mathcal{B}_1$ randomly samples $\mu \leftarrow \mathcal{M}$

and sends $\mu_0' = \mu_0 - \mu$ and $\mu_1' = \mu_1 - \mu$ as the challenge plaintexts. $\mathcal{B}_1$ receives the challenge ciphertext $\mathsf{c}_0^* = \mathsf{IBE.Enc}(\mathsf{PP}, \mathsf{id}^*, \mu_\beta')$ where β is $\mathcal{B}_2$'s challenge bit chosen randomly by its challenger. $\mathcal{B}_2$ then computes $\{\mathsf{c}_i^* = \mathsf{IBE.Enc}(\mathsf{PP}, \mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}, \mu)\}_{i\in[\ell]}$ and sends $\mathsf{c}^* = (\mathsf{c}_0^*, ..., \mathsf{c}_\ell^*)$ to $\mathcal{A}_2$.

– Guess: $\mathcal{A}_2$ outputs a guess bit β' and $\mathcal{B}_2$ sets β' as its guess. Note that $\mathcal{A}_2$ never make a secret key query for id^*. So $\mathcal{B}_2$ perfectly simulates $\mathcal{A}_2$'s view so that $\mathcal{B}_2$'s challenge bit is also $\mathcal{A}_2$'s challenge bit. $\mathcal{B}_2$ just forwards $\mathcal{A}_2$'s guess so the probability that $\mathcal{B}_2$ wins in IND-ID-CPA game is equal to the probability that $\mathcal{A}_2$ wins in IND-RID-CPA game.

When we put the results for two types of adversary together, we can conclude that the revocable IBE is adaptive-ID secure if the underlying IBE is adaptive-ID secure.

4 Generic Construction of RIBE with DKER

It is obvious that our construction is not decryption key exposure resistance. Inspired by the work of [25], we can construct a RIBE with DKER from a HIBE scheme and an IBE scheme. Let ($\mathsf{I.Setup}, \mathsf{I.Enc}, \mathsf{I.KeyGen}, \mathsf{I.Dec}$) be an IBE scheme with $\mathcal{ID} = \{0,1\}^{[\ell+1,2\ell]}$ and ($\mathsf{H.Setup}, \mathsf{H.Enc}, \mathsf{H.KeyDer}, \mathsf{H.Dec}$) be a two-level HIBE scheme where the element identity is in $\{0,1\}^\ell$. We assume the HIBE scheme and the IBE scheme have the same plaintext space $\mathcal{M}$ which is finite and forms an abelian group with the group operation " + "

Utilizing the above primitives, we will show how to construct a RIBE scheme Π = (Setup,KeyGen,KeyUp,DkGen,Encrypt,Decrypt,Revoke) as follows. In our RIBE scheme, the plaintext space is $\mathcal{M}$ and identity space is $\{0,1\}^\ell$. Moreover, we assume the time period space $\mathcal{T}$ is a subset of the identity space, i.e. $\mathcal{T} \subseteq \{0,1\}^\ell$.

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{PP}, \mathsf{MK})$: This algorithm takes as input the security parameter 1^λ and runs $(\mathsf{I.PP}, \mathsf{I.MK}) \leftarrow \mathsf{I.Setup}(1^\lambda)$ and $(\mathsf{H.PP}, \mathsf{H.MK}) \leftarrow \mathsf{H.Setup}(1^\lambda)$. It sets the public parameter PP = ($\mathsf{I.PP}$,$\mathsf{H.PP}$), master secret key $\mathsf{MK} = \mathsf{H.MK}$ and secret state $\mathsf{st} = \mathsf{I.MK}$. The following algorithms implicitly take PP as input.
- $\mathsf{Encrypt}(\mathsf{PP}, \mathsf{id}, \mathsf{t}, \mu) \to \mathsf{c}$: Parse PP as ($\mathsf{H.PP}$,$\mathsf{I.PP}$,). Randomly sample a pair of plaintexts $(\mu_0, \mu_1) \in \mathcal{M}^2$ with the condition that $\mu = \mu_0 + \mu_1$. Then it computes $\mathsf{c}_0 = \mathsf{H.Enc}(\mathsf{H.PP}, \mathsf{id}||\mathsf{t}, \mu_0)$ and $\{\mathsf{c}_i = \mathsf{I.Enc}(\mathsf{I.PP}, \mathsf{t}||\mathsf{id}_{[1,i]}, \mu_1)\}_{i\in[\ell]}$. Finally, it outputs the ciphertext $\mathsf{c} = (\mathsf{c}_0, ..., \mathsf{c}_\ell)$.
- $\mathsf{KeyGen}(\mathsf{MK}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$: It runs $\mathsf{hsk}_{\mathsf{id}} \leftarrow \mathsf{H.KeyDer}(\mathsf{MK}, \mathsf{id})$.
- $\mathsf{KeyUp}(\mathsf{t}, \mathsf{RL}, \mathsf{st}) \to \mathsf{ku}_{\mathsf{t}}$: Let BT be a complete binary tree of depth ℓ. Every identity id in the identity space $\{0,1\}^\ell$ can be viewed as a leaf node of BT. For each node $\theta \in \mathsf{KUNode}(\mathsf{BT}, \mathsf{RL}, \mathsf{t})$, compute $\mathsf{isk}_{\mathsf{t}||\theta} \leftarrow \mathsf{I.KeyGen}(\mathsf{I.MK}, \mathsf{t}||\theta)$. It outputs $\mathsf{ku}_{\mathsf{t}} = \{(\theta, \mathsf{isk}_{\mathsf{t}||\theta})\}_{\theta\in\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$.
- $\mathsf{DkGen}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ku}_{\mathsf{t}}) \to \mathsf{sk}_{\mathsf{id},\mathsf{t}}$: Run $\mathsf{hsk}_{\mathsf{id}||\mathsf{t}} \leftarrow \mathsf{H.KeyDer}(\mathsf{hsk}_{\mathsf{id}}, \mathsf{id}||\mathsf{t})$. Parse ku_{t} as $\{(\theta, \mathsf{isk}_{\mathsf{t}||\theta})\}_{\theta\in\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$. If no node $\theta \in \mathsf{Path}(\mathsf{id})$, return $\perp$. Otherwise, pick the node $\theta \in \mathsf{Path}(\mathsf{id})$ and output $\mathsf{sk}_{\mathsf{id},\mathsf{t}} = (i, \mathsf{hsk}_{\mathsf{id}||\mathsf{t}}, \mathsf{isk}_{\mathsf{t}||\theta})$ where $i = |\theta|$ is the length of θ.

- $\mathsf{Decrypt}(\mathsf{c}, \mathsf{sk}_{\mathsf{id},\mathsf{t}}) \rightarrow \mu$: Parse c as $(\mathsf{c}_0, ..., \mathsf{c}_\ell)$ and $\mathsf{sk}_{\mathsf{id},\mathsf{t}}$ as $(i, \mathsf{hsk}_{\mathsf{id}||\mathsf{t}}, \mathsf{isk}_{\mathsf{t}||\theta})$. Then, compute $\mu_0 \leftarrow \mathsf{H.Dec}(\mathsf{hsk}_{\mathsf{id}||\mathsf{t}}, \mathsf{c}_0)$ and $\mu_1 \leftarrow \mathsf{I.Dec}(\mathsf{isk}_{\mathsf{t}||\theta}, \mathsf{c}_i)$. Finally, output $\mu = \mu_0 + \mu_1$.
- $\mathsf{Revoke}(\mathsf{t}, \mathsf{RL}, \mathsf{id}) \rightarrow (\mathsf{RL})$: Add the pair $(\mathsf{id}, \mathsf{t})$ to the revocation list by $\mathsf{RL} \leftarrow \mathsf{RL} \cup \{(\mathsf{id}, \mathsf{t})\}$ and output RL.

4.1 Correctness

The correctness of the RIBE construction is guaranteed by the correctness of the underlying IBE and HIBE schemes.

4.2 Security Analysis

Theorem 2 *The revocable IBE is adaptive-ID (selective-ID) secure with decryption key exposure resilience if the underlying IBE scheme and the underlying HIBE scheme are adaptive-ID (selective-ID) secure.*

Proof. We will prove the adaptive-ID security and the proof for selective-identity security are exactly the same. For any PPT adversary against the adaptive-ID security of revocable IBE, we can construct a PPT algorithm $\mathcal{B}$ against the adaptive-ID security of the underlying IBE or HIBE scheme. $\mathcal{B}$ randomly guesses an adversarial type among the following two types which are mutually exclusive and cover all possibilities:

1. Type-1 adversary: $\mathcal{A}$ issues a secret key query for id^* hence id^* has been revoked before t^*.
2. Type-2 adversary: $\mathcal{A}$ does not issue a secret key query for id^*.

Note that $\mathcal{B}$'s guess is independent of the attack that $\mathcal{A}$ chooses, so the probability that $\mathcal{B}$ guesses right is $\frac{1}{2}$. We separately describe $\mathcal{B}$'s strategy by its guess.

Type-1 adversary: We will show that if adversary $\mathcal{A}_1$ makes a Type-1 attack successfully, there exists an adversary $\mathcal{B}_1$ breaking the multi-identity adaptive security of IBE defined in Figure 2. $\mathcal{B}_1$ proceeds as follows:

- Setup: $\mathcal{B}_1$ obtains a public parameter $\mathsf{I.PP}$ from its challenger. It generates $(\mathsf{H.PP}, \mathsf{H.MK}) \leftarrow \mathsf{H.Setup}(1^\lambda)$ and sends $(\mathsf{H.PP}, \mathsf{I.PP})$ to $\mathcal{A}_1$. $\mathcal{B}_1$ keeps $\mathsf{H.MK}$ as the master secret key.
- KeyGen: When receiving a secret key query for id, $\mathcal{B}_1$ generates the secret key normally by running $\mathsf{hsk}_{\mathsf{id}} \leftarrow \mathsf{H.KeyDer}(\mathsf{H.MK}, \mathsf{id})$.
- Revoke: $\mathcal{B}_1$ receives $(\mathsf{id}, \mathsf{t})$ from $\mathcal{A}_1$, and add $(\mathsf{id}, \mathsf{t})$ to RL.
- KeyUp: Upon receiving t, $\mathcal{B}_1$ queries secret keys for $\{\mathsf{t}||\theta\}_{\theta \in \mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$ and sends $\{(\theta, \mathsf{isk}_{\mathsf{t}||\theta})\}_{\theta \in \mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$ to $\mathcal{A}_1$.
- $\mathsf{Challenge}$: $\mathcal{A}_1$ outputs an identity id^*, a time period t^* and two plaintexts μ_0, μ_1 with the same length. $\mathcal{B}_1$ randomly samples $\mu \leftarrow \mathcal{M}$ and sends $\{\mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}\}_{i \in [\ell]}$ as challenger identities and $\mu'_0 = \mu_0 - \mu$ and $\mu'_1 = \mu_1 - \mu$ as the challenge plaintexts. The challenger randomly chooses a challenge bit β and

sends the challenge ciphertexts $\{\mathsf{c}_i^* = \mathsf{IBE.Enc}(\mathsf{I.PP}, \mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}, \mu'_\beta)\}_{i\in[\ell]}$ to $\mathcal{B}_1$. $\mathcal{B}_1$ then computes $\mathsf{c}_0^* = \mathsf{HIBE.Enc}(\mathsf{H.PP}, \mathsf{id}^*, \mu)$ and sends $\mathsf{c}^* = (\mathsf{c}_0^*, ..., \mathsf{c}_\ell^*)$ to $\mathcal{A}_1$.
- Guess: $\mathcal{A}_1$ outputs a guess bit β' and $\mathcal{B}_1$ set β' as its guess.

For the KeyUp oracle, note that id^* has been revoked before t^* which means $\mathsf{id}^*_{[1,\,i]} \notin \mathsf{KUNode}(\mathsf{BT}, \mathsf{RL}_{\mathsf{t}^*}, \mathsf{t}^*)$ for all $i \in [\ell]$, so that $\mathcal{B}_1$ never queries secret keys for identities $\{\mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}\}_{i\in[\ell]}$ submitted to its challenger. Hence $\mathcal{B}_1$ perfectly simulates $\mathcal{A}_1$'s view so that $\mathcal{B}_1$'s challenge bit is also $\mathcal{A}_1$'s challenge bit. $\mathcal{B}_1$ just forwards $\mathcal{A}_1$'s guess so the probability that $\mathcal{B}_1$ wins in IND-mID-CPA is equal to the probability that $\mathcal{A}_1$ wins in IND-RID-CPA. Due to Lemma 1, the probability that $\mathcal{A}_1$ wins in IND-RID-CPA is negligible since the underlying IBE is adaptive-ID secure.
Type-2 adversary: If there exists an adversary $\mathcal{A}_2$ who makes a Type-2 attack successfully, we can construct an adversary $\mathcal{B}_2$ breaking adaptive-ID security of the underlying HIBE scheme. $\mathcal{B}_2$ proceeds as follows:

- Setup:$\mathcal{B}_2$ obtains a public parameter H.PP from its challenger. It generates (I.PP, I.MK)$\leftarrow$ $\mathsf{I.Setup}(1^\lambda)$ and sends (H.PP,I.PP) to $\mathcal{A}_2$. $\mathcal{B}_2$ keeps I.MK as the state.
- KeyGen: When receiving a secret key query for id, $\mathcal{B}_2$ just forwards the secret key query to its challenger and sends the challenger's response to $\mathcal{A}_2$.
- Revoke: $\mathcal{B}_2$ receives (id,t) from $\mathcal{A}_2$, and adds (id, t) to RL.
- KeyUp: When $\mathcal{A}_2$ makes a key update query for time t, $\mathcal{B}_2$ generates $\{\mathsf{isk}_{\mathsf{t}||\theta} \leftarrow \mathsf{I.KeyGen}(\mathsf{I.MK}, \mathsf{t}||\theta)\}_{\theta\in\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$ and sends $\{(\theta, \mathsf{isk}_{\mathsf{t}||\theta})\}_{\theta\in\mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})}$ to $\mathcal{A}_2$.
- Challenge: $\mathcal{A}_2$ outputs a challenge identity id^*, a time period t^* and two plaintexts μ_0 and μ_1 with the same length. $\mathcal{B}_1$ randomly samples $\mu \leftarrow \mathcal{M}$ and sends $\mu'_0 = \mu_0 - \mu$ and $\mu'_1 = \mu_1 - \mu$ as the challenge plaintexts. $\mathcal{B}_1$ receives the challenge ciphertext $\mathsf{c}_0^* = \mathsf{HIBE.Enc}(\mathsf{H.PP}, \mathsf{id}^*, \mu'_\beta)$ where β is $\mathcal{B}_2$'s challenge bit chosen randomly by its challenger. $\mathcal{B}_2$ then computes $\{\mathsf{c}_i^* = \mathsf{IBE.Enc}(\mathsf{I.PP}, \mathsf{t}^*||\mathsf{id}^*_{[1,\,i]}, \mu)\}_{i\in[\ell]}$ and sends $\mathsf{c}^* = (\mathsf{c}_0^*, ..., \mathsf{c}_\ell^*)$ to $\mathcal{A}_2$.
- Guess: $\mathcal{A}_2$ outputs a guess bit β' and $\mathcal{B}_2$ sets β' as its guess. Note that $\mathcal{A}_2$ never make a secret key query for id^*. So $\mathcal{B}_2$ perfectly simulates $\mathcal{A}_2$'s view so that $\mathcal{B}_2$'s challenge bit is also $\mathcal{A}_2$'s challenge bit. $\mathcal{B}_2$ just forwards $\mathcal{A}_2$'s guess so the probability that $\mathcal{B}_2$ wins in IND-ID-CPA game of HIBE scheme is equal to the probability that $\mathcal{A}_2$ wins in IND-RID-CPA game of RIBE scheme.

When we put the results for two types of adversary together, we can conclude that the revocable IBE is adaptive-ID secure if both the underlying IBE and HIBE schemes are adaptive-ID secure.

5 Discussion

Server-Aided. In RIBE schemes, non-revoked user should receive the key update in every time period. In server-aided model, there exists a untrusted server without any secret key information that takes almost all the workload on users. The server should perform correct operations and give correct results to the users. More specifically, the server partially decrypts the ciphertexts and leaves less decryption task to users. It is easy to convert our scheme to be server-aided, given the key update $\mathsf{ku_t} = \{(\theta, \mathsf{sk}_{\mathsf{t},\theta})\}$ where $\theta \in \mathsf{KUNode}(\mathsf{BT},\mathsf{RL},\mathsf{t})$ and a ciphertext $\mathsf{c} = (\mathsf{c}_0, ..., \mathsf{c}_\ell)$ under identity id and time t, the sever chooses $\theta \in \mathsf{Path}(\mathsf{id})$ and computes $\mu' \leftarrow \mathsf{Dec}(\mathsf{sk}_{\mathsf{t}||\theta}, \mathsf{c}_i)$ where $i = |\theta|$. Finally, the sever sends (c_0, μ') as the transformed ciphertext to the receiver. The receiver only needs to operate the decryption algorithm of underlying IBE (HIBE) scheme in our RIBE without (with) DKER scheme. It also reduces the communication cost of the receiver.

Short Ciphertext. The size of ciphertext is logarithmic in the number of users in our construction as we should encrypt the same plaintext under ℓ different identities. Fortunately, we can replace the underlying IBE scheme with IBBE scheme and there exists IBBE schemes with constant size of ciphertext and secret key. The intuition of security proof is that the adaptive (selective) security of IBBE implies multi-identity adaptive (selective) security of IBE.

6 Conclusion

In this paper, we proposed two generic constructions of RIBE. The first construction is a RIBE scheme without DKER using an IBE as the basic building block. Furthermore, inspired by the work [25], our second construction is a RIBE scheme with DKER using HIBE and IBE schemes as building blocks. Our two RIBE constructions inherits the security of the underlying primitives, therefore, our construction implies the first RIBE from quadratic residues modulo composite and the first adaptive-ID secure RIBE from lattices by instantiating the required primitives with appropriate concrete schemes. Furthermore, our conversion is efficient and flexible. The sizes of public parameters and secret keys are the same as those of the underlying IBE scheme. In the server-aided model, the communication and computation overheads are the same as those of the underlying IBE scheme.We can reduce the size of ciphertexts by replacing the underlying IBE with appropriate IBBE.

References

1. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In *EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer, 2010.
2. Daniel Apon, Xiong Fan, and Feng-Hao Liu. Fully-secure lattice-based IBE as compact as PKE. *IACR Cryptology ePrint Archive*, 2016:125, 2016.
3. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *CCS '93,*, pages 62–73. ACM, 1993.
4. Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar. Identity-based encryption with efficient revocation. In *CCS 2008*, pages 417–426. ACM, 2008.

5. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 2004.
6. Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In *CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer, 2004.
7. Dan Boneh and Matthew K Franklin. Identity-based encryption from the weil pairing. *international cryptology conference*, 2001:213–229, 2001.
8. Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryption without pairings. *IACR Cryptology ePrint Archive*, 2007:177, 2007.
9. Xavier Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In *Public Key Cryptography - PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 499–517. Springer, 2010.
10. Xavier Boyen and Qinyi Li. Towards tightly secure lattice short signature and id-based encryption. In *ASIACRYPT 2016*, volume 10032 of *Lecture Notes in Computer Science*, pages 404–434, 2016.
11. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *J. Cryptology*, 25(4):601–639, 2012.
12. Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Khoa Nguyen. Revocable identity-based encryption from lattices. In *ACISP 2012*, volume 7372 of *Lecture Notes in Computer Science*, pages 390–403. Springer, 2012.
13. Shantian Cheng and Juanyang Zhang. Adaptive-id secure revocable identity-based encryption from lattices via subset difference method. In *ISPEC 2015*, volume 9065 of *Lecture Notes in Computer Science*, pages 283–297. Springer, 2015.
14. Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *Cryptography and Coding*, pages 360–363, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.
15. Hui Cui, Robert H. Deng, Yingjiu Li, and Baodong Qin. Server-aided revocable attribute-based encryption. In *Computer Security - ESORICS 2016*, volume 9879 of *Lecture Notes in Computer Science*, pages 570–587. Springer, 2016.
16. Cécile Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In *ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 200–215. Springer, 2007.
17. Nico Döttling and Sanjam Garg. From selective IBE to full IBE and selective HIBE. In *TCC 2017*, volume 10677 of *Lecture Notes in Computer Science*, pages 372–408. Springer, 2017.
18. Nico Döttling and Sanjam Garg. Identity-based encryption from the diffie-hellman assumption. In *CRYPTO 2017*, volume 10401 of *Lecture Notes in Computer Science*, pages 537–569. Springer, 2017.
19. Keita Emura, Jae Hong Seo, and Taek-Young Youn. Semi-generic transformation of revocable hierarchical identity-based encryption and its DBDH instantiation. *IEICE Transactions*, 99-A(1):83–91, 2016.
20. Craig Gentry. Practical identity-based encryption without random oracles. In Serge Vaudenay, editor, *EUROCRYPT 2006*, pages 445–464, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
21. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC 2008*, pages 197–206. ACM, 2008.
22. Craig Gentry and Alice Silverberg. Hierarchical id-based cryptography. In *ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, 2002.

23. Craig Gentry and Brent Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In *EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 171–188. Springer, 2009.
24. Yuu Ishida, Junji Shikata, and Yohei Watanabe. Cca-secure revocable identity-based encryption schemes with decryption key exposure resistance. *IJACT*, 3(3):288–311, 2017.
25. Shuichi Katsumata, Takahiro Matsuda, and Atsushi Takayasu. Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. *IACR Cryptology ePrint Archive*, 2018:420, 2018.
26. Kwangsu Lee. Revocable hierarchical identity-based encryption with adaptive security. *IACR Cryptology ePrint Archive*, 2016:749, 2016.
27. Kwangsu Lee, Dong Hoon Lee, and Jong Hwan Park. Efficient revocable identity-based encryption via subset difference methods. *Des. Codes Cryptography*, 85(1):39–76, 2017.
28. Kwangsu Lee and Seunghwan Park. Revocable hierarchical identity-based encryption with shorter private keys and update keys. *Des. Codes Cryptography*, 86(10):2407–2440, 2018.
29. Benoît Libert and Damien Vergnaud. Adaptive-id secure revocable identity-based encryption. In *CT-RSA 2009*, volume 5473 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2009.
30. Xianping Mao, Junzuo Lai, Kefei Chen, Jian Weng, and Qixiang Mei. Efficient revocable identity-based encryption from multilinear maps. *Security and Communication Networks*, 8(18):3511–3522, 2015.
31. Dalit Naor, Moni Naor, and Jeffery Lotspiech. Revocation and tracing schemes for stateless receivers. In *CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 41–62. Springer, 2001.
32. Khoa Nguyen, Huaxiong Wang, and Juanyang Zhang. Server-aided revocable identity-based encryption from lattices. In *Cryptology and Network Security - 15th International Conference, CANS 2016, Milan, Italy, November 14-16, 2016, Proceedings*, volume 10052 of *Lecture Notes in Computer Science*, pages 107–123, 2016.
33. Seunghwan Park, Dong Hoon Lee, and Kwangsu Lee. Revocable hierarchical identity-based encryption from multilinear maps. *CoRR*, abs/1610.07948, 2016.
34. Seunghwan Park, Kwangsu Lee, and Dong Hoon Lee. New constructions of revocable identity-based encryption from multilinear maps. *IEEE Trans. Information Forensics and Security*, 10(8):1564–1577, 2015.
35. Baodong Qin, Robert H. Deng, Yingjiu Li, and Shengli Liu. Server-aided revocable identity-based encryption. In *Computer Security - ESORICS 2015*, volume 9326 of *Lecture Notes in Computer Science*, pages 286–304, 2015.
36. Somindu C. Ramanna. More efficient constructions for inner-product encryption. In *ACNS 2016s*, volume 9696 of *Lecture Notes in Computer Science*, pages 231–248. Springer, 2016.
37. Geumsook Ryu, Kwangsu Lee, Seunghwan Park, and Dong Hoon Lee. Unbounded hierarchical identity-based encryption with efficient revocation. In *WISA 2015*, volume 9503 of *Lecture Notes in Computer Science*, pages 122–133. Springer, 2015.
38. Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer, 2005.
39. Jae Hong Seo and Keita Emura. Revocable identity-based encryption revisited: Security model and construction. In *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara,*

Japan, February 26 - March 1, 2013. Proceedings, volume 7778 of *Lecture Notes in Computer Science*, pages 216–234. Springer, 2013.
40. Jae Hong Seo and Keita Emura. Revocable hierarchical identity-based encryption via history-free approach. *Theor. Comput. Sci.*, 615:45–60, 2016.
41. Adi Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.
42. Atsushi Takayasu and Yohei Watanabe. Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance. In *ACISP 2017*, volume 10342 of *Lecture Notes in Computer Science*, pages 184–204. Springer, 2017.
43. 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 *CT-RSA 2017*, volume 10159 of *Lecture Notes in Computer Science*, pages 432–449. Springer, 2017.
44. Brent Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *EUROCRYPT 2005*, pages 114–127, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.
45. Brent Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In Shai Halevi, editor, *CRYPTO 2009*, pages 619–636, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.
46. Shota Yamada. Asymptotically compact adaptively secure lattice ibes and verifiable random functions via generalized partitioning techniques. In *CRYPTO 2017*, volume 10403 of *Lecture Notes in Computer Science*, pages 161–193. Springer, 2017.
47. Jiang Zhang, Yu Chen, and Zhenfeng Zhang. Programmable hash functions from lattices: Short signatures and ibes with small key sizes. In *CRYPTO 2016*, volume 9816 of *Lecture Notes in Computer Science*, pages 303–332. Springer, 2016.
48. Leyou Zhang, Yupu Hu, and Qing Wu. Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups. *Mathematical and Computer Modelling*, 55(1-2):12–18, 2012.