Adaptively Secure Lattice-based Revocable IBE in the QROM: Compact Parameters, Tight Security, and Anonymity

Atsushi Takayasu*

May 27, 2021

Abstract

Revocable identity-based encryption (RIBE) is an extension of IBE that satisfies a key revocation mechanism to manage a number of users dynamically and efficiently. To resist quantum attacks, two adaptively secure lattice-based RIBE schemes are known in the (quantum) random oracle model ((Q)ROM). Wang et al.'s scheme that is secure in the ROM has large secret keys depending on the depth of a binary tree and its security reduction is not tight. Ma and Lin's scheme that is secure in the QROM has large ciphertexts depending on the length of identities and is not anonymous. In this paper, we propose an adaptively secure lattice-based RIBE scheme that is secure in the QROM. Our scheme has compact parameters, where the ciphertext-size is smaller than Wang et al.'s scheme and the secret key size is the same as Ma and Lin's scheme. Moreover, our scheme is anonymous and its security reduction is completely tight. We design the proposed scheme by modifying Ma-Lin's scheme instantiated by the Gentry-Peikert-Vaikuntanathan (GPV) IBE. We can obtain the advantages of our scheme by making use of Katsumata et al.'s proof technique of the GPV IBE in the QROM.

*National Institute of Information and Communications Technology (NICT), Japan. e-mail: takayasu@nict.go.jp

Contents

1 Introduction

1.1 Background

Identity-based encryption (IBE) whose notion was introduced by Shamir [Sha84] is an advanced form of public key encryption (PKE). As opposed to the traditional PKE, the common master public key MPK can be used to encrypt a plaintext for arbitrary users. In particular, encryptors take MPK and an arbitrary string ID such as user names, e-mail addresses, and so on, like a public key for a user identified as ID. Due to the feature, an IBE system does not require a public key infrastructure (PKI). Furthermore, if we consider a system in which numerous users want to communicate with each other, PKE requires public keys whose number is the same as that of users, while IBE requires only one MPK. Thanks to these benefits, IBE has been discussed in the context of several practical applications such as Health care [TWZL08, TWZL09, PSK18], IoT [MSW15, San16], delay tolerant network [AKGL07, SK05], wireless ad hoc network [ddAL08], P2P network [BRTM09], private matching [ZC11], cloud computing [KBL13], and so on. The first practical IBE scheme was proposed by Boneh and Franklin [BF01] over bilinear groups.

Due to the absence of PKI, an IBE system does not have a trivial way to revoke malicious users dynamically as opposed to the traditional PKE. Therefore, the key revocation mechanism is indispensable in a practical case. Boneh and Franklin [BF01] addressed the issue and claimed a naive solution. Simply speaking, if the key generation center (KGC) of an IBE system sends each non-revoked user ID a secret key of an identity $\mathsf{ID}\|\mathsf{T}$ in every time period T, only revoked users lose their decryption capabilities. Unfortunately, the solution is inefficient since the KGC has to sends many secret keys in each time period if a large number of users participate in the system.

Boldyreva et al. [BGK08] proposed a novel solution to achieve efficient revocation called *revocable IBE (RIBE)*. A RIBE system has three types of keys, i.e., secret key, key update, decryption key. A RIBE ciphertext depends on a receiver's identity ID and a time period T as well as a plaintext M. When a user ID joins the system, he/she receives a *secret key* $\mathsf{sk}_{\mathsf{ID}}$ depending on ID. In every time period T, the KGC broadcasts a *key update* ku_{T} depending on T. After receiving the key update, each user ID combines their own secret key $\mathsf{sk}_{\mathsf{ID}}$ and the broadcast key update ku_{T} and derives a *decryption key* $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ depending on ID and T. Here, only non-revoked users can derive well-formed decryption keys. In other words, revoked users ID cannot decrypt ciphertexts $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$ if they are revoked by a time period T. Compared with Boneh-Franklin's naive solution, Boldyreva et al.'s RIBE scheme is efficient since the size of a key update ku_{T} is logarithmic in the number of system users.

In this paper, we propose a RIBE scheme that has several attractive features. To illustrate the advantages, we explain several factors to be considered in RIBE construction.

Adaptive Security. *Adaptive security* is desirable security of RIBE that ensures a ciphertext of any identity ID does not reveal the information for a plaintext M. In contrast, the weaker notion called selective security only ensures that a ciphertext of a fixed identity $\mathsf{ID}^\star$ who is specified before launching a RIBE system does not reveal the information for a plaintext M. In other words, selective security does not ensure the security of the other users $\mathsf{ID} \neq \mathsf{ID}^\star$.

Post-quantum Security. Since Shor's quantum algorithm [Sho94] can compute factoring and discrete logarithm in polynomial time, RIBE schemes based on factoring and Diffie-Hellman-like assumptions [BGK08, ETW20, ETW21, GW19, HLCL18, LK21, LV09, SE13, Tak21, WES17] are vulnerable against quantum attacks. Thus, we want a RIBE scheme satisfying post-quantum security. So far, several RIBE schemes based on the learning with errors (LWE) assumptions [Reg05] have been proposed [CLL+12, KMT19, Lee19, ML19, TW17, TW21, WZH+19]. Among them, Ma-Lin's scheme [ML19] and Wang et al.'s scheme [WZH+19] are the only known schemes with adaptive

security proposed in 2019. To be precise, Ma and Lin [ML19] proposed a generic construction of RIBE from any IBE. Throughout this paper, we use the Gentry-Peikert-Vaikuntanathan (GPV) IBE [GPV08] to instantiate Ma-Lin's scheme since the GPV IBE is more efficient than other adaptively secure lattice-based IBE schemes [Boy10, Kat17, KY16, Yam16, Yam17]. Wang et al.'s scheme [WZH+19] is a modification of the Agrawal-Boneh-Boyen HIBE [ABB10b].

Wang et al.'s RIBE scheme achieves adaptive security in the *classical* random oracle model (ROM). In contrast, the security of Wang et al.'s scheme has not been discussed in the *quantum* random oracle model (QROM) introduced by Boneh et al. [BDF+11]. If we want to ensure post-quantum security, a scheme that is secure in the ROM based on the post-quantum computational assumption is insufficient. Indeed, Yamakawa and Zhandry [YZ20] claimed that there is a natural cryptographic scheme that is secure in the ROM; however, insecure in the QROM. Thus, Wang et al.'s RIBE scheme is still insufficient to achieve post-quantum security. We note that there may be a proof of Wang et al.'s RIBE scheme in the QROM since the Agrawal-Boneh-Boyen HIBE is secure in the QROM proved by Zhandry [Zha12b]. In contrast, Zhandry [Zha12b] proved that the GPV IBE is also secure in the QROM. Thus, Ma-Lin's RIBE scheme achieves post-quantum security.

Tight Security. The efficiency of cryptographic schemes depends on the tightness of security reduction. If the reduction is loose, we should set larger parameters to ensure the concrete security of cryptographic schemes. Unfortunately, the security of Wang et al.'s RIBE scheme is loosely reduced from the LWE assumption since the reduction loss depends on the number of secret key queries made by an adversary and a lifetime of a RIBE system. In contrast, the security of Ma-Lin's scheme is almost tightly reduced from the GPV IBE since the reduction loss only depends on the length of an identity. Moreover, Katsumata et al. [KYY18] proved that the security of the GPV IBE is tightly reduced from the LWE assumption in the QROM. Thus, Ma-Lin's RIBE scheme can rely on the hardness of the weaker LWE problem than Wang et al.'s scheme. As we claimed above, Wang et al.'s scheme may be secure in the QROM since the Agrawal-Boneh-Boyen HIBE is secure in the QROM [Zha12b]. However, the reduction loss of the Agrawal-Boneh-Boyen HIBE in the QROM is larger than that in the ROM. Thus, even if Wang et al.'s scheme is proven secure in the QROM, it will suffer from a larger reduction loss.

Anonymity. Most lattice-based IBE schemes satisfy anonymity. The anonymity ensures that a ciphertext $\mathsf{ct}_{\mathsf{ID}}$ of anonymous IBE schemes do not reveal not only the information of a plaintext M but also that of an identity ID. Thus, even if an adversary of an anonymous IBE system successfully obtains a ciphertext $\mathsf{ct}_{\mathsf{ID}}$, it cannot guess not only the secret document encrypted as $\mathsf{ct}_{\mathsf{ID}}$ but also which user communicated with each other. Although Wang et al.'s RIBE scheme [WZH+19] does not achieve anonymity, their scheme satisfies another security notion called decryption key exposure resistance (DKER) [SE13] (that will be explained below). Moreover, we can easily modify Wang et al.'s RIBE scheme to satisfy anonymity by sacrificing DKER. In contrast, although the GPV IBE satisfies anonymity, Ma-Lin's RIBE scheme does not satisfy anonymity.

(Bounded) Decryption Key Exposure Resistance. DKER is the security notion of RIBE introduced by Seo and Emura [SE13]. As opposed to RIBE without DKER, RIBE with DKER ensures that a RIBE scheme is secure even when an adversary obtains polynomially many decryption keys of the target identity $\mathsf{ID}^\star$. Although DKER is an important security notion, Katsumata et al. [KMT19] showed that RIBE without DKER can become RIBE with DKER by combining with 2-level HIBE. Since there are adaptively secure lattice-based HIBE schemes [ABB10a, ABB10b, CHKP12] in the QROM [Zha12b], constructing RIBE without DKER is sufficient for obtaining RIBE with DKER.

All the currently known RIBE schemes with DKER do not satisfy anonymity. Thus, anonymity and DKER does not seem to coexist. In contrast, Takayasu and Watanabe [TW17, TW21] proposed

lattice/pairing-based RIBE schemes with bounded DKER, where an adversary can obtain a-priori bounded number of decryption keys of $\mathsf{ID}^\star$, that simultaneously satisfy anonymity. Therefore, constructing an anonymous RIBE scheme without DKER and that with bounded DKER is sufficient for obtaining all desirable RIBE schemes. Here, we note that Takayasu and Watanabe's lattice-based anonymous RIBE scheme with bounded DKER does not satisfy adaptive security.

Compact Parameters. To achieve a key revocation mechanism, a RIBE scheme tends to sacrifice the efficiency of the underlying IBE scheme. Let N be the maximum number of users in a RIBE system. Roughly speaking, a secret key of Wang et al.'s RIBE scheme consists of $\log N$ secret keys of the underlying Agrawal-Boneh-Boyen IBE scheme [ABB10b]. Thus, Wang et al.'s RIBE scheme suffers from a large secret key. Let κ_{ID} be the length of an identity. Roughly speaking, a ciphertext of Ma-Lin's RIBE scheme consists of $(\kappa_{\mathsf{ID}}+1)$ GPV ciphertexts [GPV08]. Thus, Ma-Lin's RIBE scheme suffers from a large ciphertext.

1.2 Our Contribution

In this paper, we propose a lattice-based RIBE scheme that enjoys several attractive features simultaneously. At first, our proposed scheme achieves adaptive security in the quantum random oracle model. Moreover, the adaptive security of our proposed RIBE scheme is tightly reduced from the LWE assumption. Our proposed RIBE scheme also satisfies anonymity. Finally, a secret key-size and a ciphertext-size of our proposed scheme are almost the same as those of the GPV IBE. Moreover, we can modify our proposed scheme to achieve bounded DKER without sacrificing anonymity.

Table 1: Security comparison among adaptively secure lattice-based RIBE schemes

Scheme	reduction loss	anonymity	model
WZH+19 [WZH+19]	$O(Q_{\mathsf{sk}}\mathsf{T}_{\max})$	Yes	ROM
ML19 [ML19]+GPV08 [GPV08]	$O(\kappa_{\mathsf{ID}})$	No	QROM
Ours	$O(1)$	Yes	QROM

Table 1 compares the security of our proposed RIBE scheme and those of the other adaptively secure lattice-based RIBE schemes [ML19, WZH+19]. Here, Q_{sk}, $\mathsf{T}_{\max}$, and κ_{ID} denote the number of secret key queries made by an adversary, a lifetime of the system, and the length of an identity. Wang et al.'s scheme suffers from a huge reduction loss depending on Q_{sk} and $\mathsf{T}_{\max}$. Although the reduction loss of Ma-Lin's scheme is not very large, it is strictly larger than ours. Furthermore, Ma-Lin's scheme does not satisfy anonymity and Wang et al.'s scheme was proved to be secure only in the ROM, i.e., there has been no proof in the QROM.

Table 2 compares the efficiency of our proposed RIBE scheme and the other adaptively secure lattice-based RIBE schemes [ML19, WZH+19]. Let $|\mathsf{MPK}|$, $|\mathsf{ct}|$, $|\mathsf{sk}|$, $|\mathsf{ku}|$, and $|\mathsf{dk}|$ denote the sizes of the master public key, ciphertext, secret key, key update, and decryption key, respectively. Let N, κ_{ID}, and R denote the number of users in the system, the length of an identity, and the number of revoked users, respectively. m, q, and σ are parameters depending on n although we do not specify the values in detail. As illustrated in Table 1, our proposed scheme achieves tight security, while the other schemes [ML19, WZH+19] suffer from reduction losses. In other words, we can use shorter lattice parameters n in Table 2 than the other schemes [ML19, WZH+19]. Even when we

Table 2: Efficiency comparison among adaptively secure lattice-based RIBE schemes

Scheme	$\lvert\mathsf{MPK}\rvert$	$\lvert\mathsf{ct}\rvert$	$\lvert\mathsf{sk}\rvert$
WZH+19 [WZH+19]	$n(2m+1)\log q$	$(2m+1)\log q$	$m\log\sigma\cdot O(\log N)$
ML19 [ML19]+GPV08 [GPV08]	$nm\log q$	$(\kappa_{\mathsf{ID}}+1)(m+1)\log q$	$m\log\sigma$
Ours	$nm\log q$	$(m+\kappa_{\mathsf{ID}}+1)\log q$	$m\log\sigma$

Scheme	$\lvert\mathsf{ku}\rvert$	$\lvert\mathsf{dk}\rvert$
WZH+19 [WZH+19]	$m\log\sigma\cdot O(R(\log N-\log R))$	$2m\log\sigma$
ML19 [ML19]+GPV08 [GPV08]	$m\log\sigma\cdot O(R(\kappa_{\mathsf{ID}}-\log R))$	$2m\log\sigma$
Ours	$m\log\sigma\cdot O(R(\kappa_{\mathsf{ID}}-\log R))$	$m\log\sigma$

ignore the benefit, our scheme achieves the best efficiency. Since $\kappa_{\mathsf{ID}}\le m$ holds, our scheme has the shortest master public key, ciphertext, secret keys, and decryption keys. Since $\log N<\kappa_{\mathsf{ID}}$ holds, our scheme has larger key updates than Wang et al.'s scheme. However, we can easily overcome the drawback with a collision resistant hash function.

1.3 Technical Overview

Here, we briefly summarize the spirit of our construction. Our proposed scheme is a modification of Ma-Lin's scheme [ML19] instantiated by the GPV IBE [GPV08]. Thus, we start from Ma-Lin's scheme and modifies it to be our scheme via several changes.

GPV IBE. At first, we explain the non-revocable GPV IBE. A master public key is a uniformly random matrix $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$. A ciphertext for a plaintext M and an identity ID is $\mathsf{ct}_{\mathsf{ID}}=(c_{\mathsf{ID},0},\mathbf{c}_{\mathsf{ID},1})\in\mathbb{Z}_q\times\mathbb{Z}_q^m$, where $\mathbf{s}\in\mathbb{Z}_q^n$ is a uniformly random vector and

$$c_{\mathsf{ID},0}=\mathbf{u}_{\mathsf{ID}}^\top\mathbf{s}+\mathsf{noise}+\mathsf{M}\cdot\lfloor q/2\rfloor,\quad \mathbf{c}_{\mathsf{ID},1}=\mathbf{A}^\top\mathbf{s}+\mathsf{noise}.$$

Here, a vector $\mathbf{u}_{\mathsf{ID}}=\mathsf{H}(\mathsf{ID})$ is computed by a hash function $\mathsf{H}(\cdot)$ that is modeled as a random oracle in a security proof. A secret key is a vector $\mathbf{e}_{\mathsf{ID}}\in\mathbb{Z}^m$ sampled according to a discrete Gaussian distribution subject to $\mathbf{A}\mathbf{e}_{\mathsf{ID}}=\mathbf{u}_{\mathsf{ID}}$. A user ID can recover $\mathsf{M}\in\{0,1\}$ by computing $c=c_0-\mathbf{e}_{\mathsf{ID}}^\top\mathbf{c}_1\in\mathbb{Z}_q$ and checking whether $c\in\mathbb{Z}$ is closer to 0 or $q/2$.

Katsumata et al. [KYY18] proved tight security of the GPV IBE in the QROM. For simplicity, we explain an overview of the security proof in the ROM. To answer an adversary's random oracle queries on ID, the reduction algorithm samples $\mathbf{e}_{\mathsf{ID}}$ from a discrete Gaussian distribution over $\mathbb{Z}^m$ and sets $\mathbf{u}_{\mathsf{ID}}=\mathbf{A}\mathbf{e}_{\mathsf{ID}}$. Under the appropriate parameter setting, $\mathbf{u}_{\mathsf{ID}}$ follows a uniform distribution over $\mathbb{Z}_q^n$ and $\mathbf{e}_{\mathsf{ID}}$ follows a discrete Gaussian distribution subject to $\mathbf{u}_{\mathsf{ID}}=\mathbf{A}\mathbf{e}_{\mathsf{ID}}$ from an adversary's view as required. Thus, the reduction algorithm can answer an adversary's all random oracle queries and secret key queries. Let $\mathsf{ID}^\star$ denote a target identity. Here, the reduction algorithm knows a secret key $\mathbf{e}_{\mathsf{ID}^\star}$. The reduction algorithm is given an LWE instance $(\mathbf{A},\mathbf{b})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m$, where $\mathbf{b}=\mathbf{A}^\top\mathbf{s}+\mathsf{noise}$ holds or $\mathbf{b}$ is a uniformly random vector, and creates a challenge ciphertext by computing[1]

$$c_0=\mathbf{e}_{\mathsf{ID}^\star}^\top\mathbf{b}+\mathsf{M}\cdot\lfloor q/2\rfloor,\quad \mathbf{c}_1=\mathbf{b}.$$

[1]Here, we ignore the distribution of noise for simplicity.

If $\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathsf{noise}$ holds, the challenge ciphertext follows the same distribution as the real scheme. Otherwise, the challenge ciphertext follows a uniform distribution over $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ since an adversary does not know $\mathbf{e}_{\mathsf{ID}^\star}$. The uniformity ensures that the GPV IBE satisfies anonymity.

Ma-Lin's RIBE Scheme. Ma-Lin's RIBE scheme instantiated by the GPV IBE has the same master public key $\mathbf{A}$ and secrete keys $\mathbf{e}_{\mathsf{ID}}$ as the GPV IBE. In contrast, Ma-Lin's ciphertext consists of $(\kappa_{\mathsf{ID}} + 1)$ GPV ciphertexts. Let M_1 and M_2 denote uniformly random elements in a plaintext space subject to $\mathsf{M}_1 + \mathsf{M}_2 = \mathsf{M}$. The first κ_{ID} ciphertexts $\mathsf{ct}_{\mathsf{ID}[1]\|\mathsf{T}}, \ldots, \mathsf{ct}_{\mathsf{ID}[\kappa_{\mathsf{ID}}]\|\mathsf{T}}$ are encryptions of M_1 for identities $\mathsf{ID}[1]\|\mathsf{T}, \ldots, \mathsf{ID}[\kappa_{\mathsf{ID}}]\|\mathsf{T}$;

$$c_{\mathsf{ID}[i]\|\mathsf{T},0} = \mathbf{u}_{\mathsf{ID}[i]\|\mathsf{T}}^\top \mathbf{s}_i + \mathsf{noise} + \mathsf{M}_1 \cdot \lfloor q/2 \rfloor, \qquad \mathbf{c}_{\mathsf{ID}[i]\|\mathsf{T},1} = \mathbf{A}^\top \mathbf{s}_i + \mathsf{noise},$$

where $\mathsf{ID}[i]\|\mathsf{T}$ is a concatenation of the first i-bit of ID and T. The last ciphertext $\mathsf{ct}_{\mathsf{ID}}$ is an encryption of M_2 for an identity ID;

$$c_{\mathsf{ID},0} = \mathbf{u}_{\mathsf{ID}}^\top \mathbf{s}_{\kappa_{\mathsf{ID}}+1} + \mathsf{noise} + \mathsf{M}_2 \cdot \lfloor q/2 \rfloor, \qquad \mathbf{c}_{\mathsf{ID},1} = \mathbf{A}^\top \mathbf{s}_{\kappa_{\mathsf{ID}}+1} + \mathsf{noise}.$$

Users ID can recover M_2 with a secret key $\mathbf{e}_{\mathsf{ID}}$; however, cannot recover M_1 by themselves. For each time period, the KGC broadcast a key update. Then, all non-revoked users ID can obtain $\mathbf{e}_{\mathsf{ID}[d]\|\mathsf{T}}$ for some unique $d \in \{1, 2, \ldots, \kappa_{\mathsf{ID}}\}$, while all revoked users ID cannot obtain $\mathbf{e}_{\mathsf{ID}[d]\|\mathsf{T}}$ for any $d \in \{1, 2, \ldots, \kappa_{\mathsf{ID}}\}$.

When an adversary receives a secret key $\mathbf{e}_{\mathsf{ID}^\star}$ such that $\mathbf{A}\mathbf{e}_{\mathsf{ID}^\star} = \mathbf{u}_{\mathsf{ID}^\star}$ in a security proof, the target user $\mathsf{ID}^\star$ must be revoked by the challenge time period $\mathsf{T}^\star$. In this case, an adversary does not receive any key updates $\mathbf{e}_{\mathsf{ID}^\star[1]\|\mathsf{T}^\star}, \ldots, \mathbf{e}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}]\|\mathsf{T}^\star}$ such that $\mathbf{A}\mathbf{e}_{\mathsf{ID}^\star[i]\|\mathsf{T}^\star} = \mathbf{u}_{\mathsf{ID}^\star[i]\|\mathsf{T}^\star}$. Thus, by applying Katsumata et al.'s proof κ_{ID} times, we can successfully change each $\mathsf{ct}_{\mathsf{ID}^\star[1]\|\mathsf{T}^\star}, \ldots, \mathsf{ct}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}]\|\mathsf{T}^\star}$ to be a uniformly random element in $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$. Since the challenge ciphertext does not have the information of M_1 after the change, the information of M is completely hidden. On the other hand, in this case, Ma-Lin's scheme does not satisfy anonymity since there is no way for changing $(\kappa_{\mathsf{ID}} + 1)$-th ciphertext element $\mathsf{ct}_{\mathsf{ID}^\star}$ to be a uniformly random element in $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ since an adversary knows a secret key $\mathbf{e}_{\mathsf{ID}^\star}$.

When an adversary does not receive a secret key $\mathbf{e}_{\mathsf{ID}^\star}$ such that $\mathbf{A}\mathbf{e}_{\mathsf{ID}^\star} = \mathbf{u}_{\mathsf{ID}^\star}$ in a security proof, we can successfully change $(\kappa_{\mathsf{ID}} + 1)$-th ciphertext element $\mathsf{ct}_{\mathsf{ID}^\star}$ to be a uniformly random element in $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ by applying Katsumata et al.'s proof. Since the challenge ciphertext does not have the information of M_2, the information of M is completely hidden. On the other hand, the target user $\mathsf{ID}^\star$ may not be revoked by the challenge time period $\mathsf{T}^\star$. In this case, an adversary receives a key update $\mathbf{e}_{\mathsf{ID}^\star[d]\|\mathsf{T}^\star}$ for some unique $d \in \{1, 2, \ldots, \kappa_{\mathsf{ID}}\}$ such that $\mathbf{A}\mathbf{e}_{\mathsf{ID}^\star[d]\|\mathsf{T}^\star} = \mathbf{u}_{\mathsf{ID}^\star[d]\|\mathsf{T}^\star}$. Thus, in this case, Ma-Lin's scheme does not satisfy anonymity since there is no way for changing the ciphertext elements $\mathsf{ct}_{\mathsf{ID}^\star[d]\|\mathsf{T}^\star}$ to be a uniformly random element in $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$.

Modification for Short Ciphertexts and Tight Security. At first, we modify Ma-Lin's RIBE scheme to obtain short ciphertexts and achieve tight security that does not depend on the length of an identity κ_{ID}. To compress the ciphertext of Ma-Lin's RIBE scheme, we use the structure of multi-bit encryption schemes and obtain a single-bit RIBE scheme. As we explained above, Ma-Lin's ciphertext consists of $(\kappa_{\mathsf{ID}} + 1)$ single-bit GPV ciphertexts whose first κ_{ID} ciphertext is an encryption of M_1 and the last ciphertext is an encryption of M_2. In contrast, our ciphertext is a $(\kappa_{\mathsf{ID}} + 1)$-bit single GPV ciphertext whose first κ_{ID} bits are encryptions of M_1 and the last bit is an encryption of M_2. As the case of Ma-Lin's RIBE scheme, the first κ_{ID}-bit is encryptions of M_1 and the last bit is an encryption of M_2 as follows:

$$c_{\mathsf{ID}[i]\|\mathsf{T},0} = \mathbf{u}_{\mathsf{ID}[i]\|\mathsf{T}}^\top \mathbf{s} + \mathsf{noise} + \mathsf{M}_1 \cdot \lfloor q/2 \rfloor \quad \text{for } i = 1, 2, \ldots, \kappa_{\mathsf{ID}},$$

$$c_{\mathsf{ID},0} = \mathbf{u}_{\mathsf{ID}}^\top \mathbf{s} + \mathsf{noise} + \mathsf{M}_2 \cdot \lfloor q/2 \rfloor, \qquad \mathbf{c}_{\mathsf{ID},1} = \mathbf{A}^\top \mathbf{s} + \mathsf{noise}.$$

Here, the same secret key and key update as Ma-Lin's scheme are sufficient for decrypting the ciphertext.

As the case of Ma-Lin's proof, when an adversary receives a secret key $\mathbf{e}_{\mathsf{ID}^\star}$, we can successfully change $c_{\mathsf{ID}^\star[1]\|\mathsf{T}^\star,0}, \ldots, c_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}]\|\mathsf{T}^\star,0}$ and $\mathbf{c}_{\mathsf{ID}^\star,1}$ to be a uniformly random element in $\mathbb{Z}_q^{\kappa_{\mathsf{ID}}} \times \mathbb{Z}_q^m$. As opposed to Ma-Lin's scheme, we can apply the change at once since all of them depend on the same uniformly random vector $\mathbf{s}$; hence, a single LWE instance is sufficient for the change. Similarly, when an adversary does not receive a secret key $\mathbf{e}_{\mathsf{ID}^\star}$, we can successfully change $c_{\mathsf{ID}^\star,0}$ and $c_{\mathsf{ID}^\star,1}$ to be a uniformly random element in $\mathbb{Z}_q \times \mathbb{Z}_q^m$. After these changes, the information of M is completely hidden.

Modification for Anonymity. Our modification above does not still achieve anonymity. Indeed, there is no way for changing $c_{\mathsf{ID}^\star,0}$ to be a uniformly random element in $\mathbb{Z}_q$ when an adversary receives a secret key $\mathbf{e}_{\mathsf{ID}^\star}$, while there is no way for changing $c_{\mathsf{ID}^\star[d]\|\mathsf{T}^\star,0}$ to be a uniformly random element in $\mathbb{Z}_q$ when an adversary does not receive a secret key $\mathbf{e}_{\mathsf{ID}^\star}$ but receives a key update $\mathbf{e}_{\mathsf{ID}^\star[d]\|\mathsf{T}^\star}$ for some unique $d \in \{1, 2, \ldots, \kappa_{\mathsf{ID}}\}$.

To achieve anonymity, we aggregate each $c_{\mathsf{ID}[1]\|\mathsf{T},0}, \ldots, c_{\mathsf{ID}[\kappa_{\mathsf{ID}}]\|\mathsf{T},0}$ and $c_{\mathsf{ID},0}$ as

$$c_{\mathsf{ID}[i]\|\mathsf{T},0} = (\mathbf{u}_{\mathsf{ID}}^\top + \mathbf{u}_{\mathsf{ID}[i]\|\mathsf{T}}^\top)\mathbf{s} + \mathsf{noise} + \mathsf{M} \cdot \lfloor q/2 \rfloor.$$

Non-revoked users can decrypt the ciphertext with a secret key $\mathbf{e}_{\mathsf{ID}}$ such that $\mathbf{A}\mathbf{e}_{\mathsf{ID}} = \mathbf{u}_{\mathsf{ID}}$ and a key update $\mathbf{e}_{\mathsf{ID}[d]\|\mathsf{T}}$ such that $\mathbf{A}\mathbf{e}_{\mathsf{ID}[d]\|\mathsf{T}} = \mathbf{u}_{\mathsf{ID}[d]\|\mathsf{T}}$ by computing $c = c_{\mathsf{ID}[i]\|\mathsf{T},0} - (\mathbf{e}_{\mathsf{ID}}^\top + \mathbf{e}_{\mathsf{ID}[d]\|\mathsf{T}}^\top)\mathbf{c}_{\mathsf{ID},1}$.

As in the previous discussion, when an adversary receives a secret key $\mathbf{e}_{\mathsf{ID}^\star}$, we can successfully change $\mathbf{u}_{\mathsf{ID}^\star[1]\|\mathsf{T}^\star}^\top \mathbf{s} + \mathsf{noise}, \ldots, \mathbf{u}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}]\|\mathsf{T}^\star}^\top \mathbf{s} + \mathsf{noise}$ and $\mathbf{c}_{\mathsf{ID}^\star,1}$ to be a uniformly random element in $\mathbb{Z}_q^{\kappa_{\mathsf{ID}}} \times \mathbb{Z}_q^m$. Thus, the challenge ciphertext is a uniformly random element in $\mathbb{Z}_q^{\kappa_{\mathsf{ID}}} \times \mathbb{Z}_q^m$. When an adversary does not receive a secret key $\mathbf{e}_{\mathsf{ID}^\star}$ but receives a key update $\mathbf{e}_{\mathsf{ID}^\star[d]\|\mathsf{T}^\star}$, we can successfully change $\mathbf{u}_{\mathsf{ID}^\star[1]\|\mathsf{T}^\star}^\top \mathbf{s} + \mathsf{noise}, \ldots, \mathbf{u}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}]\|\mathsf{T}^\star}^\top \mathbf{s} + \mathsf{noise}$ only except $\mathbf{u}_{\mathsf{ID}^\star[d]\|\mathsf{T}^\star}^\top \mathbf{s} + \mathsf{noise}$, $\mathbf{u}_{\mathsf{ID}^\star}^\top \mathbf{s} + \mathsf{noise}$, and $\mathbf{c}_{\mathsf{ID}^\star,1}$ to be a uniformly random element in $\mathbb{Z}_q^{\kappa_{\mathsf{ID}}} \times \mathbb{Z}_q^m$. Thus, the challenge ciphertext is a uniformly random element in $\mathbb{Z}_q^{\kappa_{\mathsf{ID}}} \times \mathbb{Z}_q^m$. Therefore, the RIBE scheme satisfies anonymity.

1.4 Roadmap

In Section 2, we review lattice preliminaries. In Section 3, we review the definition of RIBE. In Section 4, we propose our RIBE scheme without DKER. A proof of the scheme in the QROM may be technically difficult to follow. Thus, in Section 5, we first show a security proof of our scheme in the ROM. Then, in Section 6, we show a security proof of our scheme in the QROM. In Section 7, we extend the scheme for achieving bounded DKER without sacrificing anonymity.

2 Preliminaries on Lattices

Notation. Let λ denote the security parameter throughout the paper. For integers $a, b \in \mathbb{N}$ such that $a \leq b$, let $[a, b] \coloneqq \{a, a+1, \ldots, b\}$ and $[a] \coloneqq \{1, 2, \ldots, a\}$. For two binary strings a and b, let $a\|b$ denote their concatenation. For a finite set S, let $s \leftarrow_R S$ denote the operation of sampling s from S uniformly at random. For a probability distribution $\mathcal{S}$, let $s \leftarrow \mathcal{S}$ denote the operation of sampling s according to $\mathcal{S}$. For two random variables X and Y over S, the statistical distance $\Delta(X, Y)$ between X and Y is defined as $\Delta(X, Y) \coloneqq \sum_{s \in S} |\Pr[X = s] - \Pr[Y = s]|$. We say that the two distributions X and Y are statistically close when $\Delta(X, Y)$ is negligible in the security parameter. Throughout the paper, the base of the logarithm is 2. The min-entropy of a random

variable X is defined as $\mathbf{H}_\infty := -\log(\max_x \Pr[X = x])$. For two sets $\mathcal{X}$ and $\mathcal{Y}$, let $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ denote the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$.

We use a lowercase bold letter $\mathbf{b}$ and an uppercase bold letter $\mathbf{B}$ to denote a vector and matrix, respectively. Let $\mathbf{0}_n$ denote an n-dimensional zero vector. Let $\mathbf{I}_m$ denote an identity matrix of the size $m \times m$. For a matrix $\mathbf{R} \in \mathbb{R}^{n \times n}$, let $\|\mathbf{R}\|$ denote the length of the longest column of $\mathbf{R}$ and let $\|\mathbf{R}\|_{\mathrm{GS}}$ denote the longest column of the Gram-Schmidt orthogonalization of $\mathbf{R}$.

Lattices. A (full-rank) m-dimensional integer lattice $\Lambda \subseteq \mathbb{Z}^m$ is a set of m-dimensional integer vectors with the form $\{\sum_{i \in [m]} x_i \mathbf{b}_i | x_i \in \mathbb{Z}\}$, where $\{\mathbf{b}_1, \cdots, \mathbf{b}_m\}$ is called the basis of the lattice Λ. For any positive integers n, m, and $q \geq 2$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, we define $\Lambda_q^\perp(\mathbf{A}) := \{\mathbf{z} \in \mathbb{Z}^m | \mathbf{A}\mathbf{z} = \mathbf{0}_n \mod q\}$ and $\Lambda_q^{\mathbf{u}}(\mathbf{A}) := \{\mathbf{z} \in \mathbb{Z}^m | \mathbf{A}\mathbf{z} = \mathbf{u} \mod q\}$.

Gaussian Measures. Let $\mathcal{D}_{\Lambda,\sigma}$ denote a discrete Gaussian distribution over Λ with a Gaussian parameter σ. In the following, we review some basic properties of discrete Gaussian distributions.

Lemma 1 ([GPV08])**.** *Let n, m, q be positive integers such that $m \geq 2n \log q$, where q is prime. Let σ be any positive real number such that $\sigma \geq \sqrt{n + \log m}$. Then for $\mathbf{A} \leftarrow_R \mathbb{Z}_q^{n \times m}$ and $\mathbf{e} \leftarrow D_{\mathbb{Z}^m,\sigma}$, the distribution of $\mathbf{u} = \mathbf{A}\mathbf{e} \mod q$ is $2^{-\Omega(n)}$-statistically close to uniform over $\mathbb{Z}_q^n$. Furthermore, for a fixed $\mathbf{u} \in \mathbb{Z}_q^n$, the conditional distribution of $\mathbf{e} \leftarrow D_{\mathbb{Z}^m,\sigma}$, given $\mathbf{A}\mathbf{e} = \mathbf{u} \mod q$ for a uniformly random $\mathbf{A}$ in $\mathbb{Z}_q^{n \times m}$ is $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma}$.*

Lemma 2 ([GPV08, MR07])**.** *Let $\sigma > 16\sqrt{\log 2m/\pi}$ and $\mathbf{u}$ be any vector in $\mathbb{Z}_q^n$. Then, for all but q^{-n} fraction of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, we have*

$$\Pr_{\mathbf{x} \leftarrow D_{\Lambda_{\mathbf{u}}^\perp(\mathbf{A}),\sigma}}[\|\mathbf{x}\| \geq \sigma\sqrt{m}] \leq 2^{-(m-1)}.$$

Lemma 3 ([GPV08, Pei07, PR06])**.** *Let $\sigma > 16\sqrt{\log 2m/\pi}$ and $\mathbf{u}$ be any vector in $\mathbb{Z}_q^n$. Then, for all but q^{-n} fraction of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, we have*

$$\mathbf{H}_\infty(D_{\Lambda_{\mathbf{u}}^\perp(\mathbf{A}),\sigma}) \geq m - 1.$$

Lemma 4 (Noise Re-randomization, [KY16], Lemma 1)**.** *Let q, ℓ, m be positive integers and r a positive real satisfying $r > \max\{\omega(\sqrt{\log m}), \omega(\sqrt{\log \ell})\}$. Let $\mathbf{b} \in \mathbb{Z}_q^m$ be arbitrary and $\mathbf{z}$ chosen from $D_{\mathbb{Z}^m,r}$. Then there exists a PPT algorithm ReRand such that for any $\mathbf{V} \in \mathbb{Z}^{m \times \ell}$ and positive real $\sigma > \|\mathbf{V}\|_2$, $\mathsf{ReRand}(\mathbf{V}, \mathbf{b} + \mathbf{z}, r, \sigma)$ outputs $\mathbf{b}'^\top = \mathbf{b}^\top\mathbf{V} + \mathbf{z}'^\top \in \mathbb{Z}_q^\ell$ where $\mathbf{z}'$ is distributed $2^{-\Omega(n)}$-statistically close to $D_{\mathbb{Z}^\ell,2r\sigma}$.*

Sampling Algorithms. We review some of the algorithms for sampling short vectors from a given lattice.

Lemma 5. *Let $n, m, q > 0$ be positive integers with $m \geq 3n\lceil \log q \rceil$ and q a prime. Then, we have the following polynomial time algorithms:*

$\mathsf{TrapGen}(1^n, 1^m, q) \to (\mathbf{A}, \mathbf{T}_\mathbf{A})$ *([MP12, Ajt99, AP11]): a PPT algorithm that outputs a full rank matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a basis $\mathbf{T}_\mathbf{A} \in \mathbb{Z}^{m \times m}$ for $\Lambda_q^\perp(\mathbf{A})$ such that $\mathbf{A}$ is $2^{-\Omega(n)}$-statistically close to uniform and $\|\mathbf{T}_\mathbf{A}\|_{\mathrm{GS}} = O(\sqrt{n \log q})$.*

$\mathsf{SamplePre}(\mathbf{A}, \mathbf{T}_\mathbf{A}, \mathbf{u}, \sigma) \to \mathbf{e}$ *([ABB10a, MP12]): a PPT algorithm that is given a full rank matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, a basis $\mathbf{T}_\mathbf{A} \in \mathbb{Z}^{m \times m}$ of a lattice $\Lambda_q^\perp(\mathbf{A})$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and $\sigma \geq \|\mathbf{T}_\mathbf{A}\|_{\mathrm{GS}} \cdot \omega(\sqrt{\log m})$, and outputs a vector $\mathbf{e} \in \mathbb{Z}^m$ sampled from a distribution $2^{-\Omega(n)}$-statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma}$.*

$\mathsf{Sample}\mathbb{Z}(\sigma)$: *a PPT algorithm that is given* $\sigma > \omega(\sqrt{\log m})$ *and outputs a vector* $\mathbf{e} \in \mathbb{Z}^m$ *sampled from a distribution* $2^{-\Omega(n)}$*-statistically close to* $\mathcal{D}_{\mathbb{Z}^m,\sigma}$.

Learning with Errors Assumption. The security of our RIBE scheme is reduced to the learning with errors (LWE) assumption introduced by Regev [Reg05].

Definition 1 (Learning with Errors)**.** *For integers* $n = n(\lambda), m = m(n)$*, a prime* $q = q(n) > 2$*, an error distribution* $\chi = \chi(n)$ *over* $\mathbb{Z}$*, and a quantum polynomial time algorithm* $\mathcal{A}$*, the advantage for the* learning with errors problem $\mathsf{LWE}_{n,m,q,\chi}$ *of* $\mathcal{A}$ *is defined as follows:*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LWE}_{n,m,q,\chi}} = \left| \Pr\left[\mathcal{A}(\mathbf{A}, \mathbf{A}^\top \mathbf{s} + \mathbf{z}) = 1\right] - \Pr\left[\mathcal{A}(\mathbf{A}, \mathbf{w} + \mathbf{z}) = 1\right] \right|$$

where $\mathbf{A} \leftarrow_R \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$, $\mathbf{w} \leftarrow_R \mathbb{Z}_q^m$, $\mathbf{z} \leftarrow \chi^m$. *We say that the* LWE *assumption holds if* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LWE}_{n,m,q,\chi}}$ *is negligible for all quantum polynomial time algorithm* $\mathcal{A}$.

Regev [Reg05] gave a quantum reduction from the worst-case hardness of lattice problems to the average-case hardness of the $\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}$ for $\alpha q > 2\sqrt{n}$.

3 Revocable Identity-Based Encryption

In this section, we review the definition of RIBE by following [KMT19]. In the following syntax, a revocation list RL_T of a time period T is a subset of an identity space $\mathcal{ID}$ such as $\mathsf{RL}_\mathsf{T} \subseteq \mathcal{ID}$. A revoke algorithm of a RIBE scheme is just adding a set of newly revoked users to the revocation list. Hence, the algorithm does not explicitly appear in the following syntax.

Syntax. A RIBE scheme Π consists of the following six algorithms ($\mathsf{Setup}, \mathsf{Enc}, \mathsf{GenSK}, \mathsf{KeyUp}, \mathsf{GenDK}, \mathsf{Dec}$):

$\mathsf{Setup}(1^\lambda) \to (\mathsf{MPK}, \mathsf{MSK})$: This is the *setup* algorithm that takes the security parameter 1^λ as input, and outputs the master public key MPK and master secret key MSK.
We assume that the plaintext space $\mathcal{M}$, the time period space $\mathcal{T} := \{1, 2, \ldots, \mathsf{T}_{\max}\}$, where $\mathsf{T}_{\max}$ is polynomial in λ, and the identity space $\mathcal{ID}$, are determined only by the security parameter λ, and their descriptions are contained in MPK.

$\mathsf{Enc}(\mathsf{MPK}, \mathsf{ID}, \mathsf{T}, \mathsf{M}) \to \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$: This is the *encryption* algorithm that takes a master public key MPK, an identity $\mathsf{ID} \in \mathcal{ID}$, time period $\mathsf{T} \in \mathcal{T}$, and plaintext $\mathsf{M} \in \mathcal{M}$ as input, and outputs a ciphertext $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$.

$\mathsf{GenSK}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID}) \to \mathsf{sk}_\mathsf{ID}$: This is the *secret key generation* algorithm that takes the master pubic key MPK, master secret key MSK, and identity $\mathsf{ID} \in \mathcal{ID}$ as input, and outputs a secret key sk_ID for the identity ID.

$\mathsf{KeyUp}(\mathsf{MPK}, \mathsf{T}, \mathsf{MSK}, \mathsf{RL}_\mathsf{T}) \to \mathsf{ku}_\mathsf{T}$: This is the *key update information generation* algorithm that takes the master pubic key MPK, time period $\mathsf{T} \in \mathcal{T}$, master secret key MSK, and revocation list $\mathsf{RL}_\mathsf{T} \subseteq \mathcal{ID}$ as input, and outputs a key update ku_T for a time period $\mathsf{T} \in \mathcal{T}$.

$\mathsf{GenDK}(\mathsf{MPK}, \mathsf{sk}_\mathsf{ID}, \mathsf{ku}_\mathsf{T}) \to \mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ or $\perp$: This is the *decryption key generation* algorithm that takes the master public key MPK, secret key sk_ID of a user $\mathsf{ID} \in \mathcal{ID}$, and key update ku_T as input, and outputs a decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ for a time period $\mathsf{T} \in \mathcal{T}$ or the spacial symbol $\perp$ indicating that ID has been revoked.

$\mathsf{Dec}(\mathsf{MPK}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}) \to \mathsf{M}$: This is the *decryption* algorithm that takes the master public key MPK, decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$, and ciphertext $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$ as input, and outputs the decryption result M.

Correctness. We require a ciphertext corresponding with $(\mathsf{ID}, \mathsf{T})$ to be properly decrypted by a decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ of the same $(\mathsf{ID}, \mathsf{T})$ if the user is not revoked by T. To fully capture this, we consider all the possible scenarios of creating the secret key for user ID. Namely, for all $n \in \mathbb{N}$, $(\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(1^n)$, $\mathsf{ID} \in \mathcal{ID}$, $\mathsf{T} \in \mathcal{T}$, $\mathsf{M} \in \mathcal{M}$, $\mathsf{RL}_\mathsf{T} \subseteq \mathcal{ID}$, if $\mathsf{ID} \notin \mathsf{RL}_\mathsf{T}$ holds, then we require $\mathsf{M}' = \mathsf{M}$ to hold after executing the following:

- $\mathsf{sk}_\mathsf{ID} \leftarrow \mathsf{GenSK}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID})$,
- $\mathsf{ku}_\mathsf{T} \leftarrow \mathsf{KeyUp}(\mathsf{MPK}, \mathsf{T}, \mathsf{MSK}, \mathsf{RL}_\mathsf{T})$,
- $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} \leftarrow \mathsf{GenDK}(\mathsf{MPK}, \mathsf{sk}_\mathsf{ID}, \mathsf{ku}_\mathsf{T})$,
- $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} \leftarrow \mathsf{Enc}(\mathsf{MPK}, \mathsf{ID}, \mathsf{T}, \mathsf{M})$, and
- $\mathsf{M}' \leftarrow \mathsf{Dec}(\mathsf{MPK}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}})$.

Security Definition. Let Π be a RIBE scheme. The adaptive-identity anonymity is defined via a game between an adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ parameterized by the security parameter 1^λ. The game has the global counter $\mathsf{T}_\mathtt{cu}$ initialized with 1 to denote the "*current* time period" and the subscript "$\mathtt{ct}$" stands for *current*. $\mathcal{C}$'s responses to $\mathcal{A}$'s queries are controlled by $\mathsf{T}_\mathtt{cu}$. The game proceeds as follows:

$\mathcal{C}$ first runs $(\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(1^\lambda)$, and prepares $\mathtt{SKList}$ and into which identity/secret key pairs $(\mathsf{ID}, \mathsf{sk}_\mathsf{ID})$ generated during the game will be stored. Whenever a new secret key is generated for an identity $\mathsf{ID} \in \mathcal{ID}$ due to the execution of GenSK, $\mathcal{C}$ will store $(\mathsf{ID}, \mathsf{sk}_\mathsf{ID})$ in $\mathtt{SKList}$, and we will not explicitly mention this addition. Then, $\mathcal{C}$ executes $\mathsf{ku}_1 \leftarrow \mathsf{KeyUp}(\mathsf{MPK}, \mathsf{T}_\mathtt{cu} = 1, \mathsf{MSK}, \mathsf{RL}_1 = \emptyset)$ for generating a key update for the initial time period $\mathsf{T}_\mathtt{cu} = 1$, and gives MPK and ku_1 to $\mathcal{A}$.

Then, $\mathcal{A}$ may adaptively make the following four types of queries to $\mathcal{C}$:

Secret Key Generation Query: Upon a query $\mathsf{ID} \in \mathcal{ID}$ from $\mathcal{A}$, $\mathcal{C}$ checks if $(\mathsf{ID}, *) \notin \mathtt{SKList}$, and returns $\perp$ to $\mathcal{A}$ if this is *not* the case. Otherwise, $\mathcal{C}$ executes $\mathsf{sk}_\mathsf{ID} \leftarrow \mathsf{GenSK}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID})$ and returns *nothing* to $\mathcal{A}$.

Secret Key Reveal Query: Until the challenge query, upon a query $\mathsf{ID} \in \mathcal{ID}$ from $\mathcal{A}$, $\mathcal{C}$ finds sk_ID from $\mathtt{SKList}$, and returns it to $\mathcal{A}$. After the challenge query, $\mathcal{C}$ checks

- If $\mathsf{T}_\mathtt{cu} \geq \mathsf{T}^\star$ and $\mathsf{ID} \notin \mathsf{RL}^\star_\mathsf{T}$, then $\mathsf{ID} \neq \mathsf{ID}^\star$.

If the condition is *not* satisfied, then $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ finds sk_ID from $\mathtt{SKList}$, and returns it to $\mathcal{A}$.

Revoke & Key Update Query: Until the challenge query, upon a query $\mathsf{RL} \subseteq \mathcal{ID}$ (which denotes the set of identities that are going to be revoked in the next time period) from $\mathcal{A}$, $\mathcal{C}$ checks if the following condition is satisfied:

- $\mathsf{RL}_{\mathsf{T}_\mathtt{cu}} \subseteq \mathsf{RL}$.[2]

After the challenge query, $\mathcal{C}$ also checks

- If $\mathsf{T}_\mathtt{cu} = \mathsf{T}^\star - 1$ and $\mathsf{sk}_{\mathsf{ID}^\star}$ has already been revealed by the secret key reveal query, then $\mathsf{ID}^\star \in \mathsf{RL}$.

If the conditions are *not* satisfied, then $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$.
Otherwise $\mathcal{C}$ increments the current time period by $\mathsf{T}_\mathtt{cu} \leftarrow \mathsf{T}_\mathtt{cu} + 1$, and executes $\mathsf{RL}_{\mathsf{T}_\mathtt{cu}} \leftarrow \mathsf{RL}$, $\mathsf{ku}_{\mathsf{T}_\mathtt{cu}} \leftarrow \mathsf{KeyUp}(\mathsf{MPK}, \mathsf{T}_\mathtt{cu}, \mathsf{MSK}, \mathsf{RL}_{\mathsf{T}_\mathtt{cu}})$. Finally, $\mathcal{C}$ returns $\mathsf{ku}_{\mathsf{T}_\mathtt{cu}}$ to $\mathcal{A}$.

Challenge Query: $\mathcal{A}$ is allowed to make this query only once. Upon a query $(\mathsf{ID}^\star, \mathsf{T}^\star, \mathsf{M}^\star)$ from $\mathcal{A}$, $\mathcal{C}$ checks if the following condition is satisfied:

- If $\mathsf{T}^\star \leq \mathsf{T}_\mathtt{cu}$ and $\mathsf{sk}_{\mathsf{ID}^\star}$ has been revealed to $\mathcal{A}$, then $\mathsf{ID} \in \mathsf{RL}_{\mathsf{T}^\star}$.

[2] This check ensures that the identities that have already been revoked will remain revoked in the next time period.

$\mathcal{C}$ picks $\mathsf{coin} \leftarrow_R \{0,1\}$. If $\mathsf{coin} = 0$, $\mathcal{C}$ runs $\mathsf{ct}^\star \leftarrow \mathsf{Enc}(\mathsf{MPK}, \mathsf{ID}^\star, \mathsf{T}^\star, \mathsf{M}^\star)$. Otherwise, $\mathcal{C}$ samples $\mathsf{ct}^\star$ from a ciphertext space uniformly at random. Finally, $\mathcal{C}$ returns the challenge ciphertext $\mathsf{ct}^\star$ to $\mathcal{A}$.

At some point, $\mathcal{A}$ outputs $\widehat{\mathsf{coin}} \in \{0,1\}$ as its guess for coin and terminates.

The above completes the description of the game. In this game, $\mathcal{A}$'s adaptive-identity anonymity advantage is defined by $\mathsf{Adv}^{\mathtt{RIBE}}_{\Pi,\mathcal{A}}(\lambda) := 2 \cdot |\Pr[\widehat{\mathsf{coin}} = \mathsf{coin}] - 1/2|$.

Definition 2. *We say that a RIBE scheme* Π *satisfies* adaptive-identity anonymity*, if the advantage* $\mathsf{Adv}^{\mathtt{RIBE}}_{\Pi,\mathcal{A}}(\lambda)$ *is negligible for all PPT adversaries* $\mathcal{A}$*.*

4 Construction

In this section, we propose a RIBE scheme. Let n, m, q be positive integers, where q is prime. Let σ, α, α' be positive real numbers that will serve as discrete Gaussian parameters. Let a plaintext space be $\mathcal{M} := \{0,1\}$. An identity space is a set of $(\kappa_{\mathsf{ID}}+1)$-bit binary strings whose first bit is always 0. Thus, $|\mathcal{ID}| = 2^{\kappa_{\mathsf{ID}}}$ holds. A time period space is a set of κ_{T}-bit binary string without 0. Let $\mathsf{H} : \{0,1\}^{(\kappa_{\mathsf{ID}}+\kappa_{\mathsf{T}}+1)} \to \mathbb{Z}_q^n$ be a hash function that will be modeled as a (quantum) random oracle in a security proof.

Binary Tree Data Structure. We use a binary tree $\mathtt{BT}$ with $2^{\kappa_{\mathsf{ID}}}$ leaves to realize a scalable revocation. Each node $\theta \in \mathtt{BT}$ is labeled by a binary string of an appropriate length. Specifically, the root node is labeled as 0 and other nodes of depth d are labeled as $(d+1)$-bit binary strings whose first bit are always 0. For a node with a label $\theta \in \mathtt{BT}$, its left and right children are labeled as $\theta\|0$ and $\theta\|1$, respectively. Note that all leaf nodes are labeled by some binary strings $\mathsf{ID} \in \mathcal{ID}$. For an identity ID of a $(\kappa_{\mathsf{ID}}+1)$-bit binary string, we use $\mathsf{ID}[i]$ to denote the first $(i+1)$-bit of ID. By definition, $\mathsf{ID}[i]$ denotes a depth-i ancestor of a leaf node ID in $\mathtt{BT}$. Furthermore, a set of nodes $\{\mathsf{ID}[0] = 0, \mathsf{ID}[1], \ldots, \mathsf{ID}[\kappa_{\mathsf{ID}}] = \mathsf{ID}\}$ denotes all nodes in a path from the root to the leaf ID. It is known that KUNode algorithm [NNL01] takes a description of a binary tree $\mathtt{BT}$ and a set of its leaves $\mathsf{RL}_{\mathsf{T}} = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_R\}$ as input, then outputs a set of nodes $\mathsf{KU}_{\mathsf{T}} := \{\theta_1, \ldots, \theta_r\}$ such that

- If $\mathsf{ID} \notin \mathsf{RL}_{\mathsf{T}}$, there is a unique node $\mathsf{ID}[d] \in \mathsf{KU}_{\mathsf{T}}$ for some $d \in [0, \kappa_{\mathsf{ID}}]$.
- If $\mathsf{ID} \in \mathsf{RL}_{\mathsf{T}}$, there is no node $\mathsf{ID}[d] \in \mathsf{KU}_{\mathsf{T}}$ for all $d \in [0, \kappa_{\mathsf{ID}}]$.

In particular, $|\mathsf{KU}_{\mathsf{T}}| = O(|\mathsf{RL}_{\mathsf{T}}|(\kappa_{\mathsf{ID}} - \log |\mathsf{RL}_{\mathsf{T}}|))$ holds.

Construction. We show our RIBE scheme.

$\mathsf{Setup}(1^\lambda) \to (\mathsf{MPK}, \mathsf{MSK})$: Run $(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$ and output $\mathsf{MPK} := \mathbf{A}$ and $\mathsf{MSK} := \mathbf{T}_{\mathbf{A}}$.

$\mathsf{Enc}(\mathsf{MPK}, \mathsf{ID}, \mathsf{T}, \mathsf{M}) \to \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$: Sample a uniformly random vector $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$. Sample a random vector $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,\alpha' q}$ and random integers $x_i \leftarrow D_{\mathbb{Z},\alpha' q}$ for $i \in [0, \kappa_{\mathsf{ID}}]$ from discrete Gaussian distributions. Set $\mathbf{u}_{\mathsf{ID}} := \mathsf{H}(\mathsf{ID}\|0)$ and $\mathbf{u}_{\mathsf{ID}[i],\mathsf{T}} := \mathsf{H}(\mathsf{ID}[i]\|\mathsf{T})$ for all $i \in [0, \kappa_{\mathsf{ID}}]$. Compute

$$\mathbf{c} = \mathbf{A}^\top \mathbf{s} + \mathbf{x}, \qquad c_i = (\mathbf{u}_{\mathsf{ID}}^\top + \mathbf{u}_{\mathsf{ID}[i],\mathsf{T}}^\top)\mathbf{s} + x_i + \mathsf{M} \left\lfloor \frac{q}{2} \right\rfloor \quad \text{for } i \in [0, \kappa_{\mathsf{ID}}]$$

and output $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} := (\mathbf{c}, (c_i)_{i \in [0,\kappa_{\mathsf{ID}}]}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{\kappa_{\mathsf{ID}}+1}$.

$\mathsf{GenSK}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID}) \to \mathsf{sk}_{\mathsf{ID}}$: Run

$$\mathbf{e}_{\mathsf{ID}} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{u}_{\mathsf{ID}}, \mathbf{T}_{\mathbf{A}}, \sigma)$$

and output $\mathsf{sk}_{\mathsf{ID}} \coloneqq \mathbf{e}_{\mathsf{ID}}$.

$\mathsf{KeyUp}(\mathsf{MPK}, \mathsf{T}, \mathsf{MSK}, \mathsf{RL}_{\mathsf{T}}) \to \mathsf{ku}_{\mathsf{T}}$: Run the KUNode algorithm to obtain a set of nodes KU_{T}. For every $\theta_j \in \mathsf{KU}_{\mathsf{T}}$, run

$$\mathbf{e}_{\theta_j,\mathsf{T}} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{u}_{\theta_j,\mathsf{T}}, \mathbf{T}_{\mathbf{A}}, \sigma)$$

and outputs $\mathsf{ku}_{\mathsf{T}} \coloneqq (\mathbf{e}_{\theta_j,\mathsf{T}})_{\theta_j \in \mathsf{KU}_{\mathsf{T}}}$.

$\mathsf{GenDK}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ku}_{\mathsf{T}}) \to \mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ or $\perp$: Find a node $\mathsf{ID}[d] \in \mathsf{KU}_{\mathsf{T}}$ for some $d \in [0, \kappa_{\mathsf{ID}}]$. If it does not exist, output $\perp$. Otherwise, output $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} \coloneqq \mathbf{d}_{\mathsf{ID},\mathsf{T}} \coloneqq \mathbf{e}_{\mathsf{ID}} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}$.

$\mathsf{Dec}(\mathsf{MPK}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}) \to \mathsf{M}$: Let $d \in [0, \kappa_{\mathsf{ID}}]$ be a number such that $\mathsf{ID}[d] \in \mathsf{KU}_{\mathsf{T}}$. Compute $c' = c_d - \mathbf{c}^\top \mathbf{d}_{\mathsf{ID},\mathsf{T}} \in \mathbb{Z}_q$ and output 0 if c' is closer to 0 than $\lfloor \frac{q}{2} \rfloor$. Otherwise, output 1.

Correctness. Thanks to the property of the KUNode algorithm, a non-revoked user can derive a valid decryption key $\mathbf{d}_{\mathsf{ID},\mathsf{T}} = \mathbf{e}_{\mathsf{ID}} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}$. Observe that

$$\begin{aligned} c' &= c_d - \mathbf{c}^\top \mathbf{d}_{\mathsf{ID},\mathsf{T}} \\ &= (\mathbf{u}_{\mathsf{ID}}^\top + \mathbf{u}_{\mathsf{ID}[d],\mathsf{T}}^\top)\mathbf{s} + x_d + \mathsf{M}\left\lfloor \frac{q}{2} \right\rfloor - (\mathbf{A}^\top \mathbf{s} + \mathbf{x})^\top (\mathbf{e}_{\mathsf{ID}} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}) \\ &= \mathsf{M}\left\lfloor \frac{q}{2} \right\rfloor + \underbrace{x_d - \mathbf{x}^\top (\mathbf{e}_{\mathsf{ID}} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}})}_{\text{error term}}. \end{aligned}$$

Here, we use the fact that

$$\mathbf{A}\mathbf{e}_{\mathsf{ID}} = \mathbf{u}_{\mathsf{ID}} \qquad \text{and} \qquad \mathbf{A}\mathbf{e}_{\mathsf{ID}[d],\mathsf{T}} = \mathbf{u}_{\mathsf{ID}[d],\mathsf{T}}$$

hold since $\mathbf{e}_{\mathsf{ID}} \in \Lambda^\perp_{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A})$ and $\mathbf{e}_{\theta_j,\mathsf{T}} \in \Lambda^\perp_{\mathbf{u}_{\mathsf{ID}[d],\mathsf{T}}}(\mathbf{A})$ hold by construction. The decryption succeeds if the absolute value of the error term $x_d - \mathbf{x}^\top(\mathbf{e}_{\mathsf{ID}} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}})$ is smaller than $q/4$. By Lemma 5, the distributions of $\mathbf{e}_{\mathsf{ID}}$ and $\mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}$ sampled by the $\mathsf{SamplePre}$ algorithm are $2^{-\Omega(n)}$-statistically close to $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A}),\sigma}$ and $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID}[d],\mathsf{T}}}(\mathbf{A}),\sigma}$, respectively. Therefore, by Lemma 2, $\|\mathbf{e}_{\mathsf{ID}}\| \le \sigma\sqrt{m}$ and $\|\mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}\| \le \sigma\sqrt{m}$ hold. Similarly, by Lemma 2, $|x_d| \le \alpha' q$ and $\|\mathbf{x}\| \le \alpha' q\sqrt{m}$ also hold. Thus, the absolute value of the error term is bounded by

$$\begin{aligned} |x_d - \mathbf{x}^\top(\mathbf{e}_{\mathsf{ID}} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}})| &\le |x_d| + \|\mathbf{x}\| \cdot (\|\mathbf{e}_{\mathsf{ID}}\| + \|\mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}\|) \\ &\le 3\alpha' q\sigma m. \end{aligned}$$

We will set the parameters as specified below so that the upper bound is less than $q/4$.

Parameter Selection. We set the parameters of the scheme to satisfy the following conditions:

- The absolute value of the error term is less than $q/4$ (i.e., $3\alpha' q\sigma m < q/4$).
- $\mathsf{TrapGen}$ works correctly (i.e., $m > 3n \log q$).
- $\mathsf{SamplePre}$ and $\mathsf{Sample}\mathbb{Z}(\sigma)$ works correctly (i.e., $\sigma > \|\mathbf{T}_{\mathbf{A}}\|_{\mathrm{GS}} \cdot \sqrt{\log(2m+4)/\pi} = O(\sqrt{n \log m \log q})$).

- σ is sufficiently large to apply Lemmas 1–3 (i.e., $\sigma > \sqrt{n + \log m}, 16\sqrt{\log 2m/\pi}$).
- ReRand works correctly (i.e., $\alpha'/2\alpha > \sqrt{n(\sigma^2 m + 1)}$).
- LWE is hard (i.e., $\alpha q \geq 2\sqrt{n}$).

To satisfy all the requirements, we can set the parameters as follows:

$$m = n^{1+\delta}, \qquad q = 10n^{3.5+4\delta}, \qquad \sigma = n^{0.5+\delta},$$
$$\alpha' q = n^{2+2\delta}, \qquad \alpha q = 2\sqrt{n},$$

where $\delta > 0$ can be set an arbitrarily small constant.

5 Security in the Random Oracle Model

In this section, we prove the following theorem.

Theorem 1. *If the* $\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}$ *assumption holds, our proposed RIBE scheme in Section 4 achieves adaptive-identity anonymity security in the random oracle model. In particular, for any classical PPT adversary* $\mathcal{A}$ *making at most* Q_{H} *random oracle queries to* H *and* Q_{ID} *secret key generation queries, there exists a classical PPT reduction algorithm* $\mathcal{B}$ *such that*

$$\mathsf{Adv}^{\mathtt{RIBE}}_{\Pi,\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}}_{\mathcal{B}} + (Q_{\mathsf{H}} + Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}) \cdot 2^{-\Omega(\lambda)}$$

and

$$\mathsf{Time}(\mathcal{B}) = \mathsf{Time}(\mathcal{A}) + (Q_{\mathsf{H}} + Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}) \cdot \mathsf{poly}(\lambda),$$

where $\sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}$ *denotes the number of key update vectors* $\mathbf{e}_{\theta_j,\mathsf{T}}$ *created during the security game.*

Proof of Theorem 1. The proof proceeds with a sequence of games.

Game-0. This is adaptive-identity anonymity security game. Specifically, the challenger $\mathcal{C}$ behaves as follows:

- Upon an adversary $\mathcal{A}$'s random oracle query on $(\mathsf{ID}\|0)$, $\mathcal{C}$ returns $\mathbf{u}_{\mathsf{ID}} = \mathsf{H}(\mathsf{ID}\|0)$. Similarly, upon $\mathcal{A}$'s random oracle query on $(\mathsf{ID}[i]\|\mathsf{T})$, $\mathcal{C}$ returns $\mathbf{u}_{\mathsf{ID}[i],\mathsf{T}} = \mathsf{H}(\mathsf{ID}[i]\|\mathsf{T})$.
- Upon $\mathcal{A}$'s secret key generation query on ID, $\mathcal{C}$ runs $\mathbf{e}_{\mathsf{ID}} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{u}_{\mathsf{ID}}, \mathbf{T}_{\mathbf{A}}, \sigma)$.
- Upon $\mathcal{A}$'s revoke & key update query on T, to create $\mathbf{e}_{\theta_j,\mathsf{T}}$, $\mathcal{C}$ runs $\mathbf{e}_{\theta_j,\mathsf{T}} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{u}_{\theta_j,\mathsf{T}}, \mathbf{T}_{\mathbf{A}}, \sigma)$.
- Upon $\mathcal{A}$'s challenge query, $\mathcal{C}$ returns $\mathsf{ct}^\star \leftarrow \mathsf{Enc}(\mathsf{MPK}, \mathsf{ID}^\star, \mathsf{T}^\star, \mathsf{M}^\star)$ if $\mathsf{coin} = 0$ and a uniformly random element in $\mathbb{Z}_q^{m+\kappa_{\mathsf{ID}}+1}$ if $\mathsf{coin} = 1$.

Throughout the proof, we use $\mathsf{Adv}_j(\lambda)$ to denote $\mathcal{A}$'s advantage in Game-j.

Game-1. This is the same as Game-0 except the way $\mathcal{C}$ answers the random oracle queries. Upon $\mathcal{A}$'s random oracle query on $(\mathsf{ID}, 0)$ in Game-1, $\mathcal{C}$ first samples $\bar{\mathbf{e}}_{\mathsf{ID}} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma)$ and sets $\mathbf{u}_{\mathsf{ID}} = \mathbf{A}\bar{\mathbf{e}}_{\mathsf{ID}}$. Similarly, upon $\mathcal{A}$'s random oracle query on (θ_j, T), $\mathcal{C}$ first samples $\bar{\mathbf{e}}_{\theta_j,\mathsf{T}} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma)$ and sets $\mathbf{u}_{\theta_j,\mathsf{T}} = \mathbf{A}\bar{\mathbf{e}}_{\theta_j,\mathsf{T}}$. Then, $\mathcal{C}$ returns $\mathbf{u}_{\mathsf{ID}}$ and $\mathbf{u}_{\theta_j,\mathsf{T}}$ to $\mathcal{A}$. Whenever $\mathcal{C}$ answers the random oracle queries, it stores $(\mathsf{ID}, 0, \mathbf{u}_{\mathsf{ID}}, \bar{\mathbf{e}}_{\mathsf{ID}})$ and $(\theta_j, \mathsf{T}, \mathbf{u}_{\theta_j,\mathsf{T}}, \bar{\mathbf{e}}_{\theta_j,\mathsf{T}})$.

Based on our choice of parameters, we can apply Lemma 1 which ensures that all $\mathbf{u}_{\mathsf{ID}}$ and $\mathbf{u}_{\mathsf{ID}[i],\mathsf{T}}$ are statistically close to uniform as in Game-0. Thus, the change of $\mathcal{A}$'s advantage between Game-0 and Game-1 is negligible. In particular, $|\mathsf{Adv}_0(\lambda) - \mathsf{Adv}_1(\lambda)| \leq Q_{\mathsf{H}} \cdot 2^{-\Omega(n)}$ holds.

Game-2. This is the same as Game-1 except the way $\mathcal{C}$ creates secret key vectors $\mathbf{e}_{\mathsf{ID}}$ and key update vectors $\mathbf{e}_{\theta_j,\mathsf{T}}$. In particular, $\mathcal{C}$ does not use a master secret key $\mathbf{T}_{\mathbf{A}}$ to create them. When $\mathcal{C}$ creates $\mathbf{e}_{\mathsf{ID}}$, it does not run the $\mathsf{SamplePre}$ algorithm but sets $\mathbf{e}_{\mathsf{ID}} = \bar{\mathbf{e}}_{\mathsf{ID}}$ which was created upon $\mathcal{A}$'s random oracle queries on $(\mathsf{ID}, 0)$. Similarly, when $\mathcal{C}$ creates $\mathbf{e}_{\theta_j,\mathsf{T}}$, it does not run the $\mathsf{SamplePre}$ algorithm but sets $\mathbf{e}_{\theta_j,\mathsf{T}} = \bar{\mathbf{e}}_{\theta_j,\mathsf{T}}$ which was created upon $\mathcal{A}$'s random oracle queries on (θ_j, T).

Based on our choice of parameters, we can apply Lemma 5 which ensures that $\mathbf{e}_{\mathsf{ID}}$ and $\mathbf{e}_{\theta_j,\mathsf{T}}$ in Game-1 sampled by the $\mathsf{SamplePre}$ algorithm distribute statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A}),\sigma}$ and $\mathcal{D}_{\Lambda_q^{\mathbf{u}_{\theta_j,\mathsf{T}}}(\mathbf{A}),\sigma}$, respectively. In contrast, based on our choice of parameters, we can apply Lemma 1 which ensures that $\mathbf{e}_{\mathsf{ID}}$ and $\mathbf{e}_{\theta_j,\mathsf{T}}$ in Game-2 distribute statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A}),\sigma}$ and $\mathcal{D}_{\Lambda_q^{\mathbf{u}_{\theta_j,\mathsf{T}}}(\mathbf{A}),\sigma}$ conditioned on $\mathbf{u}_{\mathsf{ID}}$ and $\mathbf{u}_{\theta_j,\mathsf{T}}$, respectively. Thus, the change of $\mathcal{A}$'s advantage between Game-1 and Game-2 is negligible. In particular, $|\mathsf{Adv}_1(\lambda) - \mathsf{Adv}_2(\lambda)| \leq (Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}) \cdot 2^{-\Omega(n)}$ holds.

Game-3. This is the same as Game-2 except the way $\mathcal{C}$ creates a master public key $\mathbf{A}$. In Game-3, $\mathcal{C}$ does not run the $\mathsf{TrapGen}$ algorithm but samples a uniformly random matrix $\mathbf{A} \leftarrow_R \mathbb{Z}_q^{n\times m}$. Since $\mathcal{C}$ did not use a master secret key $\mathbf{T}_{\mathbf{A}}$ to answer $\mathcal{A}$'s queries in Game-2, it can answer all $\mathcal{A}$'s queries in the same way.

Based on our choice of parameters, we can apply Lemma 5 which ensures that $\mathbf{A}$ in Game-2 distributes statistically close to uniform in $\mathbb{Z}_q^{n\times m}$. Thus, the change of $\mathcal{A}$'s advantage between Game-2 and Game-3 is negligible. In particular, $|\mathsf{Adv}_2(\lambda) - \mathsf{Adv}_3(\lambda)| \leq 2^{-\Omega(n)}$ holds.

Game-4. This is the same as Game-3 except the way $\mathcal{C}$ creates a challenge ciphertext $\mathsf{ct}^\star$ when $\mathsf{coin} = 0$. In Game-3, $\mathcal{C}$ samples $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,\alpha' q}$, and $x_i \leftarrow D_{\mathbb{Z},\alpha' q}$ for $i \in [0, \kappa_{\mathsf{ID}}]$, then computes

$$\mathbf{c} = \mathbf{A}^\top \mathbf{s} + \mathbf{x}, \qquad c_i = (\mathbf{u}_{\mathsf{ID}^\star}^\top + \mathbf{u}_{\mathsf{ID}^\star[i],\mathsf{T}^\star}^\top)\mathbf{s} + x_i + \mathsf{M}^\star \left\lfloor \frac{q}{2} \right\rfloor.$$

In Game-4, $\mathcal{C}$ samples $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$, $\bar{\mathbf{x}} \leftarrow D_{\mathbb{Z}^m,\alpha q}$ and computes

$$\bar{\mathbf{c}} = \mathbf{A}^\top \mathbf{s} + \bar{\mathbf{x}}. \tag{1}$$

Then, $\mathcal{C}$ finds $(\mathsf{ID}^\star, 0, \mathbf{u}_{\mathsf{ID}^\star}, \bar{\mathbf{e}}_{\mathsf{ID}^\star})$ and $(\mathsf{ID}^\star[i], \mathsf{T}^\star, \mathbf{u}_{\mathsf{ID}^\star[i],\mathsf{T}^\star}, \bar{\mathbf{e}}_{\mathsf{ID}^\star[i],\mathsf{T}^\star})$ for $i \in [0, \kappa_{\mathsf{ID}}]$ that are stored locally. $\mathcal{C}$ applies the noise rerandomization algorithm in Lemma 4 to obtain

$$[\mathbf{c} \| \bar{c}_0 \| \cdots \| \bar{c}_{\kappa_{\mathsf{ID}}}] \leftarrow \mathsf{ReRand}([\mathbf{I}_m | \bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star} | \cdots | \bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}], \bar{\mathbf{c}}, \alpha q, \frac{\alpha'}{\alpha q}). \tag{2}$$

$\mathcal{C}$ sets

$$c_i = \bar{c}_i + \mathsf{M}^\star \left\lfloor \frac{q}{2} \right\rfloor \tag{3}$$

for $i \in [0, \kappa_{\mathsf{ID}}]$ and outputs $\mathsf{ct}^\star = (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]})$.

Based on our choice of parameters, $\mathcal{C}$ can run the noise re-randomization algorithm in Lemma 4 which ensures thats

$$\begin{aligned}[\mathbf{c}\|\bar{c}_0\|\cdots\|\bar{c}_{\kappa_{\mathsf{ID}}}] &= [\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top(\mathbf{A}^\top\mathbf{s}) + \bar{\mathbf{x}}' \\ &= (\mathbf{A}\cdot[\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}])^\top\mathbf{s} + \bar{\mathbf{x}}' \\ &= [\mathbf{A}|\mathbf{u}_{\mathsf{ID}^\star} + \mathbf{u}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\mathbf{u}_{\mathsf{ID}^\star} + \mathbf{u}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top\mathbf{s} + \bar{\mathbf{x}}'\end{aligned} \tag{4}$$

holds, where $\bar{\mathbf{x}}'$ distributes statistically close to $D_{\mathbb{Z}^{m+\kappa_{\mathsf{ID}}+1},\alpha' q}$ as in Game-3. Thus, the change of $\mathcal{A}$'s advantage between Game-3 and Game-4 is negligible. In particular, $|\mathsf{Adv}_3(\lambda) - \mathsf{Adv}_4(\lambda)| \leq 2^{-\Omega(n)}$ holds.

Game-5. This is the same as Game-4 except the way $\mathcal{C}$ creates $\bar{\mathbf{c}}$ of the equation (1) when $\mathsf{coin} = 0$. In Game-5, $\mathcal{C}$ sets $\bar{\mathbf{c}} = \mathbf{v} + \mathbf{x}$, where $\mathbf{v} \leftarrow_R \mathbb{Z}_q^m$ and $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\alpha q}$.

The $\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}$ assumption ensures that Game-4 and Game-5 are computationally indistinguishable. In particular, for any classical PPT adversary $\mathcal{A}$, there exists a classical reduction algorithm $\mathcal{B}$ such that $|\mathsf{Adv}_4(\lambda) - \mathsf{Adv}_5(\lambda)| \leq \mathsf{Adv}^{\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}}_{\mathcal{B}}$.

Reduction from LWE. Given the $\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}$ instance $(\mathbf{A}, \mathbf{b})$, where $\mathbf{b} = \mathbf{A}^\top\mathbf{s}+\mathbf{x}$ or $\mathbf{b} = \mathbf{v}+\mathbf{x}$ and $\mathbf{s} \leftarrow_R \mathbb{Z}^n$, $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\alpha q}$, $\mathbf{v} \leftarrow_R \mathbb{Z}^m$, the reduction algorithm $\mathcal{B}$ gives $\mathsf{MPK} = \mathbf{A}$ to $\mathcal{A}$. Here, MPK distributes in the same way as that in Game-4. $\mathcal{B}$ behaves in the same way as $\mathcal{C}$ in Game-4 upon $\mathcal{A}$'s random oracle queries, secret key generation queries, secret key reveal queries, and revoke & key update queries. Upon $\mathcal{A}$'s challenge query, $\mathcal{B}$ behaves in the same way as $\mathcal{C}$ in Game-4 if $\mathsf{coin} = 1$. If $\mathsf{coin} = 0$, $\mathcal{B}$ sets

$$\bar{\mathbf{c}} = \mathbf{b}$$

in place of (1). The remaining procedures for computing $\mathsf{ct}^\star = (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]})$ are unchanged. After $\mathcal{B}$ receives $\widehat{\mathsf{coin}}$ from $\mathcal{A}$, it outputs $\widehat{\mathsf{coin}}$.

If $\mathbf{b} = \mathbf{A}^\top\mathbf{s} + \mathbf{x}$, where $\mathbf{s} \leftarrow_R \mathbb{Z}^n$, $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\alpha q}$, $\bar{\mathbf{c}} = \mathbf{A}^\top\mathbf{s} + \mathbf{x}$ follows the same distribution as in Game-4. Otherwise, $\bar{\mathbf{c}} = \mathbf{v} + \mathbf{x}$ follows the same distribution as in Game-5. Thus, we complete the reduction.

Game-6. This is the same as Game-5 except the way $\mathcal{C}$ computes $[\mathbf{c}\|\bar{c}_0\|\cdots\|\bar{c}_{\kappa_{\mathsf{ID}}}]$ of (2) when $\mathsf{coin} = 0$. In Game-6, $\mathcal{C}$ does not apply the noise re-randomization algorithm in Lemma 4 but samples $\bar{\mathbf{c}} \leftarrow_R \mathbb{Z}_q^m$, $\mathbf{x}' \leftarrow D_{\mathbb{Z}^{m+\kappa_{\mathsf{ID}}+1},\alpha' q}$ and computes

$$[\mathbf{c}\|\bar{c}_0\|\cdots\|\bar{c}_{\kappa_{\mathsf{ID}}}] = [\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top\bar{\mathbf{c}} + \bar{\mathbf{x}}'. \tag{5}$$

Based on our choice of parameters, $\mathcal{C}$ can run the noise re-randomization algorithm in Lemma 4 which ensures that $[\mathbf{c}\|\bar{c}_0\|\cdots\|\bar{c}_{\kappa_{\mathsf{ID}}}]$ in Game-5 distributes statistically close to (5). Thus, the change of $\mathcal{A}$'s advantage between Game-5 and Game-6 is negligible. In particular, $|\mathsf{Adv}_5(\lambda) - \mathsf{Adv}_6(\lambda)| \leq 2^{-\Omega(n)}$ holds.

Game-7. This is the same as Game-6 except the way $\mathcal{C}$ computes the challenge ciphertext $\mathsf{ct}^\star = (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]})$ when $\mathsf{coin} = 0$. In Game-7, regardless of the value $\mathsf{coin} \leftarrow_R \{0, 1\}$, $\mathcal{C}$ samples $\mathsf{ct}^\star = (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]}) \leftarrow_R \mathbb{Z}_q^m \times \mathbb{Z}_q^{\kappa_{\mathsf{ID}}+1}$. Thus, $\mathcal{A}$'s advantage in Game-7 is exactly zero. In particular, $\mathsf{Adv}_7(\lambda) = 0$ holds.

We show that Game-6 and Game-7 are statistically indistinguishable by proving that $[\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top \bar{\mathbf{c}}$ in the right hand side of (5) distributes statistically close to the uniform distribution on $\mathbb{Z}_q^{m+\kappa_{\mathsf{ID}}+1}$.

At first, we consider the case when $\mathsf{ID}^\star$ is revoked by $\mathsf{T}^\star$. In this case, $\mathcal{A}$ may receive $\bar{\mathbf{e}}_{\mathsf{ID}^\star}$ but does not receive $\bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}, \ldots, \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}$ that distribute according to $\mathcal{D}_{\Lambda_q^{\mathbf{u}_{\mathsf{ID}^\star[0]}}(\mathbf{A}),\sigma}, \ldots, \mathcal{D}_{\Lambda_q^{\mathbf{u}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}]}}(\mathbf{A}),\sigma}$, respectively. Based on our choice of parameters, Lemma 3 ensures that $\mathbf{H}_\infty(D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID}^\star[i]}}(\mathbf{A}),\sigma}) \geq m-1$ for all but $2^{-\Omega(n)}$ fraction of $\mathbf{A}$. Then, we apply the leftover hash lemma to conclude that $[\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top \bar{\mathbf{c}}$ distributes $(\kappa_{\mathsf{ID}}+1)\sqrt{q/2^{m-1}}$-close to the uniform distribution on $\mathbb{Z}_q^{m+\kappa_{\mathsf{ID}}+1}$. Thus, $[\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top \bar{\mathbf{c}}$ in the right hand side of (5) also distributes $(\kappa_{\mathsf{ID}}+1)\sqrt{q/2^{m-1}}$-close to the uniform distribution on $\mathbb{Z}_q^{m+\kappa_{\mathsf{ID}}+1}$.

Next, we consider the case when $\mathsf{ID}^\star$ is not revoked by $\mathsf{T}^\star$. In this case, $\mathcal{A}$ does not receive $\bar{\mathbf{e}}_{\mathsf{ID}^\star}$ but receives $\bar{\mathbf{e}}_{\mathsf{ID}^\star[j],\mathsf{T}^\star}$ for *only one* $i \in [0,\kappa_{\mathsf{ID}}]$. By following the same discussion as above, Lemma 3 ensures that $[\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star}|\bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star[j-1],\mathsf{T}^\star}|\bar{\mathbf{e}}_{\mathsf{ID}^\star[j+1],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top \bar{\mathbf{c}}$ is distributed uniformly at random in $\mathbb{Z}_q^{m+\kappa_{\mathsf{ID}}+1}$. Thus, $[\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top \bar{\mathbf{c}}$ in the right hand side of (5) also distributes $(\kappa_{\mathsf{ID}}+1)\sqrt{q/2^{m-1}}$-close to the uniform distribution on $\mathbb{Z}_q^{m+\kappa_{\mathsf{ID}}+1}$.

To summarize the above discussion, we have $|\mathsf{Adv}_6(\lambda) - \mathsf{Adv}_7(\lambda)| \leq 2^{-\Omega(n)} + (\kappa_{\mathsf{ID}}+1)\sqrt{q/2^{m-1}} \leq 2^{-\Omega(n)}$.

□

6 Security in the Quantum Random Oracle Model

In this section, we prove the security of our proposed RIBE scheme in the quantum random oracle model (QROM). In advance, we review the basic of the quantum random oracle model in Section 6.1 and prove the security in Section 6.2.

6.1 Preliminaries on Quantum Random Oracle Model

Quantum Computation. Let $|0\rangle := (1,0)^\top$ and $|1\rangle := (0,1)^\top$ denote the state of 1 qubit. Let $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \in \mathbb{C}^{2^n}$ denote the state of n qubits, where $\alpha_x \in \mathbb{C}$ satisfying $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$ and $|x\rangle = |x_1 x_2 \cdots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$ for $x_1, x_2, \ldots, x_n \in \{0,1\}$ is an orthonormal basis on $\mathbb{C}^{2^n}$ called the computational basis. If we measure the state $|\psi\rangle$ in the computational basis, the classical bit $x \in \{0,1\}^n$ is observed with probability $|\alpha_x|^2$ and the state becomes $|x\rangle$.

An arbitrary evolution of quantum state from $|\psi\rangle$ to $|\psi'\rangle$ is described by a unitary matrix U, where $|\psi'\rangle = U|\psi\rangle$. In short, a quantum algorithm is described by quantum evolutions that consist of evolutions with unitary matrices and measurements. The running time $\mathsf{Time}(\mathcal{A})$ of a quantum algorithm $\mathcal{A}$ is defined to be the number of universal gates and measurements required for running $\mathcal{A}$. If $\mathcal{A}$ is a quantum oracle algorithm, we assume that $\mathcal{A}$ runs in a unit time. Any efficient classical computation can be achieved by a quantum computation efficiently. In particular, for any function f that is classically computable, there exists a unitary matrix U_f such that $U_f|x,y\rangle = |x, f(x)\oplus y\rangle$, and the number of universal gates to express U_f is linear in the size of a classical circuit that computes f.

Quantum random oracle model. The notion of the QROM was introduced by Boneh et al. [BDF+11] as an extension of the (classical) random oracle model (ROM) in a quantum world. As the case of the ROM, the QROM is an idealized model, where a hash function is idealized to be an oracle that simulates a random function. On the other hand, as opposed to the ROM, the hash function in the QROM is a quantumly accessible oracle. In security proofs in the QROM, a random

function $\mathsf{H} : \mathcal{X} \to \mathcal{Y}$ is uniformly chosen at the beginning, and an adversary can make queries on a quantum state $\sum_{x,y} \alpha_{x,y}|x\rangle|y\rangle$ to the oracle and receive $\sum_{x,y} \alpha_{x,y}|x\rangle|\mathsf{H}(x) \oplus y\rangle$.

Let $\mathcal{A}^{|\mathsf{H}\rangle}$ denote a quantum algorithm that can quantumly access to the oracle $|\mathsf{H}\rangle$. Boneh et al. [BDF+11] proved the following useful lemma to simulate the quantum random oracle.

Lemma 6. *([BDF+11].) Let $\mathcal{A}$ be a quantum algorithm that makes at most Q oracle queries, and $\mathcal{X}$ and $\mathcal{Y}$ be arbitrary sets. Let $\mathcal{H}$ be a distribution over $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ such that when we take $\mathsf{H} \leftarrow_R \mathcal{H}$, for each $x \in \mathcal{X}$, $\mathsf{H}(x)$ is identically and independently distributed according to a distribution D whose statistical distance is within ϵ from uniform. Then for any input z, we have*

$$\Delta(\mathcal{A}^{|\mathsf{RF}\rangle}(z), \mathcal{A}^{|\mathsf{H}\rangle}(z)) \leq 4Q^2\sqrt{\epsilon}$$

where $\mathsf{RF} \leftarrow_R \mathsf{Func}(\mathcal{X}, \mathcal{Y})$ and $\mathsf{H} \leftarrow_R \mathcal{H}$.

Quantum-accessible Pseudorandom Function. We review the definition of quantum-accessible pseudorandom functions (PRFs) [BDF+11].

Definition 3 (Quantum-accessible PRF)**.** *We say that a function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ is a quantum-accessible pseudorandom function if for all quantum polynomial time adversaries $\mathcal{A}$, its advantage defined below is negligible:*

$$\mathsf{Adv}^{\mathsf{PRF}}_{\mathcal{A},F}(\lambda) := \left| \Pr\left[\mathcal{A}^{|\mathsf{RF}\rangle}(1^\lambda) = 1\right] - \Pr\left[\mathcal{A}^{|F(K,\cdot)\rangle}(1^\lambda) = 1\right] \right|$$

where $\mathsf{RF} \leftarrow_R \mathsf{Func}(\mathcal{X}, \mathcal{Y})$ and $K \leftarrow_R \mathcal{K}$.

Zhandry [Zha12a] showed that there are some known constructions for quantum-accessible PRFs [BPR12, GGM86]. On the other hand, their reductions are non-tight. In other words, if we rely on the constructions, we cannot achieve tight security. In turn, we use the following lemma which states that we can use a quantum random oracle as a PRF similarly to the classical case.

Lemma 7. *([SXY18, Lem. 2.2]) Let ℓ be an integer. Let $\mathsf{H}\colon \{0,1\}^\ell \times \mathcal{X} \to \mathcal{Y}$ and $\mathsf{H}'\colon \mathcal{X} \to \mathcal{Y}$ be two independent random functions. If an unbounded time quantum adversary $\mathcal{A}$ makes queries to H at most Q_{H} times, then we have*

$$\left|\Pr[\mathcal{A}^{|\mathsf{H}\rangle,|\mathsf{H}(K,\cdot)\rangle}(1^\lambda) = 1 \mid K \leftarrow \{0,1\}^\ell] - \Pr[\mathcal{A}^{|\mathsf{H}\rangle,|\mathsf{H}'\rangle}(1^\lambda) = 1]\right| \leq Q_{\mathsf{H}} \cdot 2^{\frac{-\ell+1}{2}}.$$

LWE Assumption relative to the QROM. We review the LWE assumption against adversaries that can access to a quantum random oracle defined in [KYY18].

Definition 4 (Learning with Errors relative to the QROM)**.** *Let n, m, q and χ be the same as in Definition 1, a and b be some positive integers. For a quantum polynomial time algorithm $\mathcal{A}$, the advantage for the* learning with errors problem $\mathsf{LWE}_{n,m,q,\chi}$ *of $\mathcal{A}$* relative to a quantum random oracle *is defined as follows:*

$$\mathsf{Adv}^{\mathsf{LWE}_{n,m,q,\chi}}_{\mathcal{A},\mathbf{QRO}_{a,b}}(\lambda) := \left| \Pr\left[\mathcal{A}^{|\mathsf{H}\rangle}(\mathbf{A}, \mathbf{A}^\top\mathbf{s} + \mathbf{z}) = 1\right] - \Pr\left[\mathcal{A}^{|\mathsf{H}\rangle}(\mathbf{A}, \mathbf{w} + \mathbf{z}) = 1\right] \right|$$

where $\mathbf{A} \leftarrow_R \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$, $\mathbf{w} \leftarrow_R \mathbb{Z}_q^m$, $\mathbf{z} \leftarrow \chi^m$, $\mathsf{H} \leftarrow_R \mathsf{Func}(\{0,1\}^a, \{0,1\}^b)$. We say that the LWE *assumption relative to an (a,b)-quantum random oracle holds if $\mathsf{Adv}^{\mathsf{LWE}_{n,m,q,\chi}}_{\mathcal{A},\mathbf{QRO}_{a,b}}(\lambda)$ is negligible for all quantum polynomial time algorithm $\mathcal{A}$.*

If we assume the existence of a quantum-accessible PRF, the LWE assumption relative to the QROM in Definition 4 is tightly reduced from the LWE assumption in Definition 1 as follows.

Lemma 8. *Let $F : \mathcal{K} \times \{0,1\}^a \to \{0,1\}^b$ be a quantum-accessible PRF. For any n, m, q, χ, a, b and a quantum polynomial time algorithm $\mathcal{A}$ making at most Q oracle queries, there exists quantum polynomial time algorithms $\mathcal{B}$ and $\mathcal{C}$ such that*

$$\mathsf{Adv}^{\mathsf{LWE}_{n,m,q,\chi}}_{\mathcal{A},\mathbf{QRO}_{a,b}}(\lambda) \leq \mathsf{Adv}^{\mathsf{LWE}_{n,m,q,\chi}}_{\mathcal{B}}(\lambda) + \mathsf{Adv}^{\mathsf{PRF}}_{\mathcal{C},F}(\lambda)$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A}) + Q \cdot T_F$ *and* $\mathsf{Time}(\mathcal{C}) \approx \mathsf{Time}(\mathcal{A})$*, where T_F denotes the time to evaluate F.*

6.2 Security

In this subsection, we prove the following theorem.

Theorem 2. *If the $\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}$ assumption holds, our proposed RIBE scheme in Section 4 achieves adaptive-identity anonymity security in the quantum random oracle model. In particular, for any quantum polynomial time adversary $\mathcal{A}$ making at most Q_{H} random oracle queries to $|\mathsf{H}\rangle$ and Q_{ID} secret key generation queries, there exists a quantum polynomial time reduction algorithm $\mathcal{B}$ making $Q_{\mathsf{H}} + Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}$ quantum random oracle queries such that*

$$\mathsf{Adv}^{\mathtt{RIBE}}_{\Pi,\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}}_{\mathcal{B},\mathbf{QRO}_{\kappa_{\mathsf{ID}}+\kappa_{\mathsf{T}}+1,\ell}} + (Q_{\mathsf{H}}^2 + Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}) \cdot 2^{-\Omega(\lambda)}$$

and

$$\mathsf{Time}(\mathcal{B}) = \mathsf{Time}(\mathcal{A}) + (Q_{\mathsf{H}} + Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}) \cdot \mathsf{poly}(\lambda),$$

where ℓ denotes the length of randomness for $\mathsf{Sample}\mathbb{Z}$ and $\sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}$ denotes the number of key update vectors $\mathbf{e}_{\theta_j,\mathsf{T}}$ created during the security game.

Proof of Theorem 2. The proof proceeds with a sequence of games.

Game-0. This is adaptive-identity anonymity security game. Specifically, the challenger $\mathcal{C}$ behaves as follows:

- At the beginning of the game, $\mathcal{C}$ chooses a random function $\mathsf{H} : \{0,1\}^{\kappa_{\mathsf{ID}}+\kappa_{\mathsf{T}}+1} \to \mathbb{Z}_q^n$.
- Upon an adversary $\mathcal{A}$'s quantum random oracle query on a state $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y}|(\mathsf{ID}\|\mathsf{T})\rangle|y\rangle$, $\mathcal{C}$ returns $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y}|(\mathsf{ID}\|\mathsf{T})\rangle|\mathsf{H}(\mathsf{ID}\|\mathsf{T}) \oplus y\rangle$.
- Upon $\mathcal{A}$'s secret key generation query on ID, $\mathcal{C}$ runs $\mathbf{e}_{\mathsf{ID}} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{u}_{\mathsf{ID}}, \mathbf{T}_{\mathbf{A}}, \sigma)$.
- Upon $\mathcal{A}$'s revoke & key update query on T, to create $\mathbf{e}_{\theta_j,\mathsf{T}}$, $\mathcal{C}$ runs $\mathbf{e}_{\theta_j,\mathsf{T}} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{u}_{\theta_j,\mathsf{T}}, \mathbf{T}_{\mathbf{A}}, \sigma)$.
- Upon $\mathcal{A}$'s challenge query, $\mathcal{C}$ returns $\mathsf{ct}^\star \leftarrow \mathsf{Enc}(\mathsf{MPK}, \mathsf{ID}^\star, \mathsf{T}^\star, \mathsf{M}^\star)$ if $\mathsf{coin} = 0$ and a uniformly random element in $\mathbb{Z}_q^{m+\kappa_{\mathsf{ID}}+1}$ if $\mathsf{coin} = 1$.

Throughout the proof, we use $\mathsf{Adv}_j(\lambda)$ to denote $\mathcal{A}$'s advantage in Game-j.

Game-1. This is the same as Game-0 except the way $\mathcal{C}$ answers the quantum random oracle queries. $\mathcal{C}$ first chooses a random function $\widehat{\mathsf{H}} \leftarrow_R \mathsf{Func}(\{0,1\}^{\kappa_{\mathsf{ID}}+\kappa_{\mathsf{T}}+1}, \{0,1\}^{\ell})$ and define $\mathsf{H} : \{0,1\}^{\kappa_{\mathsf{ID}}+\kappa_{\mathsf{T}}+1} \to \mathbb{Z}_q^n$ by $\mathsf{H}(\mathsf{ID}\|\mathsf{T}) := \mathbf{A}\bar{\mathbf{e}}_{\mathsf{ID},\mathsf{T}}$, where $\bar{\mathbf{e}}_{\mathsf{ID},\mathsf{T}} := \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|\mathsf{T}))$. Here, $\mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|\mathsf{T}))$ denotes running $\mathsf{Sample}\mathbb{Z}(\sigma)$ algorithm with a random coin $\widehat{\mathsf{H}}(\mathsf{ID}\|\mathsf{T})$. If $\mathsf{T} = 0$, we may simply write $\mathbf{u}_{\mathsf{ID}}$ and $\bar{\mathbf{e}}_{\mathsf{ID}}$.

By following the same argument in Game-1 of the proof of Theorem 1, $\mathbf{u}_{\mathsf{ID}}$ and $\mathbf{u}_{\mathsf{ID}[i],\mathsf{T}}$ are statistically close to uniform as in Game-0. Thus, Lemma 6 ensures that $|\mathsf{Adv}_0(\lambda) - \mathsf{Adv}_1(\lambda)| \leq 2^{-\Omega(n)} + 4Q_{\mathsf{H}}^2 \cdot \sqrt{2^{-\Omega(n)}} = Q_{\mathsf{H}}^2 \cdot 2^{-\Omega(n)}$.

Game-2. This is the same as Game-1 except the way $\mathcal{C}$ creates secret key vectors $\mathbf{e}_{\mathsf{ID}}$ and key update vectors $\mathbf{e}_{\theta_j,\mathsf{T}}$. In particular, $\mathcal{C}$ does not use the master secret key $\mathbf{T}_{\mathbf{A}}$ to create them. When $\mathcal{C}$ creates $\mathbf{e}_{\mathsf{ID}}$, it does not run the $\mathsf{SamplePre}$ algorithm but sets $\mathbf{e}_{\mathsf{ID}} = \bar{\mathbf{e}}_{\mathsf{ID}} = \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|0))$ which was created upon $\mathcal{A}$'s quantum random oracle queries on $(\mathsf{ID}\|0)$. Similarly, when $\mathcal{C}$ creates $\mathbf{e}_{\theta_j,\mathsf{T}}$, it does not run the $\mathsf{SamplePre}$ algorithm but sets $\mathbf{e}_{\theta_j,\mathsf{T}} = \bar{\mathbf{e}}_{\theta_j,\mathsf{T}} = \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\theta_j\|\mathsf{T}))$ which was created upon $\mathcal{A}$'s quantum random oracle queries on $(\theta_j\|\mathsf{T})$.

By following the same argument in Game-2 of the proof of Theorem 1, we have $|\mathsf{Adv}_1(\lambda) - \mathsf{Adv}_2(\lambda)| \leq (Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}) \cdot 2^{-\Omega(n)}$.

Game-3. This is the same as Game-2 except the way $\mathcal{C}$ creates a master public key $\mathbf{A}$. In Game-3, $\mathcal{C}$ does not run the $\mathsf{TrapGen}$ algorithm but samples a uniformly random matrix $\mathbf{A} \leftarrow_R \mathbb{Z}_q^{n\times m}$. Since $\mathcal{C}$ did not use a master secret key $\mathbf{T}_{\mathbf{A}}$ to answer $\mathcal{A}$'s queries in Game-2, it can answer all $\mathcal{A}$'s queries in the same way.

By following the same argument in Game-3 of the proof of Theorem 1, we have $|\mathsf{Adv}_2(\lambda) - \mathsf{Adv}_3(\lambda)| \leq 2^{-\Omega(n)}$.

Game-4. This is the same as Game-3 except the way $\mathcal{C}$ creates a challenge ciphertext $\mathsf{ct}^\star$ when $\mathsf{coin} = 0$. In Game-3, $\mathcal{C}$ samples $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,\alpha' q}$, and $x_i \leftarrow D_{\mathbb{Z},\alpha' q}$ for $i \in [0, \kappa_{\mathsf{ID}}]$, then computes

$$\mathbf{c} = \mathbf{A}^\top \mathbf{s} + \mathbf{x}, \qquad c_i = (\mathbf{u}_{\mathsf{ID}^\star}^\top + \mathbf{u}_{\mathsf{ID}^\star[i],\mathsf{T}^\star}^\top)\mathbf{s} + x_i + \mathsf{M}^\star \left\lfloor \frac{q}{2} \right\rfloor.$$

In Game-4, $\mathcal{C}$ samples $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$, $\bar{\mathbf{x}} \leftarrow D_{\mathbb{Z}^m,\alpha q}$ and computes

$$\bar{\mathbf{c}} = \mathbf{A}^\top \mathbf{s} + \bar{\mathbf{x}}. \tag{6}$$

Then, $\mathcal{C}$ computes $\bar{\mathbf{e}}_{\mathsf{ID}^\star} = \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}^\star\|0))$ and $\bar{\mathbf{e}}_{\mathsf{ID}^\star[i],\mathsf{T}^\star} = \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}^\star[i]\|\mathsf{T}^\star))$ for $i \in [0, \kappa_{\mathsf{ID}}]$. $\mathcal{C}$ applies the noise rerandomization algorithm in Lemma 4 to obtain

$$[\mathbf{c}\|\bar{c}_0\| \cdots \|\bar{c}_{\kappa_{\mathsf{ID}}}] \leftarrow \mathsf{ReRand}([\mathbf{I}_m | \bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star} | \cdots | \bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}], \bar{\mathbf{c}}, \alpha q, \frac{\alpha'}{\alpha q}). \tag{7}$$

$\mathcal{C}$ sets

$$c_i = \bar{c}_i + \mathsf{M}^\star \left\lfloor \frac{q}{2} \right\rfloor \tag{8}$$

for $i \in [0, \kappa_{\mathsf{ID}}]$ and outputs $\mathsf{ct}^\star = (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]})$.

By following the same argument in Game-2 of the proof of Theorem 1, we have $|\mathsf{Adv}_3(\lambda) - \mathsf{Adv}_4(\lambda)| \leq 2^{-\Omega(n)}$.

Game-5. This is the same as Game-4 except the way $\mathcal{C}$ creates $\bar{\mathbf{c}}$ of the equation (6) when $\mathsf{coin} = 0$. In Game-5, $\mathcal{C}$ sets $\bar{\mathbf{c}} = \mathbf{v} + \mathbf{x}$, where $\mathbf{v} \leftarrow_R \mathbb{Z}_q^m$ and $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\alpha q}$.

The $\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}$ assumption relative to a quantum random oracle $\widehat{\mathsf{H}} : \{0,1\}^{\kappa_{\mathsf{ID}}+\kappa_{\mathsf{T}}+1} \to \{0,1\}^{\ell}$ ensures that Game-4 and Game-5 are computationally indistinguishable. In particular, for any quantum PPT adversary $\mathcal{A}$, there exists a quantum reduction algorithm $\mathcal{B}$ such that $|\mathsf{Adv}_4(\lambda) - \mathsf{Adv}_5(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}}$.

Reduction from LWE. Given the $\mathsf{LWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}$ instance $(\mathbf{A}, \mathbf{b})$, where $\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathbf{x}$ or $\mathbf{b} = \mathbf{v} + \mathbf{x}$ and $\mathbf{s} \leftarrow \mathbb{Z}^n$, $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\alpha q}$, $\mathbf{v} \leftarrow \mathbb{Z}^m$, the reduction algorithm $\mathcal{B}$ gives $\mathsf{MPK} = \mathbf{A}$ to $\mathcal{A}$. Here, MPK distributes in the same way as that in Game-4. To answer $\mathcal{A}$'s quantum random oracle queries on a state $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y} |(\mathsf{ID}\|\mathsf{T})\rangle|y\rangle$, $\mathcal{B}$ can answer $\mathcal{A}$'s quantum random oracle queries to compute $\mathsf{H}(\mathsf{ID}\|\mathsf{T}) = \mathbf{A}\bar{\mathbf{e}}_{\mathsf{ID},\mathsf{T}}$, where $\bar{\mathbf{e}}_{\mathsf{ID},\mathsf{T}} = \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|\mathsf{T}))$, by accessing their own quantum random oracle $\widehat{\mathsf{H}} : \{0,1\}^{\kappa_{\mathsf{ID}}+\kappa_{\mathsf{T}}+1} \to \{0,1\}^{\ell}$. $\mathcal{B}$ behaves in the same way as $\mathcal{C}$ in Game-4 upon $\mathcal{A}$'s secret key generation queries, secret key reveal queries, and revoke & key update queries. Upon $\mathcal{A}$'s challenge query, $\mathcal{B}$ behaves in the same way as $\mathcal{C}$ in Game-4 if $\mathsf{coin} = 1$. If $\mathsf{coin} = 0$, $\mathcal{B}$ sets

$$\bar{\mathbf{c}} = \mathbf{b}$$

in place of (1). The remaining procedures for computing $\mathsf{ct}^\star = (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]})$ are unchanged. After $\mathcal{B}$ receives $\widehat{\mathsf{coin}}$ from $\mathcal{A}$, it outputs $\widehat{\mathsf{coin}}$.

If $\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathbf{x}$, where $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\alpha q}$, $\bar{\mathbf{c}} = \mathbf{A}^\top \mathbf{s} + \mathbf{x}$ follows the same distribution as in Game-4. Otherwise, $\bar{\mathbf{c}} = \mathbf{v} + \mathbf{x}$ follows the same distribution as in Game-5. Thus, we complete the reduction.

Game-6. This is the same as Game-5 except the way $\mathcal{C}$ computes $[\mathbf{c}\|\bar{c}_0\| \cdots \|\bar{c}_{\kappa_{\mathsf{ID}}}]$ of (7) when $\mathsf{coin} = 0$. In Game-6, $\mathcal{C}$ does not apply the noise re-randomization algorithm in Lemma 4 but samples $\bar{\mathbf{c}} \leftarrow_R \mathbb{Z}_q^m$, $\mathbf{x}' \leftarrow D_{\mathbb{Z}^{m+\kappa_{\mathsf{ID}}+1},\alpha' q}$ and computes

$$[\mathbf{c}\|\bar{c}_0\| \cdots \|\bar{c}_{\kappa_{\mathsf{ID}}}] = [\mathbf{I}_m | \bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star} | \cdots | \bar{\mathbf{e}}_{\mathsf{ID}^\star} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top \bar{\mathbf{c}} + \bar{\mathbf{x}}'. \tag{9}$$

By following the same argument in Game-6 of the proof of Theorem 1, we have $|\mathsf{Adv}_5(\lambda) - \mathsf{Adv}_6(\lambda)| \leq 2^{-\Omega(n)}$ holds.

Game-7. This is the same as Game-6 except the way $\mathcal{C}$ computes the challenge ciphertext $\mathsf{ct}^\star = (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]})$ when $\mathsf{coin} = 0$. In Game-7, regardless of the value $\mathsf{coin} \leftarrow_R \{0,1\}$, $\mathcal{C}$ samples $\mathsf{ct}^\star = (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]}) \leftarrow_R \mathbb{Z}_q^m \times \mathbb{Z}_q^{\kappa_{\mathsf{ID}}+1}$. Thus, $\mathcal{A}$'s advantage in Game-7 is exactly zero. In particular, $\mathsf{Adv}_7(\lambda) = 0$ holds.

By following the same argument in Game-7 of the proof of Theorem 1, we have $|\mathsf{Adv}_6(\lambda) - \mathsf{Adv}_7(\lambda)| \leq 2^{-\Omega(n)} + (\kappa_{\mathsf{ID}} + 1)\sqrt{q/2^{m-1}} \leq 2^{-\Omega(n)}$.

□

7 Achieving (Bounded) Decryption Key Exposure Resistance

In this section, we briefly summarize the modification of our RIBE scheme for achieving the stronger security requirement called (bounded) decryption key exposure resistance (DKER).

7.1 RIBE with DKER

Seo and Emura [SE13] introduced a security notion called DKER. Compared with the security definition in Section 3, RIBE with DKER has the following decryption key reveal queries:

Decryption Key Reveal Query: Until the challenge query, upon a query $(\mathsf{ID}, \mathsf{T}) \in \mathcal{ID} \times \mathcal{T}$ from $\mathcal{A}$, $\mathcal{C}$ checks

- If $\mathsf{T} \leq \mathsf{T}_{\mathsf{cu}}$ holds.
- If $\mathsf{ID} \notin \mathsf{RL}_{\mathsf{T}}$ holds.

After the challenge query, $\mathcal{C}$ also checks

- If $(\mathsf{ID}, \mathsf{T}) \neq (\mathsf{ID}^\star, \mathsf{T}^\star)$ holds.

If the conditions are *not* satisfied, then $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ finds $\mathsf{sk}_{\mathsf{ID}}$ from $\mathtt{SKList}$, runs $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} \leftarrow \mathsf{GenDK}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ku}_{\mathsf{T}})$, and returns $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ to $\mathcal{A}$.

To capture the additional queries, upon $\mathcal{A}$'s challenge query, $\mathcal{C}$ also checks

- If $\mathsf{T}^\star \leq \mathsf{T}_{\mathsf{cu}}$, $\mathcal{A}$ has not submitted $(\mathsf{ID}^\star, \mathsf{T}^\star)$ as a decryption key reveal query.

The security of RIBE with DKER is strictly stronger than RIBE without DKER. Indeed, our RIBE scheme in Section 4 has a concrete attack in the security model of RIBE with DKER. If an adversary $\mathcal{A}$ does not revoke $\mathsf{ID}^\star$ at a time period $\mathsf{T}^\star$ and receives a key update $\mathbf{e}_{\theta_d,\mathsf{T}}$ and a decryption key $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}} = \mathbf{e}_{\mathsf{ID}^\star} + \mathbf{e}_{\theta_d,\mathsf{T}}$ for the same T, it can retrieve $\mathsf{ID}^\star$'s secret key by computing $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}} - \mathbf{e}_{\theta_d,\mathsf{T}} = \mathbf{e}_{\mathsf{ID}^\star}$. Then, an adversary can compute a decryption key $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}^\star} = \mathbf{e}_{\mathsf{ID}^\star} + \mathbf{e}_{\theta_d,\mathsf{T}^\star}$ by using the retrieved secret key $\mathbf{e}_{\mathsf{ID}^\star}$ and the broadcast key update $\mathbf{e}_{\theta_d,\mathsf{T}^\star}$.

Nevertheless, we can transform our RIBE scheme to satisfy DKER. Katsumata et al. [KMT19] proved that we can obtain RIBE with DKER by combining RIBE without DKER and 2-level HIBE scheme. Thus, we can obtain a RIBE scheme with DKER by combining our RIBE scheme in Section 4 and adaptively secure lattice-based HIBE schemes in the QROM [ABB10a, ABB10b, Zha12b]. A point to note is that this transformation sacrifices two benefits of our RIBE scheme. At first, the transformation sacrifices anonymity. However, the fact is not very pessimistic since all known RIBE schemes with DKER do not satisfy anonymity. Next, since all known adaptively secure lattice-based HIBE schemes in the QROM [ABB10a, ABB10b, Zha12b] suffer from loose reduction, we have to sacrifice the tight reduction.

7.2 Anonymous RIBE with Bounded DKER

Takayasu and Watanabe [TW17] formalized bounded DKER which is a weaker security notion than the above full DKER. The main difference between the security definition with bounded DKER and full DKER is that there is a-priori bounded number Q and an adversary $\mathcal{A}$ is allowed to make decryption key queries at most Q times on $\mathsf{ID}^\star$. Compared with the security definition in Section 3, RIBE with bounded DKER has the following decryption key reveal queries:

Decryption Key Reveal Query: Until the challenge query, upon a query $(\mathsf{ID}, \mathsf{T}) \in \mathcal{ID} \times \mathcal{T}$ from $\mathcal{A}$, $\mathcal{C}$ checks

- If $\mathsf{T} \leq \mathsf{T}_{\mathsf{cu}}$ holds.
- If $\mathsf{ID} \notin \mathsf{RL}_{\mathsf{T}}$ holds.

After the challenge query, $\mathcal{C}$ also checks

- If $(\mathsf{ID}, \mathsf{T}) \neq (\mathsf{ID}^\star, \mathsf{T}^\star)$ holds.
- If $\mathsf{T}_{\mathsf{cu}} \geq \mathsf{T}^\star$ and $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}}$ has been revealed to $\mathcal{A}$ Q times by the decryption key reveal queries, $\mathsf{ID} \neq \mathsf{ID}^\star$.

If the conditions are *not* satisfied, then $\mathcal{C}$ returns $\bot$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ finds $\mathsf{sk}_{\mathsf{ID}}$ from $\mathtt{SKList}$, runs $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} \leftarrow \mathsf{GenDK}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ku}_{\mathsf{T}})$, and returns $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ to $\mathcal{A}$.

To capture the additional queries, there are two modifications. At first, upon $\mathcal{A}$'s revoke & key update query, after the challenge query $\mathcal{C}$ also checks that

- If $\mathsf{T}_{\mathsf{cu}} = \mathsf{T}^\star - 1$ and $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}}$ has been revealed to $\mathcal{A}$ Q times by the decryption key reveal queries, then $\mathsf{ID}^\star \in \mathsf{RL}$.

Next, upon $\mathcal{A}$'s challenge query, $\mathcal{C}$ also checks that

- If $\mathsf{T}^\star \leq \mathsf{T}_{\mathsf{cu}}$, $\mathcal{A}$ has not submitted $(\mathsf{ID}^\star, \mathsf{T}^\star)$ as a decryption key reveal query.
- If $\mathsf{T}^\star \leq \mathsf{T}_{\mathsf{cu}}$ and $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}}$ has been revealed to $\mathcal{A}$ more than Q times, then $\mathsf{ID}^\star \in \mathsf{RL}_{\mathsf{T}^\star}$.

As we discussed above, bounded DKER itself is a weaker security notion than full DKER. In contrast, the benefit of bounded DKER is that there are anonymous RIBE schemes with bounded DKER [TW17, TW21] although there are no anonymous RIBE schemes with full DKER. The constructions [TW17, TW21] make use of cover free families (CFF) [TW17, TW21]. Thus, we also apply CFF to our RIBE scheme in Section 4 and transform the scheme to satisfy bounded DKER without sacrificing anonymity. Although Takayasu and Watanabe's anonymous RIBE scheme with bounded DKER under the LWE assumption does not satisfy adaptive security, our scheme in the QROM achieves adaptive security.

Cover Free Family. We use the following result of CFF in our construction.

Definition 5 (Cover Free Families [EFF85])**.** *Let a, t, Q be positive integers, and $\mathcal{F} := \{\mathcal{F}_\mu\}_{\mu\in[a]}$ be a family of subsets of $[t]$, where $|\mathcal{F}_\mu| = w$ for all $\mu \in [a]$. $\mathcal{F}$ is said to be w-uniform Q-cover-free if it holds that $\bigcup_{j=1}^{Q} \mathcal{F}_{i_j} \not\supset \mathcal{F}_{i_{Q+1}}$ for any $\mathcal{F}_{i_1}, \mathcal{F}_{i_2}, \ldots, \mathcal{F}_{i_{Q+1}} \in \mathcal{F}$ such that $\mathcal{F}_{i_k} \neq \mathcal{F}_{i_\ell}$ for any distinct $k, \ell \in [Q+1]$.*

Lemma 9 ([KRS99])**.** *There is a deterministic polynomial time algorithm $\mathsf{CFF.Gen}$ that, on input of positive integers a and Q, returns $d \in \mathbb{N}$ and a family $\mathcal{F} = \{\mathcal{F}_\mu\}_{\mu\in[a]}$, such that $\mathcal{F}$ is Q-cover free over $[d]$ and w-uniform, where $t \leq 16Q^2 \log a$ and $w = d/4Q$.*

Construction. Let $\mathsf{H} : \{0,1\}^{(\kappa_{\mathsf{ID}}+\log t+\kappa_{\mathsf{T}}+1)} \to \mathbb{Z}_q^n$ be a hash function that will be modeled as a quantum random oracle.

$\mathsf{Setup}(1^n) \to (\mathsf{MPK}, \mathsf{MSK})$: Run $(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$ and output $\mathsf{MPK} := \mathbf{A}$ and $\mathsf{MSK} := \mathbf{T}_{\mathbf{A}}$.

$\mathsf{Enc}(\mathsf{MPK}, \mathsf{ID}, \mathsf{T}, \mathsf{M}) \to \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$: Sample a uniformly random vector $\mathbf{s} \leftarrow_R \mathbb{Z}_q^n$. Sample a random vector $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,\alpha' q}$ and random integers $x_i \leftarrow D_{\mathbb{Z},\alpha' q}$ for $i \in [0, \kappa_{\mathsf{ID}}]$ from discrete Gaussian distributions. Set $\mathbf{u}_{\mathsf{ID},k} := \mathsf{H}(\mathsf{ID}\|k\|0)$ for $k \in \mathcal{F}_{\mathsf{T}}$ and $\mathbf{u}_{\mathsf{ID}[i],\mathsf{T}} := \mathsf{H}(\mathsf{ID}[i]\|0\|\mathsf{T})$ for all $i \in [0, \kappa_{\mathsf{ID}}]$. Compute

$$\mathbf{c} = \mathbf{A}^\top \mathbf{s} + \mathbf{x}, \qquad c_i = \left(\sum_{k\in\mathcal{F}_{\mathsf{T}}} \mathbf{u}_{\mathsf{ID},k}^\top + \mathbf{u}_{\mathsf{ID}[i],\mathsf{T}}^\top \right) \mathbf{s} + x_i + \mathsf{M} \left\lfloor \frac{q}{2} \right\rfloor \quad \text{for } i \in [0, \kappa_{\mathsf{ID}}]$$

and output $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} := (\mathbf{c}, (c_i)_{i\in[0,\kappa_{\mathsf{ID}}]}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{\kappa_{\mathsf{ID}}+1}$.

$\mathsf{GenSK}(\mathsf{MPK}, \mathsf{MSK}, \mathsf{ID}) \to \mathsf{sk}_{\mathsf{ID}}$: Run

$$\mathbf{e}_{\mathsf{ID},k} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{u}_{\mathsf{ID},k}, \mathbf{T}_{\mathbf{A}}, \sigma) \quad \text{for } k \in [t]$$

and output $\mathsf{sk}_{\mathsf{ID}} := (\mathbf{e}_{\mathsf{ID},k})_{k\in[t]}$.

$\mathsf{KeyUp}(\mathsf{MPK}, \mathsf{T}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{RL}_{\mathsf{T}}) \to \mathsf{ku}_{\mathsf{T}}$: Run the KUNode algorithm to obtain a set of nodes KU_{T}. For every $\theta_j \in \mathsf{KU}_{\mathsf{T}}$, run

$$\mathbf{e}_{\theta_j,\mathsf{T}} \leftarrow \mathsf{SamplePre}(\mathbf{A}, \mathbf{u}_{\theta_j,\mathsf{T}}, \mathbf{T}_{\mathbf{A}}, \sigma)$$

and outputs $\mathsf{ku}_{\mathsf{T}} := (\mathbf{e}_{\theta_j,\mathsf{T}})_{\theta_j \in \mathsf{KU}_{\mathsf{T}}}$.

$\mathsf{GenDK}(\mathsf{MPK}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ku}_{\mathsf{T}}) \to \mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ or $\perp$: Find a node $\mathsf{ID}[d] \in \mathsf{KU}_{\mathsf{T}}$ for some $d \in [0, \kappa_{\mathsf{ID}}]$. If it does not exist, output $\perp$. Otherwise, output $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} := \mathbf{d}_{\mathsf{ID},\mathsf{T}} := \sum_{k \in \mathcal{F}_{\mathsf{T}}} \mathbf{e}_{\mathsf{ID},k} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}$.

$\mathsf{Dec}(\mathsf{MPK}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}) \to \mathsf{M}$: Let $d \in [0, \kappa_{\mathsf{ID}}]$ be a number such that $\mathsf{ID}[d] \in \mathsf{KU}_{\mathsf{T}}$. Compute $c' = c_d - \mathbf{c}^\top \mathbf{d}_{\mathsf{ID},\mathsf{T}} \in \mathbb{Z}_q$ and output 0 if c' is closer to 0 than $\lfloor \frac{q}{2} \rfloor$. Otherwise, output 1.

Correctness. Thanks to the property of the KUNode algorithm, a non-revoked user can derive a valid decryption key $\mathbf{d}_{\mathsf{ID},\mathsf{T}} = \sum_{k \in \mathcal{F}_{\mathsf{T}}} \mathbf{e}_{\mathsf{ID},k} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}$. Observe that

$$\begin{aligned} c' &= c_d - \mathbf{c}^\top \mathbf{d}_{\mathsf{ID},\mathsf{T}} \\ &= \left(\sum_{k \in \mathcal{F}_{\mathsf{T}}} \mathbf{u}_{\mathsf{ID},k}^\top + \mathbf{u}_{\mathsf{ID}[d],\mathsf{T}}^\top \right) \mathbf{s} + x_d + \mathsf{M} \left\lfloor \frac{q}{2} \right\rfloor - (\mathbf{A}^\top \mathbf{s} + \mathbf{x})^\top \left(\sum_{k \in \mathcal{F}_{\mathsf{T}}} \mathbf{e}_{\mathsf{ID},k} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}} \right) \\ &= \mathsf{M} \left\lfloor \frac{q}{2} \right\rfloor + \underbrace{x_d - \mathbf{x}^\top \left(\sum_{k \in \mathcal{F}_{\mathsf{T}}} \mathbf{e}_{\mathsf{ID},k} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}} \right)}_{\text{error term}}. \end{aligned}$$

Here, we use the fact that

$$\mathbf{A}\mathbf{e}_{\mathsf{ID},k} = \mathbf{u}_{\mathsf{ID},k} \qquad \text{and} \qquad \mathbf{A}\mathbf{e}_{\mathsf{ID}[d],\mathsf{T}} = \mathbf{u}_{\mathsf{ID}[d],\mathsf{T}}$$

hold since $\mathbf{e}_{\mathsf{ID},k} \in \Lambda^{\perp}_{\mathbf{u}_{\mathsf{ID},k}}(\mathbf{A})$ and $\mathbf{e}_{\theta_j,\mathsf{T}} \in \Lambda^{\perp}_{\mathbf{u}_{\mathsf{ID}[d],\mathsf{T}}}(\mathbf{A})$ hold by construction. The decryption succeeds if the absolute value of the error term $x_d - \mathbf{x}^\top \left(\sum_{k \in \mathcal{F}_{\mathsf{T}}} \mathbf{e}_{\mathsf{ID},k} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}} \right)$ is smaller than $q/4$. By Lemma 5, the distributions of $\mathbf{e}_{\mathsf{ID},k}$ and $\mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}$ sampled by the $\mathsf{SamplePre}$ algorithm are $2^{-\Omega(n)}$-statistically close to $D_{\Lambda^{\perp}_{\mathbf{u}_{\mathsf{ID},k}}(\mathbf{A}),\sigma}$ and $D_{\Lambda^{\perp}_{\mathbf{u}_{\mathsf{ID}[d],\mathsf{T}}}(\mathbf{A}),\sigma}$, respectively. Therefore, by Lemma 2, $\|\mathbf{e}_{\mathsf{ID},k}\| \leq \sigma\sqrt{m}$ and $\|\mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}\| \leq \sigma\sqrt{m}$ hold. Similarly, by Lemma 2, $|x_d| \leq \alpha' q$ and $\|\mathbf{x}\| \leq \alpha' q\sqrt{m}$ also hold. Thus, the absolute value of the error term is bounded by

$$\begin{aligned} |x_d - \mathbf{x}^\top (\sum_{k \in \mathcal{F}_{\mathsf{T}}} \mathbf{e}_{\mathsf{ID},k} + \mathbf{e}_{\mathsf{ID}[d],\mathsf{T}})| &\leq |x_d| + \|\mathbf{x}\| \cdot (\sum_{k \in \mathcal{F}_{\mathsf{T}}} \|\mathbf{e}_{\mathsf{ID},k}\| + \|\mathbf{e}_{\mathsf{ID}[d],\mathsf{T}}\|) \\ &\leq (w+2)\alpha' q \sigma m. \end{aligned}$$

We will set the parameters as specified below so that the upper bound is less than $q/4$.

Parameter Selection. We set the parameters of the scheme to satisfy the following conditions:

- The absolute value of the error term is less than $q/4$ (i.e., $(w+2)\alpha' q\sigma m < q/4$).
- $\mathsf{TrapGen}$ works correctly (i.e., $m > 3n \log q$).
- $\mathsf{SamplePre}$ and $\mathsf{Sample}\mathbb{Z}(\sigma)$ works correctly (i.e., $\sigma > \|\mathbf{T}_{\mathbf{A}}\|_{\mathrm{GS}} \cdot \sqrt{\log(2m+4)/\pi} = O(\sqrt{n \log m \log q})$).

- σ is sufficiently large to apply Lemmas 1–3 (i.e., $\sigma > \sqrt{n + \log m}, 16\sqrt{\log 2m/\pi}$).
- ReRand works correctly (i.e., $\alpha'/2\alpha > \sqrt{n(\sigma^2 m + 1)}$).
- LWE is hard (i.e., $\alpha q \geq 2\sqrt{n}$).

To satisfy all the requirements, we can set the parameters as follows:

$$m = n^{1+\delta}, \qquad q = 10wn^{3.5+4\delta}, \qquad \sigma = n^{0.5+\delta},$$
$$\alpha' q = n^{2+2\delta}, \qquad \alpha q = 2\sqrt{n},$$

where $\delta > 0$ can be set an arbitrarily small constant.

Security. A proof of the security is almost the same as those of Theorems 1 and 2. The only difference is the analysis of Game-7 since the equation (5) is replaced by

$$[\mathbf{c}\|\bar{c}_0\|\cdots\|\bar{c}_{\kappa_{\mathsf{ID}}}] = [\mathbf{I}_m|\sum_{k\in\mathcal{F}_{\mathsf{T}}}\bar{\mathbf{e}}_{\mathsf{ID}^\star,k} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\sum_{k\in\mathcal{F}_{\mathsf{T}}}\bar{\mathbf{e}}_{\mathsf{ID}^\star,k} + \bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top\bar{\mathbf{c}} + \bar{\mathbf{x}}'.$$

Even when an adversary $\mathcal{A}$ obtains at most Q decryption keys $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}}$ for $\mathsf{T} \neq \mathsf{T}^\star$, CFF ensure that there is at least one index $k^\star \in [t]$, where $\bar{\mathbf{e}}_{\mathsf{ID}^\star,k^\star}$ is not revealed to $\mathcal{A}$. Thus, as $[\mathbf{I}_m|\bar{\mathbf{e}}_{\mathsf{ID}^\star}|\bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star[j-1],\mathsf{T}^\star}|\bar{\mathbf{e}}_{\mathsf{ID}^\star[j+1],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top\bar{\mathbf{c}}$ is distributed uniformly at random in $\mathbb{Z}^{m+\kappa_{\mathsf{ID}}+1}$ in the proofs of Theorems 1 and 2, $[\mathbf{I}_m|\sum_{k\in\mathcal{F}_{\mathsf{T}}}\bar{\mathbf{e}}_{\mathsf{ID}^\star,k}|\bar{\mathbf{e}}_{\mathsf{ID}^\star[0],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star[j-1],\mathsf{T}^\star}|\bar{\mathbf{e}}_{\mathsf{ID}^\star[j+1],\mathsf{T}^\star}|\cdots|\bar{\mathbf{e}}_{\mathsf{ID}^\star[\kappa_{\mathsf{ID}}],\mathsf{T}^\star}]^\top\bar{\mathbf{c}}$ is distributed uniformly at random in $\mathbb{Z}^{m+\kappa_{\mathsf{ID}}+1}$.

References

[ABB10a] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer, 2010.

[ABB10b] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference*, volume 6223 of *Lecture Notes in Computer Science*, pages 98–115. Springer, 2010.

[Ajt99] Miklós Ajtai. Generating hard instances of the short basis problem. In Jirí Wiedermann, Peter van Emde Boas, and Mogens Nielsen, editors, *Automata, Languages and Programming, 26th International Colloquium, ICALP'99*, volume 1644 of *Lecture Notes in Computer Science*, pages 1–9. Springer, 1999.

[AKGL07] N. Asokan, Kari Kostiainen, Philip Ginzboorg, and Cheng Luo. Applicability of identity-based cryptography for disruption-tolerant networking. *MobiOpp'07: Proceedings of the First International MobiSys Workshop on Mobile Opportunistic Networking*, 01 2007.

[AP11] Joël Alwen and Chris Peikert. Generating shorter bases for hard random lattices. *Theory Comput. Syst.*, 48(3):535–553, 2011.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[BGK08] Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar. Identity-based encryption with efficient revocation. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008*, pages 417–426. ACM, 2008.

[Boy10] Xavier Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 499–517. Springer, 2010.

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 719–737. Springer, 2012.

[BRTM09] Kevin R.B. Butler, Sunam Ryu, Patrick Traynor, and Patrick Drew McDaniel. Leveraging identity-based cryptography for node id assignment in structured p2p systems. *IEEE Transactions on Parallel and Distributed Systems*, 20(12):1803–1815, December 2009.

[CHKP12] 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.

[CLL+12] 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 - 17th Australasian Conference, ACISP 2012*, volume 7372 of *Lecture Notes in Computer Science*, pages 390–403. Springer, 2012.

[ddAL08] E. da Silva, A. L. dos Santos, L. C. P. Albini, and M. N. Lima. Identity-based key management in mobile ad hoc networks: techniques and applications. *IEEE Wireless Communications*, 15(5):46–52, 2008.

[EFF85] P. Erdös, P. Frankl, and Z. Füredi. Families of finite sets in which no set is covered by the union of r others. *Israel Journal of Mathematics*, 51(1):79–89, 1985.

[ETW20] Keita Emura, Atsushi Takayasu, and Yohei Watanabe. Adaptively secure revocable hierarchical IBE from k-linear assumption. *IACR Cryptol. ePrint Arch.*, 2020:886, 2020.

[ETW21] Keita Emura, Atsushi Takayasu, and Yohei Watanabe. Generic constructions of revocable hierarchical identity-based encryption. *IACR Cryptol. ePrint Arch.*, 2021:515, 2021.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, 1986.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 197–206. ACM, 2008.

[GW19] Aijun Ge and Puwen Wei. Identity-based broadcast encryption with efficient revocation. In Dongdai Lin and Kazue Sako, editors, *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Proceedings, Part I*, volume 11442 of *Lecture Notes in Computer Science*, pages 405–435. Springer, 2019.

[HLCL18] Ziyuan Hu, Shengli Liu, Kefei Chen, and Joseph K. Liu. Revocable identity-based encryption from the computational Diffie-Hellman problem. In Willy Susilo and Guomin Yang, editors, *Information Security and Privacy - 23rd Australasian Conference, ACISP 2018, Proceedings*, volume 10946 of *Lecture Notes in Computer Science*, pages 265–283. Springer, 2018.

[Kat17] Shuichi Katsumata. On the untapped potential of encoding predicates by arithmetic circuits and their applications. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Proceedings, Part III*, volume 10626 of *Lecture Notes in Computer Science*, pages 95–125. Springer, 2017.

[KBL13] N. Kaaniche, A. Boudguiga, and M. Laurent. Id based cryptography for cloud data storage. In *2013 IEEE Sixth International Conference on Cloud Computing*, pages 375–382, 2013.

[KMT19] 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 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Proceedings, Part II*, volume 11443 of *Lecture Notes in Computer Science*, pages 441–471. Springer, 2019.

[KRS99] Ravi Kumar, Sridhar Rajagopalan, and Amit Sahai. Coding constructions for blacklisting problems without computational assumptions. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference*, volume 1666 of *Lecture Notes in Computer Science*, pages 609–623. Springer, 1999.

[KY16] Shuichi Katsumata and Shota Yamada. Partitioning via non-linear polynomial functions: More compact ibes from ideal lattices and bilinear maps. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 682–712, 2016.

[KYY18] Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa. Tighter security proofs for GPV-IBE in the quantum random oracle model. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part II*, volume 11273 of *Lecture Notes in Computer Science*, pages 253–282. Springer, 2018.

[Lee19] Kwangsu Lee. A generic construction for revocable identity-based encryption with subset difference methods. *IACR Cryptology ePrint Archive*, 2019:798, 2019.

[LK21] Kwangsu Lee and Joon Sik Kim. A generic approach to build revocable hierarchical identity-based encryption. *IACR Cryptology ePrint Archive*, 2021:502, 2021.

[LV09] Benoît Libert and Damien Vergnaud. Adaptive-ID secure revocable identity-based encryption. In Marc Fischlin, editor, *Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009. Proceedings*, volume 5473 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2009.

[ML19] Xuecheng Ma and Dongdai Lin. Generic constructions of revocable identity-based encryption. In Zhe Liu and Moti Yung, editors, *Information Security and Cryptology - 15th International Conference, Inscrypt 2019, Revised Selected Papers*, volume 12020 of *Lecture Notes in Computer Science*, pages 381–396. Springer, 2019.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer, 2012.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007.

[MSW15] Tobias Markmann, Thomas C. Schmidt, and Matthias Wählisch. Federated end-to-end authentication for the constrained internet of things using ibc and ecc. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, pages 603–604. Association for Computing Machinery, 2015.

[NNL01] Dalit Naor, Moni Naor, and Jeffery Lotspiech. Revocation and tracing schemes for stateless receivers. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference. Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 41–62. Springer, 2001.

[Pei07] Chris Peikert. Limits on the hardness of lattice problems in ell _p norms. In *22nd Annual IEEE Conference on Computational Complexity (CCC 2007)*, pages 333–346. IEEE Computer Society, 2007.

[PR06] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, Proceedings*, volume 3876 of *Lecture Notes in Computer Science*, pages 145–166. Springer, 2006.

[PSK18] D. N. Purnamasari, A. Sudarsono, and P. Kristalina. Secure data sharing scheme using identity-based encryption for e-health record. In *2018 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)*, pages 60–65, 2018.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 84–93. ACM, 2005.

[San16] S. Sankaran. Lightweight security framework for iots using identity based cryptography. In *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pages 880–886, 2016.

[SE13] 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 - 16th International Conference on Practice and Theory in Public-Key Cryptography. Proceedings*, volume 7778 of *Lecture Notes in Computer Science*, pages 216–234. Springer, 2013.

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society, 1994.

[SK05] A. Seth and S. Keshav. Practical security for disconnected nodes. In *1st IEEE ICNP Workshop on Secure Network Protocols, 2005. (NPSec).*, pages 31–36, 2005.

[SXY18] Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 520–551. Springer, 2018.

[Tak21] Atsushi Takayasu. More efficient adaptively secure revocable hierarchical identity-based encryption with compact ciphertexts: Achieving shorter keys and tighter reductions. *IACR Cryptol. ePrint Arch.*, 2021:539, 2021.

[TW17] 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 - 22nd Australasian Conference, ACISP 2017, Proceedings, Part I*, volume 10342 of *Lecture Notes in Computer Science*, pages 184–204. Springer, 2017.

[TW21] Atsushi Takayasu and Yohei Watanabe. Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more. *Theor. Comput. Sci.*, 849:64–98, 2021.

[TWZL08] Chiu Chiang Tan, Haodong Wang, Sheng Zhong, and Qun Li. Body sensor network security: an identity-based cryptography approach. In Virgil D. Gligor, Jean-Pierre

Hubaux, and Radha Poovendran, editors, *Proceedings of the First ACM Conference on Wireless Network Security, WISEC 2008,*, pages 148–153. ACM, 2008.

[TWZL09] Chiu Chiang Tan, Haodong Wang, Sheng Zhong, and Qun Li. Ibe-lite: A lightweight identity-based cryptography for body sensor networks. *IEEE Trans. Inf. Technol. Biomed.*, 13(6):926–932, 2009.

[WES17] 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 - The Cryptographers' Track at the RSA Conference 2017. Proceedings*, volume 10159 of *Lecture Notes in Computer Science*, pages 432–449. Springer, 2017.

[WZH+19] Shixiong Wang, Juanyang Zhang, Jingnan He, Huaxiong Wang, and Chao Li. Simplified revocable hierarchical identity-based encryption from lattices. In Yi Mu, Robert H. Deng, and Xinyi Huang, editors, *Cryptology and Network Security - 18th International Conference, CANS 2019, Proceedings*, volume 11829 of *Lecture Notes in Computer Science*, pages 99–119. Springer, 2019.

[Yam16] Shota Yamada. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9666 of *Lecture Notes in Computer Science*, pages 32–62. Springer, 2016.

[Yam17] Shota Yamada. Asymptotically compact adaptively secure lattice ibes and verifiable random functions via generalized partitioning techniques. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference*, volume 10403 of *Lecture Notes in Computer Science*, pages 161–193. Springer, 2017.

[YZ20] Takashi Yamakawa and Mark Zhandry. Classical vs quantum random oracles. *IACR Cryptol. ePrint Arch.*, 2020:1270, 2020.

[ZC11] Sheng Zhong and Tingting Chen. An efficient identity-based protocol for private matching. *Int. J. Communication Systems*, 24(4):543–552, 2011.

[Zha12a] Mark Zhandry. How to construct quantum random functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012*, pages 679–687. IEEE Computer Society, 2012.

[Zha12b] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 758–775. Springer, 2012.