Efficient Revocable Identity-Based Encryption from Middle-Product LWE

Takumi Nishimura[1] and Atsushi Takayasu[1,2]

[1] The University of Tokyo, Japan
[2] National Institute of Advanced Industrial Science and Technology, Japan
{takunishi23,takayasu-a}@g.ecc.u-tokyo.ac.jp

Abstract. The *Middle-Product Learning with Errors (MPLWE) assumption* is a variant of the Learning with Errors (LWE) assumption. The MPLWE assumption reduces the key size of corresponding LWE-based schemes by setting keys as sets of polynomials. Moreover, MPLWE has more robust security than other LWE variants such as Ring-LWE and Module-LWE. Lombardi et al. proposed an identity-based encryption (IBE) scheme (LVV-IBE) based on the MPLWE assumption in the random oracle model (ROM) by following Gentry et al.'s IBE scheme (GPV-IBE) based on LWE. Due to the benefit of MPLWE, LVV-IBE has a shorter master public key and a secret key than GPV-IBE without changing the size of a ciphertext. However, Lombardi et al.'s proof is not tight in the ROM, while Katsumata et al. proved that GPV-IBE achieves *tight* adaptive *anonymity* in the *quantum ROM (QROM)*. Revocable IBE (RIBE) is a variant of IBE supporting a key revocation mechanism to remove malicious users from the system. Takayasu proposed the most efficient RIBE scheme (Takayasu-RIBE) based on LWE achieving tight adaptive anonymity in the QROM. Although a concrete RIBE scheme based on MPLWE has not been proposed, we can construct a scheme (LVV-based RIBE) by applying Ma and Lin's generic transformation to LVV-IBE. Due to the benefit of MPLWE, LVV-based RIBE has an asymptotically shorter master public key and a shorter secret key than Takayasu-RIBE although the former has a larger ciphertext than the latter. Moreover, the security proof is not tight and anonymous in the ROM due to security proofs of Ma-Lin and Lombardi et al. In this paper, we propose a concrete RIBE scheme based on MPLWE. Compared with the above RIBE schemes, the proposed RIBE scheme is the most asymptotically efficient since the sizes of a master public key and a secret key (resp. ciphertext) of the proposed scheme are the same as those of LVV-based RIBE scheme (resp. Takayasu-RIBE). Moreover, we prove the tight adaptive anonymity of the proposed RIBE scheme in the QROM. For this purpose, we also prove the tight adaptive anonymity of LVV-IBE in the QROM.

Keywords: Identity-based Encryption · Revocable Identity-based Encryption · Middle-Product Learning with Errors · Tight Security · Anonymity · Quantum Random Oracle Model.

1 Introduction

1.1 Background

Lattice-based cryptography based on the Learning with Errors (LWE) assumption [26] has been actively studied because they are resilient even against quantum attacks. Moreover, we can construct cryptography schemes with advanced functionality based on the LWE assumption such as identity-based encryption (IBE). Among several adaptively secure IBE schemes based on the LWE assumption [1,2,3,7,8,13,34,35], Gentry et al.'s IBE scheme (GPV-IBE) [13] is the most efficient. Specifically, the sizes of a master public key, a secret key and a ciphertext of an n-bit plaintext are $O(n^2 \log^2 n)$, $O(n^2 \log^2 n)$, and $O(n \log^2 n)$, respectively for the security parameter n. Although Gentry et al.'s original proof is not tight in the random oracle model (ROM), Katsumata et al. [17] slightly modified the scheme and proved the *tight* adaptive *anonymity* in the *quantum ROM (QROM)* [6]. Since a proof in the ROM may not ensure post-quantum security [36], Katsumata et al.'s proof ensures the post-quantum security of GPV-IBE under better parameters.

Rosca et al. [27] proposed the *Middle-Product LWE (MPLWE) assumption* as a variant of LWE. The MPLWE assumption can reduce the key size of corresponding LWE-based schemes by replacing matrices and vectors in LWE-based schemes with sets of polynomials. While other LWE variants over a specific ring such as Ring-LWE [23] and Module-LWE [19] also reduce the key size, the MPLWE-based schemes have more robust security guarantees than these variants because the MPLWE problem is as hard as the polynomial LWE (PLWE) problem [29], which is a variant of the LWE over broader class of rings. So far, various MPLWE-based schemes have been proposed by modifying LWE-based schemes such as public key encryption [22,27], digital signatures [4,14,21], ring signatures [10,21], IBE [12,22], hierarchical IBE [20], and inner product encryption [37,38]. Among known MPLWE-based IBE schemes [12,22], Lombardi et al.'s scheme (LVV-IBE) [22] which is a MPLWE variant of GPV-IBE is the most efficient. Due to the benefit of MPLWE, LVV-IBE has a shorter master public key and a secret key of the size $O(n \log^2 n)$ than GPV-IBE without changing the size of a ciphertext $O(n \log^2 n)$. Therefore, LVV-IBE is asymptotically more efficient than GPV-IBE. LVV-IBE is the only known adaptively secure IBE scheme based on MPLWE.[3] Although Lombardi et al. [22] did not provide a concrete security proof, they claimed that we can apply Gentry et al.'s proof technique of GPV-IBE [13] to LVV-IBE; thus, a proof is not tight in the ROM. In other words, it is not known whether we can prove tight adaptive anonymity of LVV-IBE in the QROM as GPV-IBE [17].

Since IBE cannot revoke malicious users efficiently in a generic way, Boldyreva et al. [5] proposed a notion of revocable IBE (RIBE). Since Ma and Lin [24] proposed a generic transformation from IBE to RIBE that preserves the

[3] Although Fan et al. [12] tried to construct an adaptively secure IBE scheme based on MPLWE, the security definition is weaker than the standard adaptive security since the number of adversary's secret key queries is a-priori bounded.

adaptive security, we can obtain LWE-based and MPLWE-based RIBE schemes (GPV-based RIBE and LVV-based RIBE) by applying the transformation to GPV-IBE [13] and LVV-IBE [22], respectively. Since Ma-Lin's transformation preserves the sizes of a master public key and a secret key, the sizes of GPV-based RIBE (resp. LVV-based RIBE) are both $O(n^2 \log^2 n)$ (resp. $O(n \log^2 n)$). However, since Ma-Lin's transformation suffers from large ciphertexts, the sizes of GPV-based RIBE and LVV-based RIBE become $O(L_{\mathsf{ID}} n \log^2 n)$. Since Ma-Lin's transformation does not also preserve the tight security and anonymity, the security of GPV-based RIBE is not tight or anonymous although GPV-IBE satisfies the tight anonymity. Among several concrete LWE-based RIBE schemes [9,15,30,31,32,33], Takayasu's scheme (Takayasu-RIBE) [30] that is a modification of GPV-based RIBE is the most efficient and resolves the above issue of GPV-based RIBE. In particular, the sizes of a master public key, a secret key, and a ciphertext are $O(n^2 \log^2 n)$, $O(n^2 \log^2 n)$, and $O(L_{\mathsf{ID}} n \log n)$, respectively; thus, Takayasu-RIBE is asymptotically more efficient than GPV-based RIBE. Moreover, Takayasu RIBE satisfies the tight adaptive anonymity in the QROM. However, Takayasu RIBE is not strictly asymptotically more efficient than LVV-based RIBE since the sizes of a master public key and a secret key of the former $O(n^2 \log^2 n)$ are larger than those of the latter $O(n \log^2 n)$. As MPLWE-based LVV-IBE [22] improves the efficiency of LWE-based GPV-IBE [13], MPLWE may enable us to construct an RIBE scheme that is asymptotically more efficient than Takayasu-RIBE [30]. Then, it is desirable to prove the tight adaptive anonymity of such an MPLWE-based RIBE scheme in the QROM.

1.2 Our Contribution

In this paper, we propose an RIBE scheme based on MPLWE. We modify LVV-based RIBE and obtain the proposed RIBE scheme by following the way Takayasu [30] modified GPV-based RIBE and obtained Takayasu-RIBE. We reduce the size of a ciphertext of LVV-based RIBE from $O(L_{\mathsf{ID}} n \log^2 n)$ to $O(L_{\mathsf{ID}} n \log n)$ as Takayasu reduced the size of a ciphertext of GPV-based RIBE from $O(L_{\mathsf{ID}} n \log^2 n)$ to $O(L_{\mathsf{ID}} n \log n)$. Similarly, the proposed scheme preserves the sizes of a master public key and a secret key $O(n \log^2 n)$ of LVV-based RIBE as Takayasu-RIBE preserves the sizes of a master public key and a secret key $O(n^2 \log^2 n)$ of GPV-based RIBE. Thus, the proposed scheme achieves the shortest master public key, the secret key, and the ciphertext, simultaneously compared with known LWE-based and MPLWE-based RIBE schemes. The top of Table 1 compares the efficiency among GPV-based RIBE, LVV-based RIBE, Takayasu-RIBE, and the proposed scheme. Although we have not explained the detailed syntax of RIBE, there are also key updates and decryption keys. We do not compare the efficiency of key updates and decryption keys in Table 1 since they are the same among all four schemes. The bottom of Table 1 compares the security among GPV-based RIBE, LVV-based RIBE, Takayasu-RIBE, and the proposed scheme.

Table 1. Comparison among adaptively secure RIBE schemes based on LWE and MPLWE in the (Q)ROM

Scheme	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{ct}\rvert$	$\lvert\mathsf{sk}_{\mathsf{ID}}\rvert$
GPV-based RIBE [13]+ [24]	$O(n^2 \log^2 n)$	$O(L_{\mathsf{ID}} n \log^2 n)$	$O(n^2 \log^2 n)$
LVV-based RIBE [22]+ [24]	$O(n \log^2 n)$	$O(L_{\mathsf{ID}} n \log^2 n)$	$O(n \log^2 n)$
Takayasu-RIBE [30]	$O(n^2 \log^2 n)$	$O(L_{\mathsf{ID}} n \log n)$	$O(n^2 \log^2 n)$
Our Scheme (Section 5)	$O(n \log^2 n)$	$O(L_{\mathsf{ID}} n \log n)$	$O(n \log^2 n)$

Scheme	Anonymity	Reduction loss	Model	Assumption
GPV-based RIBE [13]+ [24]		$O(L_{\mathsf{ID}})$	QROM	LWE
LVV-based RIBE [22]+ [24]		$O(Q_{\mathsf{H}} L_{\mathsf{ID}})$	ROM	MPLWE
Takayasu-RIBE [30]	✓	$O(1)$	QROM	LWE
Our Scheme (Section 5)	✓	$O(1)$	QROM	MPLWE

GPV-based RIBE (resp. LVV-based RIBE) denotes a resulting RIBE scheme by applying Ma-Lin's transformation [24] to GPV-IBE [13] (resp. LVV-IBE [22]). n denotes the security parameter. $\lvert\mathsf{mpk}\rvert$ and $\lvert\mathsf{ct}\rvert$ denote the size of a master public key and a ciphertext for an n-bit plaintext, respectively. $L_{\mathsf{ID}} = O(n)$ denotes the length of an identity. Q_{H} denotes the number of adversary's random oracle queries.

We try to prove the tight adaptive anonymity of the proposed RIBE scheme in the QROM as Takayasu-RIBE [30]. Although a naive approach to complete the task is combining security proofs of LVV-IBE and Takayasu-RIBE, it is insufficient for our purpose since Lombardi et al.'s proof of LVV-IBE [22] is not tight in the ROM. Therefore, we first prove the tight adaptive anonymity of LVV-IBE in the QROM. To this end, we slightly modify LVV-IBE and prove the tight adaptive anonymity in the QROM by following Katsumata et al.'s approach [17] for GPV-IBE [13]. As a result, we successfully prove that LVV-IBE ensures the post-quantum security. Table 2 compares the original LVV-IBE [22] and our modification. We achieve the tight adaptive anonymity in the QROM without sacrificing the efficiency of LVV-IBE [22]. Then, we prove the tight adaptive anonymity of the proposed RIBE scheme in the QROM by combining our security proof of modified LVV-IBE and Takayasu's proof [30].

1.3 Technical Overview

We explain an overview of our proposed RIBE scheme. We first review GPV-IBE [13] and show how to obtain Takayasu-RIBE [30] by modifying GPV-IBE. Then, we review LVV-IBE [22] and show how to obtain the proposed RIBE scheme by modifying LVV-IBE. We note that all the schemes encrypt an n-bit plaintext $\mathsf{m} \in \{0,1\}^n$.

Table 2. Comparison among adaptively secure IBE schemes based on MPLWE in the (Q)ROM

Scheme	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{ct}\rvert$	Reduction loss	Model
LVV-IBE [22]	$O(n\log^2 n)$	$O(n\log^2 n)$	$O(Q_{\mathsf{H}})$	ROM
Our Scheme	$O(n\log^2 n)$	$O(n\log^2 n)$	$O(1)$	QROM

n denotes the security parameter. $\lvert\mathsf{mpk}\rvert$ and $\lvert\mathsf{ct}\rvert$ denote the size of a master public key and a ciphertext for an n-bit plaintext, respectively. Q_{H} denotes the number of adversary's random oracle queries.

GPV-IBE. Let H denote a hash function that maps an identity ID to a matrix $\mathbf{U}_{\mathsf{ID}} \in \mathbb{Z}_q^{n\times n}$. A master public key and a master secret key are a matrix $\mathsf{GPV.mpk} = \mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and its short trapdoor basis $\mathsf{GPV.msk} = \mathbf{T}_{\mathbf{A}}$, respectively. The short trapdoor basis $\mathbf{T}_{\mathbf{A}}$ can sample a secret key for ID as a short matrix $\mathsf{GPV.sk}_{\mathsf{ID}} = \mathbf{R}_{\mathsf{ID}} \in \mathbb{Z}_q^{m\times n}$ such that $\mathbf{A}\mathbf{R}_{\mathsf{ID}} = \mathbf{U}_{\mathsf{ID}} \mod q$. A ciphertext for ID and a plaintext $\mathsf{m} \in \{0,1\}^n$ is $\mathsf{GPV.ct}_{\mathsf{ID}} = (\mathbf{b}, \mathbf{b}') \in \mathbb{Z}_q^m \times \mathbb{Z}_q^n$;

$$\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathsf{noise}, \qquad \mathbf{b}' = \mathsf{m} \cdot \left\lfloor \frac{q}{2} \right\rfloor + \mathbf{U}_{\mathsf{ID}}^\top \mathbf{s} + \mathsf{noise},$$

where $\mathbf{s} \in \mathbb{Z}_q^n$ is a uniformly random vector and both noise's are short vectors with compatible dimensions sampled from the discrete Gaussian distribution. The second element $\mathbf{b}'$ embeds a plaintext m masked by $\mathbf{U}_{\mathsf{ID}}^\top \mathbf{s} + \mathsf{noise}$, while the first element $\mathbf{b}$ is multiplied by a secret key $\mathbf{R}_{\mathsf{ID}}$ and becomes $\mathbf{U}_{\mathsf{ID}}^\top \mathbf{s} + \mathsf{noise}$ to cancel the mask of $\mathbf{b}'$. Specifically, the decryption algorithm computes

$$\begin{aligned}
\mathbf{b}' - \mathbf{R}_{\mathsf{ID}}^\top \mathbf{b} &= \mathsf{m} \cdot \left\lfloor \frac{q}{2} \right\rfloor + \mathbf{U}_{\mathsf{ID}}^\top \mathbf{s} + \mathsf{noise} - \left([\mathbf{A}\mathbf{R}_{\mathsf{ID}}]^\top \mathbf{s} + \mathbf{R}_{\mathsf{ID}}^\top \cdot \mathsf{noise} \right) \mod q \\
&= \mathsf{m} \cdot \left\lfloor \frac{q}{2} \right\rfloor + \cancel{\mathbf{U}_{\mathsf{ID}}^\top \mathbf{s}} + \mathsf{noise} - \cancel{\mathbf{U}_{\mathsf{ID}}^\top \mathbf{s}} + \mathsf{noise} \mod q \\
&= \mathsf{m} \cdot \left\lfloor \frac{q}{2} \right\rfloor + \mathsf{noise} \mod q
\end{aligned}$$

by using the fact that $\mathbf{R}_{\mathsf{ID}}$ is a short matrix such that $\mathbf{A}\mathbf{R}_{\mathsf{ID}} = \mathbf{U}_{\mathsf{ID}} \mod q$. Since noise is small, we can recover a plaintext $\mathsf{m} \in \{0,1\}^n$ by comparing whether each coordinate of $\mathbf{b}' - \mathbf{R}_{\mathsf{ID}}^\top \mathbf{b}$ is close to 0 or $q/2$.

In Katsumata et al.'s security proof [17], the LWE assumption ensures that $\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathsf{noise}$ is indistinguishable from uniform. Since an IBE adversary cannot receive $\mathsf{GPV.sk}_{\mathsf{ID}^\star} = \mathbf{R}_{\mathsf{ID}^\star}$ for the target identity $\mathsf{ID}^\star$, the entropy of $\mathbf{R}_{\mathsf{ID}^\star}$ ensures that $\mathbf{U}_{\mathsf{ID}^\star}^\top \mathbf{s} + \mathsf{noise} \approx \mathbf{R}_{\mathsf{ID}^\star}^\top \mathbf{b}$ is indistinguishable from uniform and completely masks a plaintext.

Takayasu-RIBE. Takayasu-RIBE is a revocable variant of GPV-IBE. Let H denote a hash function that maps a binary string to a matrix in $\mathbb{Z}_q^{n\times n}$. We use the hash function to compute $\mathsf{H}(\mathsf{ID}) = \mathbf{U}_{\mathsf{ID}}$ and $\mathsf{H}(\theta, \mathsf{T}) = \mathbf{U}_{\mathsf{T},\theta}$. Let RL_{T} be a

revocation list at T, a set of identities that are revoked at T. Let $\mathcal{I}_{\mathsf{ID}}$ (resp. $\mathcal{I}_{\mathsf{T}}$) denote a set of binary strings associated with ID (resp. RL_{T}). Although we omit the detail, Naor et al.'s KUNode algorithm [25] ensures that there is a unique binary string $\tilde{\theta} \in \mathcal{I}_{\mathsf{ID}} \cap \mathcal{I}_{\mathsf{T}}$ if $\mathsf{ID} \notin \mathsf{RL}_{\mathsf{T}}$ and $\mathcal{I}_{\mathsf{ID}} \cap \mathcal{I}_{\mathsf{T}} = \emptyset$ holds if $\mathsf{ID} \in \mathsf{RL}_{\mathsf{T}}$. See Section 5 for the details of the KUNode algorithm. A master public/secret key pair $(\mathsf{Tak.mpk}, \mathsf{Tak.msk}) = (\mathbf{A}, \mathbf{T}_{\mathbf{A}})$ and a secret key $\mathsf{Tak.sk}_{\mathsf{ID}} = \mathbf{R}_{\mathsf{ID}}$ are the same as GPV-IBE. A ciphertext for $(\mathsf{ID}, \mathsf{T})$ and a plaintext $\mathsf{m} \in \{0,1\}^n$ is $\mathsf{Tak.ct}_{\mathsf{ID},\mathsf{T}} = (\mathbf{b}, \{\mathbf{b}'_\theta\}_{\theta \in \mathcal{I}_{\mathsf{ID}}}) \in \mathbb{Z}_q^m \times (\mathbb{Z}_q^n)^{|\mathcal{I}_{\mathsf{ID}}|}$;

$$\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathsf{noise}, \qquad \mathbf{b}'_\theta = \mathsf{m} \cdot \left\lfloor \frac{q}{2} \right\rfloor + [\mathbf{U}_{\mathsf{ID}} + \mathbf{U}_{\mathsf{T},\theta}]^\top \mathbf{s} + \mathsf{noise},$$

where $\mathbf{s} \in \mathbb{Z}_q^n$ is a uniformly random vector and all noise's are short vectors with compatible dimensions sampled from the discrete Gaussian distribution. All the latter elements $\mathbf{b}'_\theta$ embed a plaintext m masked by $[\mathbf{U}_{\mathsf{ID}} + \mathbf{U}_{\mathsf{T},\theta}]^\top \mathbf{s} + \mathsf{noise}$. Unlike the case of GPV-IBE, a secret key $\mathbf{R}_{\mathsf{ID}}$ itself cannot decrypt a ciphertext $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$ since the first ciphertext element $\mathbf{b}$ multiplied by $\mathbf{R}_{\mathsf{ID}}$ becomes $\mathbf{U}_{\mathsf{ID}}^\top \mathbf{s} + \mathsf{noise}$ that cannot cancel the mask $\mathbf{U}_{\mathsf{T},\theta}^\top \mathbf{s} + \mathsf{noise}$ of $\mathbf{b}'_\theta$ for all $\theta \in \mathcal{I}_{\mathsf{ID}}$. To decrypt a ciphertext $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$, we have to use a key update $\mathsf{ku}_{\mathsf{T}} = \{\theta, \mathbf{R}_{\mathsf{T},\theta}\}_{\theta \in \mathcal{I}_{\mathsf{T}}}$ such that $\mathbf{A}\mathbf{R}_{\mathsf{T},\theta} = \mathbf{U}_{\mathsf{T},\theta} \bmod q$. If ID is not revoked at T, the property of the KUNode algorithm [25] ensures that there is a binary string $\tilde{\theta} \in \mathcal{I}_{\mathsf{ID}} \cap \mathcal{I}_{\mathsf{T}}$. Thus, a non-revoked ID can cancel $\mathbf{R}_{\mathsf{T},\theta}^\top c_0 \approx \mathbf{U}_{\mathsf{T},\theta}^\top \mathbf{s} + \mathsf{noise}$ and decrypt a ciphertext $\mathsf{Tak.ct}_{\mathsf{ID},\mathsf{T}}$ from $(\mathbf{b}, \mathbf{b}'_{\tilde{\theta}})$.

In a security proof, the LWE assumption ensures that $\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathsf{noise}$ is indistinguishable from uniform. Let $\mathsf{ID}^\star$ (resp. $\mathsf{T}^\star$) denote the target identity (resp. target time period). Unlike the case of IBE, an RIBE adversary may receive $\mathsf{Tak.sk}_{\mathsf{ID}^\star} = \mathbf{R}_{\mathsf{ID}^\star}$. If the adversary receives $\mathbf{R}_{\mathsf{ID}^\star}$, the security definition of RIBE ensures that $\mathsf{ID}^\star$ is revoked by $\mathsf{T}^\star$ to prevent trivial attacks. Therefore, the property of the KUNode algorithm [25] ensures that $\mathsf{Tak.ku}_{\mathsf{T}^\star} = \{\mathbf{R}_{\theta,\mathsf{T}^\star}\}_{\theta \in \mathcal{I}_{\mathsf{T}^\star}}$ which the adversary receives satisfies $\mathsf{Tak.ku}_{\mathsf{T}^\star} \cap (\mathcal{I}_{\mathsf{ID}^\star} \cap \mathcal{I}_{\mathsf{T}^\star}) = \emptyset$. As a result, each entropy of $\mathbf{R}_{\theta,\mathsf{T}^\star}$ for $\theta \in \mathcal{I}_{\mathsf{ID}^\star}$ ensures that $\mathbf{U}_{\theta,\mathsf{T}^\star}^\top \mathbf{s} + \mathsf{noise} \approx \mathbf{R}_{\theta,\mathsf{T}^\star}^\top \mathbf{b}$ is indistinguishable from uniform and completely masks a plaintext as the case of IBE. If the adversary does not receive $\mathsf{Tak.sk}_{\mathsf{ID}^\star} = \mathbf{R}_{\mathsf{ID}^\star}$, it can receive $\mathsf{Tak.ku}_{\mathsf{T}^\star} = \{\mathbf{R}_{\theta,\mathsf{T}^\star}\}_{\theta \in \mathcal{I}_{\mathsf{T}^\star}}$ that contains $\mathbf{R}_{\tilde{\theta},\mathsf{T}^\star}$ for $\tilde{\theta} \in \mathcal{I}_{\mathsf{ID}^\star} \cap \mathcal{I}_{\mathsf{T}^\star}$. Since the property of the KUNode algorithm [25] ensures that $\tilde{\theta}$ is a unique binary string in $\mathcal{I}_{\mathsf{ID}^\star} \cap \mathcal{I}_{\mathsf{T}^\star}$, each entropy of $\mathbf{R}_{\theta,\mathsf{T}^\star}$ for $\theta \in \mathcal{I}_{\mathsf{ID}^\star} \setminus \{\tilde{\theta}\}$ ensures that $\mathbf{U}_{\theta,\mathsf{T}^\star}^\top \mathbf{s} + \mathsf{noise} \approx \mathbf{R}_{\theta,\mathsf{T}^\star}^\top \mathbf{b}$ is indistinguishable from uniform and completely masks a plaintext of $\mathbf{b}'_\theta$. On the other hand, the entropy of $\mathbf{R}_{\mathsf{ID}^\star}$ ensures that $\mathbf{U}_{\mathsf{ID}^\star}^\top \mathbf{s} + \mathsf{noise} \approx \mathbf{R}_{\mathsf{ID}^\star}^\top \mathbf{b}$ is indistinguishable from uniform and completely masks a plaintext of $\mathbf{b}'_{\tilde{\theta}}$.

LVV-IBE. LVV-IBE is an MPLWE variant of GPV-IBE. For simplicity, we ignore degrees of polynomials to explain overviews of LVV-IBE and the proposed RIBE scheme. Hereafter, we assume all polynomials have compatible degrees. LVV-IBE and the proposed RIBE scheme use a middle product between two polynomials $a, b \in R[X]$ denoted by $a \odot b$. The result $a \odot b$ is a polynomial whose coefficients are the same as the middle degrees of $a \cdot b$, where "$\cdot$" denotes the standard polynomial multiplication over $R[X]$. Let H denote a hash function that maps an identity ID to a polynomial $u_{\mathsf{ID}} \in R[X]$. A master public key and

a master secret key are a set of polynomials $\mathsf{LVV.mpk} = (a_i)_{i=1}^{t+\gamma\tau} \in R[X]^{t+\gamma\tau}$ and a set of small trapdoor polynomials $\mathsf{LVV.msk} = (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}$, respectively. The set of small trapdoor polynomials $(w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}$ can sample a secret key for ID as a set of small polynomials $\mathsf{LVV.sk_{ID}} = (r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau} \in R[X]^{t+\gamma\tau}$ such that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i} = u_{\mathsf{ID}}$. A ciphertext for ID and a plaintext $\mathsf{m} \in \{0,1\}^n$ is $\mathsf{LVV.ct_{ID}} = ((b_i)_{i=1}^{t+\gamma\tau}, b') \in R[X]^{t+\gamma\tau} \times R[X]$;

$$b_i = a_i \odot s + 2 \cdot \mathsf{noise}, \qquad b' = \mathsf{m} + u_{\mathsf{ID}} \odot s + 2 \cdot \mathsf{noise},$$

where each coefficient of $s \in R[X]$ follows the uniform distribution and that of noise follows the discrete Gaussian distribution. The latter element b' embeds a plaintext m masked by $u_{\mathsf{ID}} \odot s + 2 \cdot \mathsf{noise}$, while a property of the middle product $(a_i \odot s) \odot r_{\mathsf{ID},i} = (a_i r_{\mathsf{ID},i}) \odot s$ ensures that the former elements $(b_i)_{i=1}^{t+\gamma\tau}$ are computed with a secret key $(r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau}$ and becomes $\sum_{i=1}^{t+\gamma\tau} b_i \odot r_{\mathsf{ID},i} \approx u_{\mathsf{ID}} \odot s + 2 \cdot \mathsf{noise}$ to cancel the mask of b'. Specifically, the decryption algorithm computes

$$\begin{aligned}
& b' - \sum_{i=1}^{t+\gamma\tau} b_i \odot r_{\mathsf{ID},i} \\
&= \mathsf{m} + u_{\mathsf{ID}} \odot s + 2 \cdot \mathsf{noise} - \sum_{i=1}^{t+\gamma\tau} ((a_i \odot s) \odot r_{\mathsf{ID},i} + 2 \cdot \mathsf{noise} \odot r_{\mathsf{ID},i}) \\
&= \mathsf{m} + u_{\mathsf{ID}} \odot s + 2 \cdot \mathsf{noise} - \sum_{i=1}^{t+\gamma\tau} ((a_i r_{\mathsf{ID},i}) \odot s + 2 \cdot \mathsf{noise} \odot r_{\mathsf{ID},i}) \\
&= \mathsf{m} + \cancel{u_{\mathsf{ID}} \odot s} + 2 \cdot \mathsf{noise} - \cancel{u_{\mathsf{ID}} \odot s} + 2 \cdot \mathsf{noise} \\
&= \mathsf{m} + 2 \cdot \mathsf{noise}
\end{aligned}$$

by using the fact that $(r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau} \in R[X]^{t+\gamma\tau}$ is a set of small polynomials such that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i} = u_{\mathsf{ID}}$. Since noise is small, we can recover a plaintext $\mathsf{m} \in \{0,1\}^n$ by computing $\left(b' - \sum_{i=1}^{t+\gamma\tau} b_i \odot r_{\mathsf{ID},i} \in R[X]\right) \mod 2$.

In our security proof following Katsumata et al. [17], the MPLWE assumption ensures that $(b_i = a_i \odot s + 2 \cdot \mathsf{noise})_{i=1}^{t+\gamma\tau}$ is indistinguishable from uniform. Since an IBE adversary cannot receive $\mathsf{LVV.sk_{ID^\star}} = (r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau} \in R[X]^{t+\gamma\tau}$ for the target identity $\mathsf{ID}^\star$, the entropy of $(r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau}$ ensures that $u_{\mathsf{ID}} \odot s + 2 \cdot \mathsf{noise} \approx \sum_{i=1}^{t+\gamma\tau} b_i \odot r_{\mathsf{ID},i}$ is indistinguishable from uniform and completely masks a plaintext.

Proposed RIBE Scheme. The proposed RIBE scheme is an MPLWE variant of Takayasu-RIBE and a revocable variant of LVV-IBE. Let H denote a hash function that maps a binary string to a polynomial in $R[X]$. We use the hash function to compute $\mathsf{H}(\mathsf{ID}) = u_{\mathsf{ID}}$ and $\mathsf{H}(\theta, \mathsf{T}) = u_{\mathsf{T},\theta}$. A master public/secret key pair $(\mathsf{mpk}, \mathsf{msk}) = ((a_i)_{i=1}^{t+\gamma\tau}, (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)})$ and a secret key $\mathsf{sk_{ID}} = (r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau}$ are the same as LVV-IBE. A key update $\mathsf{ku_T} = \{\theta, (r_{\mathsf{T},\theta,i})_{i=1}^{t+\gamma\tau}\}_{\theta \in \mathcal{I}_{\mathsf{T}}}$ such that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\theta_j,i} = u_{\mathsf{T},\theta}$ combines the structures of Takayasu-RIBE and LVV-IBE. A ciphertext for $(\mathsf{ID}, \mathsf{T})$ and a plaintext $\mathsf{m} \in \{0,1\}^n$ is an MPLWE variant of

Takayasu-RIBE's ciphertext $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} = (b, \{b'_\theta\}_{\theta\in\mathcal{I}_{\mathsf{ID}}}) \in R[X] \times R[X]^{|\mathcal{I}_{\mathsf{ID}}|}$;

$$b_i = a_i \odot s + 2 \cdot \mathsf{noise}, \qquad b'_\theta = \mathsf{m} + (u_{\mathsf{ID}} + u_{\mathsf{T},\theta}) \odot s + 2 \cdot \mathsf{noise},$$

where each coefficient of $s \in R[X]$ follows the uniform distribution and that of noise follows the discrete Gaussian distribution. All the latter elements b'_θ embed a plaintext m masked by $(u_{\mathsf{ID}} + u_{\mathsf{T},\theta}) \odot s + 2 \cdot \mathsf{noise}$. If ID is not revoked at T, the property of the KUNode algorithm [25] ensures that there is a binary string $\tilde{\theta} \in \mathcal{I}_{\mathsf{ID}} \cap \mathcal{I}_{\mathsf{T}}$. Thus, a property of the middle product $a_i \odot s \odot (r_{\mathsf{ID},i} + r_{\mathsf{T},\theta,i}) = (a_i(r_{\mathsf{ID},i} + r_{\mathsf{T},\theta,i})) \odot s$ ensures that a non-revoked ID can cancel $\sum_{i=1}^{t+\gamma\tau} b_i \odot (r_{\mathsf{ID},i} + r_{\mathsf{T},\theta,i}) \approx (u_{\mathsf{ID}} + u_{\mathsf{T},\theta}) \odot s + 2 \cdot \mathsf{noise}$ and decrypt a ciphertext $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$.

We prove the security of the proposed RIBE scheme by combining security proofs of Takayasu-RIBE and LVV-IBE. In a security proof, the MPLWE assumption ensures that $(b_i = a_i \odot s + 2 \cdot \mathsf{noise})_{i=1}^{t+\gamma\tau}$ is indistinguishable from uniform. If the adversary receives $\mathsf{sk}_{\mathsf{ID}^\star} = (r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau}$, the property of the KUNode algorithm [25] ensures that $\mathsf{ku}_{\mathsf{T}^\star} = \{\theta, (r_{\mathsf{T}^\star,\theta,i})_{i=1}^{t+\gamma\tau}\}_{\theta\in\mathcal{I}_{\mathsf{T}^\star}}$ which the adversary receives satisfies $\mathsf{ku}_{\mathsf{T}^\star} \cap (\mathcal{I}_{\mathsf{ID}^\star} \cap \mathcal{I}_{\mathsf{T}^\star}) = \emptyset$. As a result, each entropy of $(r_{\mathsf{T}^\star,\theta,i})_{i=1}^{t+\gamma\tau}$ for $\theta \in \mathcal{I}_{\mathsf{ID}^\star}$ ensures that $u_{\mathsf{T}^\star,\theta} \odot s + 2 \cdot \mathsf{noise} \approx \sum_{i=1}^{t+\gamma\tau} b_i \odot r_{\mathsf{T},\theta,i}$ is indistinguishable from uniform and completely mask a plaintext. If the adversary does not receive $\mathsf{sk}_{\mathsf{ID}^\star} = (r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau}$, it can receive $\mathsf{ku}_{\mathsf{T}^\star} = \{\theta, (r_{\mathsf{T}^\star,\theta,i})_{i=1}^{t+\gamma\tau}\}_{\theta\in\mathcal{I}_{\mathsf{T}^\star}}$ that contains $(r_{\mathsf{T}^\star,\tilde{\theta},i})_{i=1}^{t+\gamma\tau}$ for $\tilde{\theta} \in \mathcal{I}_{\mathsf{ID}^\star} \cap \mathcal{I}_{\mathsf{T}^\star}$. Since the property of the KUNode algorithm [25] ensures that $\tilde{\theta}$ is a unique binary string in $\mathcal{I}_{\mathsf{ID}^\star} \cap \mathcal{I}_{\mathsf{T}^\star}$, each entropy of $(r_{\mathsf{T}^\star,\theta,i})_{i=1}^{t+\gamma\tau}$ for $\theta \in \mathcal{I}_{\mathsf{ID}^\star} \setminus \{\tilde{\theta}\}$ ensures that $u_{\mathsf{T}^\star,\theta} \odot s + 2 \cdot \mathsf{noise} \approx \sum_{i=1}^{t+\gamma\tau} b_i \odot r_{\mathsf{T},\theta,i}$ is indistinguishable from uniform and completely masks a plaintext of b'_θ. On the other hand, the entropy of $(r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau}$ ensures that $u_{\mathsf{ID}} \odot s + 2 \cdot \mathsf{noise} \approx \sum_{i=1}^{t+\gamma\tau} b_i \odot r_{\mathsf{ID},i}$ is indistinguishable from uniform and completely masks a plaintext of $b'_{\tilde{\theta}}$.

1.4 Difference from the Conference Version

Here, we highlight differences from the conference version of our paper. In this paper, we first review LVV-IBE and prove the tight adaptive anonymity of LVV-IBE in the QROM. The security proof of our RIBE scheme is based on that of LVV-IBE. We also provide the complete proofs of the correctness and the tight adaptive anonymity of our RIBE scheme. Moreover, we give a construction of the proposed anonymous RIBE scheme with *bounded decryption key exposure resistance*, which is a stronger security notion proposed by Takayasu and Watanabe [31,32].

1.5 Roadmap

In Section 2, we review mathematical preliminaries. In Section 3, we review the definition of IBE and the construction of LVV-IBE and prove the tight adaptive anonymity in the QROM. In Section 4, we review the definition of RIBE. In Section 5, we propose our RIBE scheme and prove the tight adaptive anonymity in the QROM. In Section 6, we proposed our anonymous RIBE scheme with bounded decryption key exposure resistance and a proof overview of the tight adaptive anonymity in the QROM.

2 Preliminaries

Notation. Let λ denote the security parameter. Let $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ and $\mathbb{R}_q = \mathbb{R}/q\mathbb{R}$. Let $\mathbf{J}_n$ be an $n \times n$ anti-diagonal matrix whose all anti-diagonal components are one. For positive integers n, m such that $m \geq n$, let $[n] = \{1, \ldots, n\}$ and $[n, m] = \{n, \ldots, m\}$. Let $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ be a set of all functions from a set $\mathcal{X}$ to a set $\mathcal{Y}$. For a distribution D over $\mathbb{R}^n$, $x \leftarrow D$ and $x \leftarrow \lfloor D \rceil$ denotes that x is sampled from D, and x is sampled from D and then each coefficient is rounded to the nearest integer, respectively. For a finite set S, $x \xleftarrow{\mathrm{U}} S$ denotes that x is sampled uniformly at random from S. Let $\mathsf{poly}(\lambda)$ and $\mathsf{negl}(\lambda)$ denote unspecified functions $f(\lambda) = O(\lambda^c)$ for some constant c and $f(\lambda) = o(\lambda^{-c})$ holds for all constant c, respectively. A function f is called negligible function if $f(\lambda) = \mathsf{negl}(\lambda)$. For an event E, probabilities of occurrence of E are called negligible probability and overwhelming probability if $\Pr[E] = \mathsf{negl}(\lambda)$ holds and $\Pr[E] = 1 - \mathsf{negl}(\lambda)$ holds, respectively. For a finite set A, let $U(A)$ be a uniform distribution over A. The statistical distance between two distributions X and Y over a countable domain Ω is defined to be $\frac{1}{2}\sum_{d\in\Omega} |X(d) - Y(d)|$. We say that two distributions X and Y (formally, two ensembles of distributions indexed by n) are statistically indistinguishable if $\frac{1}{2}\sum_{d\in\Omega} |X(d) - Y(d)| = \mathsf{negl}(n)$ holds.

Quantum Computation. We briefly give some background on quantum computation. Let $\{|x\rangle\}_{x\in\{0,1\}^n}$ denote an orthonormal basis of $\mathbb{C}^{2^n}$ and $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \in \mathbb{C}^{2^n}$ denote a quantum state representing n qubits, where α_x is a complex such that $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$. If we measure a quantum state $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \in \mathbb{C}^{2^n}$, a bit sequence x is observed with probability $|\alpha_x|^2$. In the QROM, we assume that a quantumly accessible oracle hash function H exists. The quantum random oracle takes $\sum_{x,y} \alpha_{x,y} |x\rangle |y\rangle$ as input and outputs $\sum_{x,y} \alpha_{x,y} |x\rangle |\mathsf{H}(x) \oplus y\rangle$. Let $\mathcal{A}^{|\mathsf{H}\rangle}$ denote a quantum algorithm $\mathcal{A}$ that accesses to H. The running time $\mathsf{Time}(\mathcal{A})$ of a quantum algorithm $\mathcal{A}$ is defined to be the number of universal gates (e.g., Hadamard, phase, CNOT, and $\pi/8$ gates) and measurements required for running $\mathcal{A}$. Here, an oracle query is counted as a unit time if $\mathcal{A}$ is an oracle algorithm.

The following lemma states that if an oracle outputs independent and almost uniform for any inputs, this oracle is indistinguishable from a random oracle even with quantum oracle accesses.

Lemma 1 ([6]). *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 $\mathsf{H} \xleftarrow{\mathrm{U}} \mathcal{H}$, 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*

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

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

We review the definition of quantum-accessible pseudorandom functions (PRFs) [6].

Definition 1 (Quantum-accessible PRF). *For sets $\mathcal{X}$ and $\mathcal{Y}$, we say a function $F : \mathcal{X} \times \mathcal{Y} \to \mathcal{K}$ is a quantum-accessible pseudorandom function if for any quantum polynomial time algorithm $\mathcal{A}$, the advantage defined below is negligible:*

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

where $\mathsf{RF} \xleftarrow{\mathrm{U}} \mathsf{Func}(\mathcal{X}, \mathcal{Y})$ *and* $K \xleftarrow{\mathrm{U}} \mathcal{K}$.

Lattices and Discrete Gaussian Distribution. We represent column vectors in bold font small letters and matrices in bold font capital letters. When we simply refer to vectors, we mean column vectors. A symmetric matrix $\mathbf{P} \in \mathbb{R}^{n\times n}$ is called positive semi-definite if $\mathbf{x}^\top \mathbf{P}\mathbf{x} \geq 0$ holds for all $\mathbf{x} \in \mathbb{R}^n$. For a vector $\mathbf{a} \in \mathbb{R}^n$, let $\|\mathbf{a}\|$ and $\|\mathbf{a}\|_\infty$ be L_2 norm and L_∞ norm of $\mathbf{a}$, respectively.

For m linearly independent vectors $(\mathbf{b}_i)_{i=1}^m \in (\mathbb{R}^n)^m$, an n-dimensional lattice generated by $(\mathbf{b}_i)_{i=1}^m$ is defined as $\Lambda = \{\sum_{i=1}^m x_i\mathbf{b}_i \mid x_i \in \mathbb{Z}\}$. For a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, let $\Lambda^\perp_{\mathbf{u}}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{z} = \mathbf{u} \mod q\}$. For a positive semi-definite matrix $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$, the n-dimensional discrete Gaussian function $\rho_s : \Lambda \to (0, 1]$ is defined as $\rho_{\mathbf{\Sigma}}(\mathbf{x}) = \exp(-\pi\mathbf{x}^\top\mathbf{\Sigma}^{-1}\mathbf{x})$. For a positive semi-definite matrix $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$, the discrete Gaussian distribution $D_{\Lambda,\Sigma}$ on a lattice $\Lambda \subset \mathbb{R}^n$ is defined as the distribution whose density is $\rho_{\mathbf{\Sigma}}(\mathbf{x})/\sum_{\mathbf{x}\in\Lambda}\rho_{\mathbf{\Sigma}}(\mathbf{x})$ for $\mathbf{x} \in \Lambda$. Especially, for an identity matrix $\mathbf{I}_n$ and a real σ, $D_{\Lambda,\sigma}$ denotes $D_{\Lambda,\sigma\mathbf{I}_n}$.

Lemma 2 ([13], Lemma 2.9). *For $\varepsilon \in (0, \frac{1}{2})$, $\sigma \geq \sqrt{\ln(1+\varepsilon^{-1})/\pi}$, $t > \omega(\sqrt{\log n})$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, it holds that $\|\mathbf{x}\|_\infty \leq t\sigma$ with overwhelming probability in n, where $\mathbf{x} \leftarrow D_{\Lambda^\perp_{\mathbf{u}}(\mathbf{A}),\sigma}$.*

Polynomials and Matrices. For a matrix $\mathbf{M}$, let $s_i(\mathbf{M})$ be the i-th largest singular value of $\mathbf{M}$. For a vector $\mathbf{a} \in \mathbb{R}^n$, let a be a degree $n-1$ polynomial over $\mathbb{R}$ whose coefficient vector is $\mathbf{a}$. For a ring R, let $R^{<n}[X] \subset R[X]$ denote a set of polynomials of degree at most $n-1$. For a ring R and a polynomial $a \in R^{<n}[X]$, let $\mathbf{a} \in R^n$ be a coefficient vector of a. For a degree n polynomial a over $\mathbb{R}$, let $\|a\|$ and $\|a\|_\infty$ denote L_2 norm and L_∞ norm of the polynomial a's coefficient vector $\mathbf{a}$, respectively. For a distribution D, let $x \leftarrow D^{<d}[X]$ denote an operation of sampling each coefficient according to D to obtain a polynomial of degree at most $d-1$. For a distribution D, let $x \leftarrow \lfloor D \rceil^{<d}[X]$ denote an operation of sampling each coefficient according to D and rounding to the nearest integer to obtain a polynomial of degree at most $d-1$.

We use the following lemmata to construct our schemes.

Definition 2 ([27], Definition 2.5). *For positive integers d, k and a polynomial $a \in R^{<d}[X]$, let $\mathsf{T}^{d,k}(a) \in R^{(d+k-1)\times k}$ denote a matrix whose i-th row is a coeffcient vector of $x^{i-1} \cdot a$. By definition, $\mathsf{T}^{d,1}(a)$ is a coefficient vector of a. Moreover, we define $\mathsf{T}^{d,k}_{\mathsf{flip}} = \mathbf{J}_{d+k-1}\mathsf{T}^{d,k}\mathbf{J}_k$.*

Lemma 3 ([27]). *For positive integers ℓ, k, d and polynomials $a \in R^{<k}[X]$ and $b \in R^{<\ell}[X]$, it holds that $\mathsf{T}^{k,\ell+d-1}(a)\mathsf{T}^{\ell,d}(b) = \mathsf{T}^{\ell+k-1,d}(ab)$ and $\mathsf{T}^{k,\ell+d-1}_{\mathsf{flip}}(a)\mathsf{T}^{\ell,d}_{\mathsf{flip}}(b) = \mathsf{T}^{\ell+k-1,d}_{\mathsf{flip}}(ab)$.*

Lemma 4 (implicit in [22], Theorem 3 and Lemma 11). *For a distribution $\chi = D_{\mathbb{Z},\sigma}$, we define a distribution $V = ((a_i)_{i=1}^t, \sum_{i=1}^t a_i r_i)$ over $S = (\mathbb{Z}_q^{<n}[X])^t \times \mathbb{Z}_q^{<n+d-1}[X]$, where $a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n}[X]$ and $r_i \leftarrow \chi^d[X]$. If $d \leq n$, $\sigma = \omega(1)$, $q = \mathsf{poly}(n)$, $q = \omega(\sqrt{\log n})\sigma$, and $\frac{dt}{n} = \Omega(\log n)$, then V is statistically indistinguishable from $U(S)$. Let $\mathbf{A} = [\mathsf{T}^{n,d}(a_1)|\cdots|\mathsf{T}^{n,d}(a_t)]$ and $\mathbf{r} = [\mathbf{r}_1^\top|\cdots|\mathbf{r}_t^\top]^\top$, where $r_i \leftarrow \chi^d[X]$ for each $i \in [t]$. For a fixed $u \in \mathbb{Z}_q^{<n+2d-2}[X]$, the conditional distribution of $\mathbf{r}$, given $u = \sum_{i=1}^t a_i r_i \mod q$ is $D_{\Lambda_{\mathbf{u}}^\perp(\mathbf{A}),\sigma}$.*

Lemma 5 ([16], Lemma 1). *Let q, ℓ, m be positive integers, $r > \max\{\omega(\sqrt{\log m}), \omega(\sqrt{\log \ell})\}$ be a positive real, $\mathbf{b} \in \mathbb{Z}_q^m$ be a vector, and $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,r}$. For a matrix $\mathbf{V} \in \mathbb{Z}_q^{m\times\ell}$ and a positive real $\sigma > s_1(\mathbf{V})$, there is a PPT algorithm $\mathsf{Rerand}(\mathbf{V}, \mathbf{b}+\mathbf{x}, r, \sigma)$, which outputs $\mathbf{b}' = \mathbf{V}^\top\mathbf{b} + \mathbf{x}' \in \mathbb{Z}_q^\ell$. The distribution of $\mathbf{x}'$ is statistically indistinguishable from $D_{\mathbb{Z}^\ell,2r\sigma}$.*

Lemma 6 ([13,22]). *Suppose that $q = \mathsf{poly}(n)$, $d \leq n$, $\frac{dt}{n} = \Omega(\log n)$, and $\gamma = \frac{n+2d-2}{d}$. Then, there exist the following three PPT algorithms.*

- $\mathsf{TrapGen}(1^n) \to ((a_i)_{i=1}^{t+\gamma\tau}, (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)})$**:** $\mathsf{TrapGen}$ *algorithm takes n as input, and outputs $(a_i)_{i=1}^{t+\gamma\tau} \in (\mathbb{Z}_q^{<n}[X])^t \times (\mathbb{Z}_q^{<n+d-1}[X])^{\gamma\tau}$ and $(w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)} \in (\mathbb{Z}_q^{<d}[X])^{t\gamma\tau}$. $(a_i)_{i=1}^{t+\gamma\tau}$ is statistically indistinguishable from uniform. For each $(i,j) \in [\tau]\times[\gamma]$, it holds that $a_{t+(i-1)\gamma+j} = 2^{i-1}x^{d(j-1)} - \sum_{h=1}^t a_h w_{h,(i-1)\gamma+j}$.*
- $\mathsf{SamplePre}((a_i)_{i=1}^{t+\gamma\tau}, (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}, u, \sigma) \to (r_i)_{i=1}^{t+\gamma\tau}$**:** $\mathsf{SamplePre}$ *algorithm takes $(a_i)_{i=1}^{t+\gamma\tau}$, $(w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}$, $u \in \mathbb{Z}_q^{<n+2d-2}[X]$, and $\sigma = \omega(\log^2 n)\sqrt{ndt}$ as input, and outputs $(r_i)_{i=1}^{t+\gamma\tau} \in (\mathbb{Z}^{<2d-1}[X])^t \times (\mathbb{Z}^{<d}[X])^{\gamma\tau}$. Let $\mathbf{A} = [\mathsf{T}^{n,2d-1}(a_1)|\cdots|\mathsf{T}^{n+d-1,d}(a_{t+\gamma\tau})]$. $\mathbf{r} = [\mathbf{r}_1|\cdots|\mathbf{r}_{t+\gamma\tau}]$ is statistically indistinguishable from $D_{\Lambda_{\mathbf{u}}^\perp(\mathbf{A}),\sigma}$. In particular, $(\mathbf{r}_i)_{i=1}^{t+\gamma\tau}$ is statistically indistinguishable from $(D_{\mathbb{Z}^{2d-1},\sigma})^t \times (D_{\mathbb{Z}^d,\sigma})^{\gamma\tau}$ subject to the constraint that $\sum_{i=1}^{t+\gamma\tau} a_i r_i = u \mod q$.*
- $\mathsf{SampleZ}(\sigma) \to \mathbf{e}$**:** $\mathsf{SampleZ}$ *algorithm takes $\sigma > 16\sqrt{\log 2m/\pi}$ as input and outputs $\mathbf{e} \in \mathbb{Z}^m$. The distribution of $\mathbf{e}$ is statistically indistinguishable from $D_{\mathbb{Z}^m,\sigma}$.*

Middle-Product Learning with Errors. We use the following definitions and lemmata to define the MPLWE assumption.

Definition 3 ([27], Definition 3.1). *Let d_a, d_b, d, k be positive integers such that $d_a + d_b - 1 = d + 2k$. Middle Product $\odot_d : R^{<d_a}[X] \times R^{<d_b}[X] \to R^{<d}[X]$ is defined as $a \odot_d b = \left\lfloor \frac{(a\cdot b) \mod x^{k+d}}{x^k} \right\rfloor$. This operation extracts the middle-degree d terms after the multiplication of the input two polynomials.*

For example, for $a = x^2 + 2x + 3$ and $b = x^3 + 2x^2 + 3x + 4$, we have $a \cdot b = x^5 + 4x^4 + 10x^3 + 16x^2 + 17x + 12$ and $a \odot_2 b = 10x + 16$.

Lemma 7 ([27], Lemma 3.2 and Lemma 3.3). *Let $d, k, n > 0$ be positive integers. For polynomials $r \in R^{<k+1}[X]$, $a \in R^{<n}[X]$, and $s \in \mathbb{Z}_q^{<n+d+k-1}[X]$, it holds that $(a \odot_{d+k} s) \odot_d r = (ar) \odot_d s$. For polynomials $r \in R^{<k+1}[X]$, $c \in R^{<k+d}[X]$, and $b \in R^{<d}[X]$, it holds that $b = r \odot_d c \Leftrightarrow \mathbf{b} = \mathsf{T}_{\mathsf{flip}}^{k+1,d}(r)^\top \mathbf{c}$.*

We review the MPLWE assumption.

Definition 4 (MPLWE Assumption [22], Definition 9). *For an even number $n > 0$, positive integers $q \geq 2$, $m > 0$, a positive integer vector $\mathbf{d} = (d_i)_{i=1}^t \in [\frac{n}{2}]^t$, a distribution χ over $\mathbb{Z}_q$, and a quantum polynomial time algorithm $\mathcal{A}$, the advantage for the MPLWE problem $\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}$ is defined as follows: $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}}(\lambda) = \left|\Pr[\mathcal{A}((a_i, a_i \odot_{d_i} s + e_i)_{i=1}^t) = 1] - \Pr[\mathcal{A}((a_i, w_i + e_i)_{i=1}^t) = 1]\right|$, where $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n}[X]$, $a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n-d_i}[X]$, $e_i \leftarrow \chi^{<d_i}[X]$, and $w_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<d_i}[X]$ for each $i \in [t]$. We say that the $\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}$ assumption holds if $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}}$ is negligible for all quantum polynomial time algorithm $\mathcal{A}$.*

Rosca et al. [27] first defined the MPLWE assumption which is slightly different from Definition 4. In Rosca et al.'s one, all d_i are equal and Lombardi et al. [22] called Definition 4 Degree-Parametrized MPLWE assumption.

We also define the MPLWE assumption against adversaries that can access to a quantum random oracle.

Definition 5 (MPLWE Assumption relative to the QROM). *For an even number $n > 0$, positive integers $q \geq 2$, $m > 0$, a positive integer vector $\mathbf{d} = (d_i)_{i=1}^t \in [\frac{n}{2}]^t$, a distribution χ over $\mathbb{Z}_q$, and a quantum polynomial time algorithm $\mathcal{A}$, the advantage for the MPLWE problem $\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}$ relative to a quantum random oracle is defined as follows: $\mathsf{Adv}_{\mathcal{A},\mathbf{QRO}_{a,b}}^{\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}}(\lambda) = \left|\Pr[\mathcal{A}^{|\mathsf{H}\rangle}((a_i, a_i \odot_{d_i} s + e_i)_{i=1}^t) = 1] - \Pr[\mathcal{A}^{|\mathsf{H}\rangle}((a_i, w_i + e_i)_{i=1}^t) = 1]\right|$, where $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n}[X]$, $a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n-d_i}[X]$, $e_i \leftarrow \chi^{<d_i}[X]$, $w_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<d_i}[X]$ for each $i \in [t]$, and $\mathsf{H} \xleftarrow{\mathrm{U}} \mathsf{Func}(\{0,1\}^a, \{0,1\}^b)$. We say that the $\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}$ assumption to an (a,b)-quantum random oracle holds if $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}}$ is negligible for all quantum polynomial time algorithm $\mathcal{A}$.*

If we assume the existence of a quantum-accessible PRF, the MPLWE assumption relative to the QROM in Definition 5 is tightly reduced from the MPLWE assumption in Definition 4.

Lemma 8 ([39], implicit in Lemma 6.1). *Let $F : \mathcal{K} \times \{0,1\}^a \to \{0,1\}^b$ be a quantum-accessible PRF. For any $q, n, \mathbf{d}, \chi$ and a quantum polynomial time algorithm $\mathcal{A}$ making at most Q oracle queries, there are two quantum polynomial time algorithms $\mathcal{B}_1$ and $\mathcal{B}_2$ such that*

$$\mathsf{Adv}_{\mathcal{A},\mathbf{QRO}_{a,b}}^{\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{MPLWE}_{q,n,\mathbf{d},\chi}}(\lambda) + \mathsf{Adv}_{\mathcal{B}_2,F}^{\mathsf{PRF}}(\lambda),$$

$\mathsf{Time}(\mathcal{B}_1) \approx \mathsf{Time}(\mathcal{A}) + Q \cdot T_F$, and $\mathsf{Time}(\mathcal{B}_2) \approx \mathsf{Time}(\mathcal{A})$, where T_F denotes the time to evaluate F.

We review the PLWE assumption.

Definition 6 (PLWE assumption). *Let f be a polynomial of degree m, $q \geq 2$, and χ be a distribution over $\mathbb{Z}_q[X]/(f)$. For a quantum polynomial time algorithm $\mathcal{A}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PLWE}_{q,\chi}}(\lambda)$ is defined as follows:*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PLWE}_{q,\chi}}(\lambda) = \Big|\Pr[\mathcal{A}(a, as+e)=1] - \Pr[\mathcal{A}(a,w)=1]\Big|,$$

where $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q[X]/(f)$, $a \xleftarrow{\mathrm{U}} \mathbb{Z}_q[X]/(f)$, $e \leftarrow \chi$, and $w \xleftarrow{\mathrm{U}} \mathbb{Z}_q[X]/(f)$. We say that the $\mathsf{PLWE}_{q,\chi}$ assumption holds if $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PLWE}_{q,\chi}}$ is negligible for all quantum polynomial time algorithm $\mathcal{A}$.

We review a reduction from PLWE to MPLWE.

Lemma 9 ([4], implicit in Theorem 2). *For any polynomial $f \in \mathcal{E}(T, \mathbf{d}, n)$ and a real α such that $1 \geq \alpha \geq \frac{2\sqrt{n}}{qT}$, there is a PPT reduction from $\mathsf{PLWE}^{(f)}_{q,D_{\mathbb{Z}_q^m},\alpha q}$ to $\mathsf{MPLWE}_{q,n,\mathbf{d},D_{\mathbb{Z}_q,\alpha' q}}$, where $\alpha' = \alpha \cdot \sqrt{n} \cdot \mathrm{EF}(f)$.*

3 Tight Adaptive Anonymity of LVV-IBE in the QROM

In this section, we prove the tight adaptive anonymity of LVV-IBE in the QROM. In Section 3.1, we review the definition of IBE. In Section 3.2, we propose a slight modification of LVV-IBE. In Section 3.3, we prove the correctness and set parameters. In Section 3.4, we prove the tight adaptive anonymity.

3.1 Identity-based Encryption

We review the definition of IBE.

Syntax. A plaintext space, a ciphertext space, and an identity space are denoted by $\mathcal{M}$, $\mathcal{CT}$ and $\mathcal{ID}$, respectively. An IBE scheme Π consists of the following four algorithms.

$\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$**:** Setup algorithm takes a security parameter 1^λ as input, and outputs a master public key mpk and a master secret key msk.

$\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}) \to \mathsf{sk}_{\mathsf{ID}}$**:** SKGen algorithm takes mpk, msk, and an identity $\mathsf{ID} \in \mathcal{ID}$ as input, and outputs a secret key $\mathsf{sk}_{\mathsf{ID}}$ for the identity ID.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{m}) \to \mathsf{ct}_{\mathsf{ID}}$**:** Encrypt algorithm takes mpk, ID, and a plaintext $\mathsf{m} \in \mathcal{M}$ as input, and outputs a ciphertext $\mathsf{ct}_{\mathsf{ID}} \in \mathcal{CT}$ for ID.

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ct}_{\mathsf{ID}}) \to \mathsf{m}'$**:** Decrypt algorithm takes mpk, $\mathsf{sk}_{\mathsf{ID}}$, and $\mathsf{ct}_{\mathsf{ID}}$ as input, and outputs a decryption result m'.

Correctness. A ciphertext $\mathsf{ct}_{\mathsf{ID}} \in \mathcal{CT}$ for an identity ID has to be decrypted correctly by a secret key $\mathsf{sk}_{\mathsf{ID}}$ for the same ID. Namely, for all $\lambda \in \mathbb{N}$, $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{ID} \in \mathcal{ID}$, and $\mathsf{m} \in \mathcal{M}$, we require m' obtained by running the following algorithms to satisfy $\mathsf{m}' = \mathsf{m}$. (1) $\mathsf{sk}_{\mathsf{ID}} \leftarrow \mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID})$, (2) $\mathsf{ct}_{\mathsf{ID}} \leftarrow \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{m})$, and (3) $\mathsf{m}' \leftarrow \mathsf{Decrypt}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ct}_{\mathsf{ID}})$.

Security. The security of IBE is defined via a security game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

In the beginning of the security game, $\mathcal{C}$ runs $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$. $\mathcal{A}$ may adaptively make the following two queries.

Secret Key Reveal Query: Upon a query $\mathsf{ID} \in \mathcal{ID}$ by $\mathcal{A}$, if $\mathsf{ID} = \mathsf{ID}^\star$, $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ runs $\mathsf{sk}_\mathsf{ID} \leftarrow \mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID})$ and returns sk_ID to $\mathcal{A}$.

Challenge Query: $\mathcal{A}$ is allowed to make this query only once in this game. Upon a query $(\mathsf{m}^\star, \mathsf{ID}^\star)$ by $\mathcal{A}$, $\mathcal{C}$ picks $\mathsf{coin} \xleftarrow{\mathrm{U}} \{0,1\}$. If $\mathsf{coin} = 0$ holds, $\mathcal{C}$ runs $\mathsf{ct}^\star \leftarrow \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}^\star, \mathsf{m}^\star)$. If $\mathsf{coin} = 1$ holds, $\mathcal{C}$ picks $\mathsf{ct}^\star \xleftarrow{\mathrm{U}} \mathcal{CT}$. Then, $\mathcal{C}$ returns $\mathsf{ct}^\star$ to $\mathcal{A}$.

At some point in this game, $\mathcal{A}$ outputs $\widehat{\mathsf{coin}} \in \{0,1\}$ as a guess value of coin and terminates this game.

We say that $\mathcal{A}$ wins if $\widehat{\mathsf{coin}} = \mathsf{coin}$ holds. Let $\mathrm{Adv}^{\mathrm{IBE}}_{\Pi,\mathcal{A}}(\lambda) = |\Pr[\widehat{\mathsf{coin}} = \mathsf{coin}] - \frac{1}{2}|$ be the $\mathcal{A}$'s advantage in this game.

Definition 7. *An IBE scheme Π is said to satisfy the adaptive anonymity if $\mathrm{Adv}^{\mathrm{IBE}}_{\Pi,\mathcal{A}}(\lambda) = \mathsf{negl}(\lambda)$ holds for all PPT adversary $\mathcal{A}$.*

3.2 LVV-IBE

Construction and parameter settings are almost the same as LVV-IBE [22]. Let q be a prime number, and n, d, t, k, γ, τ, and $L_{\mathcal{ID}}$ be positive integers. Let α, α', σ be positive real numbers. The plaintext space, the identity space, and the ciphertext space are defined as $\mathcal{M} = \{0,1\}^{k+2}$, $\mathcal{ID} = \{0,1\}^{L_{\mathcal{ID}}}$, and $\mathcal{CT} = (\mathbb{Z}_q^{<2d+k}[X])^t \times (\mathbb{Z}_q^{<d+k+1}[X])^{\gamma\tau} \times \mathbb{Z}_q^{<k+2}[X]$, respectively. A hash function $\mathsf{H} : \{0,1\}^{L_{\mathcal{ID}}} \to \mathbb{Z}_q^{<n+2d-2}[X]$ will be modeled as a random oracle in the security proof.

$\mathsf{Setup}(1^n) \to (\mathsf{mpk}, \mathsf{msk})$**:** Run $((a_i)_{i=1}^{t+\gamma\tau}, (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}) \leftarrow \mathsf{TrapGen}(1^n)$ and output $\mathsf{mpk} = (a_i)_{i=1}^{t+\gamma\tau}$ and $\mathsf{msk} = (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}$.

$\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}) \to \mathsf{sk}_\mathsf{ID}$**:** Run $(r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau} \leftarrow \mathsf{SamplePre}(\mathsf{mpk}, \mathsf{msk}, u_\mathsf{ID}, \sigma)$, where $u_\mathsf{ID} = \mathsf{H}(\mathsf{ID})$. By Lemma 6, it holds that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i} = u_\mathsf{ID}$. Then, output $\mathsf{sk}_\mathsf{ID} = (r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau}$.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{m}) \to \mathsf{ct}_\mathsf{ID}$**:** Sample $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$, $e_i \leftarrow D^{<2d+k}_{\mathbb{Z}_q,\alpha' q}[X]$ for each $i \in [t]$, $e_i \leftarrow D^{<d+k+1}_{\mathbb{Z}_q,\alpha' q}[X]$ for $i \in [t+1, t+\gamma\tau]$, and $e' \leftarrow D^{<k+2}_{\mathbb{Z}_q,\alpha' q}[X]$. Then, compute

$$b_i = \begin{cases} a_i \odot_{2d+k} s + 2e_i & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s + 2e_i & \text{if } i \in [t+1, t+\gamma\tau] \end{cases}$$
$$b' = \mathsf{m} + u_\mathsf{ID} \odot_{k+2} s + 2e'$$

and output $\mathsf{ct}_\mathsf{ID} = ((b_i)_{i=1}^{t+\gamma\tau}, b')$.

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ct}_{\mathsf{ID}}) \to \mathsf{m}'$**:** Output

$$\mathsf{m}' = \left(b' - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} r_{\mathsf{ID},i} \mod q \right) \mod 2.$$

Here, we slightly modify LVV-IBE's $\mathsf{Encrypt}$ algorithm to apply the noise rerandomization algorithm. Concretely, in the $\mathsf{Encrypt}$ algorithm of LVV-IBE, the error polynomials are $e_i \leftarrow \lfloor D_{\mathbb{R}_q,\alpha' q} \rceil^{<2d+k}[X]$ for each $i \in [t]$, $\mathbf{e}_i \leftarrow \lfloor D_{\mathbb{R}_q}, \alpha' q \rceil^{<d+k+1}[X]$ for each $i \in [t+1, t+\gamma\tau]$, and $e' \leftarrow \lfloor D_{\mathbb{R}_q,\alpha' q} \rceil^{<k+2}[X]$.

3.3 Correctness and Parameter Settings

We prove the correctness by following the original LVV-IBE [22].

Theorem 1 ([22], Lemma 12). *For a positive real number $\alpha' < (8\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$ and a positive integer $K = t(2d-1) + \gamma\tau d$, LVV-IBE satisfies the correctness with overwhelming probability in n.*

Proof. Since $b_i = a_i \odot_{2d+k} s + 2e_i$ holds for each $i \in [t]$ and $b_i = a_i \odot_{d+k+1} s + 2e_i$ holds for each $i \in [t+1, t+\gamma\tau]$, when the $\mathsf{Decrypt}$ algorithm operates as specified, we have

$$\begin{aligned}
& b' - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} r_{\mathsf{ID},i} \\
&= \mathsf{m} + u_{\mathsf{ID}} \odot_{k+2} s + 2e' - \sum_{i=1}^{t} (a_i \odot_{2d+k} s) \odot_{k+2} r_{\mathsf{ID},i} \\
&\quad - \sum_{i=t+1}^{t+\gamma\tau} (a_i \odot_{d+k+1} s) \odot_{k+2} r_{\mathsf{ID},i} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},i}.
\end{aligned}$$

Then, by Lemma 7 and the fact that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i} = u_{\mathsf{ID}}$ holds as we explained in the SKGen algorithm, we have

$$\begin{aligned}
& \mathsf{m} + u_{\mathsf{ID}} \odot_{k+2} s + 2e' - \sum_{i=1}^{t} (a_i \odot_{2d+k} s) \odot_{k+2} r_{\mathsf{ID},i} \\
&\quad - \sum_{i=t+1}^{t+\gamma\tau} (a_i \odot_{d+k+1} s) \odot_{k+2} r_{\mathsf{ID},i} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},i} \\
&= \mathsf{m} + \cancel{u_{\mathsf{ID}} \odot_{k+2} s} + 2e' - \cancel{\sum_{i=1}^{t+\gamma\tau} (a_i r_{\mathsf{ID},i}) \odot_{k+2} s} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},i} \\
&= \mathsf{m} + \underbrace{2 \left(e' - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},i} \right)}_{\text{error terms}}.
\end{aligned}$$

If $\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},i}\|_\infty < \frac{q}{8}$ holds, the decryption of our IBE scheme satisfies the correctness. Let $\mathbf{r}_{\mathsf{ID}} = [\mathbf{r}_{\mathsf{ID},1}^\top | \cdots | \mathbf{r}_{\mathsf{ID},t+\gamma\tau}^\top]^\top$ and

$$\mathbf{A} = [\mathsf{T}^{n,2d-1}(a_1)| \cdots |\mathsf{T}^{n,2d-1}(a_t)|\mathsf{T}^{n+d-1,d}(a_{t+1})| \cdots |\mathsf{T}^{n+d-1,d}(a_{t+\gamma\tau})].$$

By Lemma 6, the property of the $\mathsf{SamplePre}$ algorithm ensures that $\mathbf{r}_{\mathsf{ID}}$ is distributed statistically close to $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A})}$. Therefore, by Lemma 2, it holds that

$$\|r_{\mathsf{ID},i}\|_\infty \le \omega(\sqrt{\log n})\sigma, \qquad \|e_i\|_\infty \le \omega(\sqrt{\log n})\alpha' q$$

with overwhelming probability in n. Since it holds that

$$\begin{aligned}
&\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},i}\|_\infty \\
&\le \|e'_\ell\|_\infty + \|\sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},i}\|_\infty \\
&\le \omega(\sqrt{\log n})\alpha' q + K(\sqrt{2}\omega(\sqrt{\log n})\sigma)(\omega(\sqrt{\log n})\alpha' q),
\end{aligned}$$

we have $\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},i}\|_\infty < \frac{q}{8}$ if $\alpha' < (8\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$ holds. □

To guarantee the correctness and the adaptive anonymity of LVV-IBE, the parameters have to satisfy the following restrictions.

- For the correctness, $\alpha' < (8\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$ holds.
- By Lemma 6, $q = \mathsf{poly}(n)$, $d \le n$, $\frac{dt}{n} = \Omega(\log n)$, $\sigma = \omega(\log^2 n)\sqrt{ndt}$, and $\gamma = \frac{n+2d-2}{d}$ hold to apply $\mathsf{TrapGen}$ and $\mathsf{SamplePre}$ algorithms properly.
- By Lemma 4, $d \le n$, $\sigma = \omega(1)$, $q = \mathsf{poly}(n)$, $q = \omega(\sqrt{\log n})\sigma$, and $\frac{dt}{n} = \Omega(\log n)$ hold so that the master public key is statistically indistinguishable from uniform.
- By Lemma 6, $\sigma > 16\sqrt{\log 2(2d-1)/\pi}$ holds to apply $\mathsf{Sample}\mathbb{Z}$ algorithm properly.
- By Lemma 5, $\frac{\alpha'}{2\alpha} > \sqrt{\sigma^2((2d-1)t + d\gamma\tau) + 1}$ and $\alpha q > \omega(\sqrt{\log(t(2d+k) + \gamma\tau d + (K+2))})$ hold to apply ReRand algorithm properly.
- Let $c > 0$ be a constant. For some polynomial $f \in \mathcal{E}(T, \mathbf{d}, n+2d+k)$ of degree $m \in [2d+k, n]$ with $\mathrm{EF}(f) = O(n^c)$, $\bar{\alpha} = \Omega(\sqrt{m}/q)$, and $1 \ge \bar{\alpha} \ge \frac{2\sqrt{n+2d+k}}{qT}$, $\mathsf{PLWE}^{(f)}_{\mathbb{Z}_q,\bar{\alpha}q}$ assumption holds. Furthermore, q is a prime and $q = \Omega(\alpha^{-1}n^{c+1})$ holds so that $\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z},\alpha q}}$ assumption holds by Lemma 9.

We note that the restrictions are almost the same as those of LVV-IBE, but we add another restriction to apply ReRand algorithm.

To satisfy these restrictions, we set

$$\begin{aligned}
&d = \Theta(n),\ k = \Theta(n),\ t = \log n,\ \gamma = \frac{n+2d-2}{d},\ \sigma = n^{1+\mu_1}, \\
&q = n^{4.5+4\mu_1+c},\ \tau = \lceil \log q \rceil,\ \alpha' = (n^{2+2\mu_1})^{-1},\ \alpha = (n^{3.5+4\mu_1})^{-1},
\end{aligned}$$

where $\mu_1 > 0$ can be set arbitrarily small and $c > 0$ is a parameter of the PLWE assumption.

3.4 The Adaptive Anonymity in the QROM

In this section, we prove the tight adaptive anonymity of LVV-IBE in the QROM.

Theorem 2. *LVV-IBE satisfies the adaptive anonymity in the QROM under the parameter settings and the* MPLWE *assumption. In particular, for any quantum adversary $\mathcal{A}$ making at most Q_{H} queries to $|\mathsf{H}\rangle$ and Q_{ID} secret key reveal queries, there exists a quantum algorithm $\mathcal{B}$ making $Q_{\mathsf{H}} + Q_{\mathsf{ID}}$ quantum random oracle queries such that*

$$\mathrm{Adv}^{\mathrm{IBE}}_{\mathit{LVV\text{-}IBE},\mathcal{A}}(n) \leq \mathsf{Adv}^{\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}}_{\mathcal{B},\mathbf{QRO}_{L_{\mathcal{ID}}+\lceil\log(t+\gamma\tau)\rceil+1,\kappa}}(n) + (Q_{\mathsf{H}}^2 + Q_{\mathsf{ID}}) \cdot \mathsf{negl}(n)$$

and

$$\mathsf{Time}(\mathcal{B}) = \mathsf{Time}(\mathcal{A}) + (Q_{\mathsf{H}} + Q_{\mathsf{ID}}) \cdot \mathsf{poly}(\lambda),$$

where κ denotes the length of randomness for $\mathsf{Sample}\mathbb{Z}$ *and*

$$\mathbf{d} = \begin{cases} 2d + k & \text{if } i \in [t] \\ d + k + 1 & \text{if } i \in [t+1, t+\gamma\tau]. \end{cases}$$

Proof. Let E_i denote an event that $\mathcal{A}$ wins in game i.

Game_0: Game_0 is the original security game. The challenger $\mathcal{C}$ chooses a hash function $\mathsf{H} : \{0,1\}^{L_{\mathcal{ID}}} \to \mathbb{Z}_q^{<n+2d-2}[X]$ at the beginning of the game. Upon a quantum random oracle query $\sum_{\mathsf{ID},y} \alpha_{\mathsf{ID},y} |\mathsf{ID}\rangle |y\rangle$ by the adversary $\mathcal{A}$, $\mathcal{C}$ returns $\sum_{\mathsf{ID},y} \alpha_{\mathsf{ID},y} |\mathsf{ID}\rangle |\mathsf{H}(\mathsf{ID}) \oplus y\rangle$.

Game_1: We change how to answer the quantum random oracle queries from Game_0. In Game_1, $\mathcal{C}$ chooses a function $\widehat{\mathsf{H}} \xleftarrow{\mathrm{U}} \mathsf{Func}(\{0,1\}^{\leq L_{\mathcal{ID}}+\lceil\log(t+\gamma\tau)\rceil}, \{0,1\}^{\kappa})$ at the beginning of the game. With respect to $\mathsf{H}(\mathsf{ID})$, sample coefficient vectors $\mathbf{r}_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|i))$ for each $i \in [t+\gamma\tau]$ and compute $\mathsf{H}(\mathsf{ID}) = \sum_{i=1}^{t+\gamma\tau} a_i \mathbf{r}_{\mathsf{ID},i}$. Here, $\mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|i))$ denotes running $\mathsf{Sample}\mathbb{Z}(\sigma)$ with $\widehat{\mathsf{H}}(\mathsf{ID}\|i)$ as an input random seed.

By Lemma 4, $\mathsf{H}(\mathsf{ID})$ is statistically indistinguishable from uniform. Therefore, Lemma 1 ensures that $|\Pr[E_0] - \Pr[E_1]| = \mathsf{negl}(n) + 4Q_{\mathsf{H}}^2\sqrt{\mathsf{negl}(n)} = Q_{\mathsf{H}} \cdot \mathsf{negl}(n)$, where Q_{H} is the number of random oracle queries.

Game_2: We change how to generate a secret key $(r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau}$ from Game_1. In Game_2, we do not use $\mathsf{SamplePre}$ algorithm. Instead, upon a secret key reveal query of ID, return $\mathbf{r}_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|i))$ for each $i \in [t+\gamma\tau]$ to $\mathcal{A}$.

Let $\mathbf{A} = [\mathsf{T}^{n,2d-1}(a_1)| \cdots |\mathsf{T}^{n+d-1,d}(a_{t+\gamma\tau})]$. By Lemma 6, the property of the $\mathsf{SamplePre}$ algorithm ensures that $\mathbf{r}_{\mathsf{ID}} = [\mathbf{r}_{\mathsf{ID},1}^\top| \cdots |\mathbf{r}_{\mathsf{ID},t+\gamma\tau}^\top]^\top$ of Game_1 is statistically indistinguishable from the discrete Gaussian distribution $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A}),\sigma}$. Moreover, by Lemma 4, $\mathbf{r}_{\mathsf{ID}} = [\mathbf{r}_{\mathsf{ID},1}^\top| \cdots |\mathbf{r}_{\mathsf{ID},t+\gamma\tau}^\top]^\top$ of Game_2 is also statistically

indistinguishable from the above distribution. Since $\mathcal{A}$ obtains at most Q_{ID} secret keys during the game, we have $|\Pr[E_2] - \Pr[E_1]| = Q_{\mathsf{ID}} \cdot \mathsf{negl}(n)$.

Game_3: We change how the master public key is generated from Game_2. In Game_3, the master public key is chosen by running $(a_i)_{i=1}^{t+\gamma\tau} \xleftarrow{\mathrm{U}} (\mathbb{Z}_q^n[X])^t \times (\mathbb{Z}_q^{n+d-1}[X])^{\gamma\tau}$.

By Lemma 6, the property of the $\mathsf{TrapGen}$ algorithm ensures that mpk of Game_2 is statistically indistinguishable from uniform, and thus $|\Pr[E_3] - \Pr[E_2]| = \mathsf{negl}(n)$ holds.

Game_4: We change how to compute the challenge ciphertext of $\mathsf{coin} = 0$ from Game_3. Let $K_e = t(2d+k) + \gamma\tau(d+k+1)$. In Game_4, $\mathcal{C}$ samples $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$, $\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q,\alpha q}^{<2d+k}[X]$ for each $i \in [t]$, and $e_i \leftarrow D_{\mathbb{Z}_q,\alpha q}^{<d+k+1}[X]$ for each $i \in [t+1, t+\gamma\tau]$. Then, $\mathcal{C}$ computes

$$v_i = \begin{cases} a_i \odot_{2d+k} s + e_i & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s + e_i & \text{if } i \in [t+1, t+\gamma\tau]. \end{cases} \tag{1}$$

By Eq. (1) and Lemma 7, we have

$$\mathbf{v}_i = \begin{cases} \mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_i)^\top \mathbf{s} + \mathbf{e}_i & \text{if } i \in [t] \\ \mathsf{T}_{\mathsf{flip}}^{n+d-1,d+k+1}(a_i)^\top \mathbf{s} + \mathbf{e}_i & \text{if } i \in [t+1, t+\gamma\tau] \end{cases}. \tag{2}$$

Let $\mathbf{v} = [\mathbf{v}_1^\top | \cdots | \mathbf{v}_{t+\gamma\tau}^\top]^\top \in \mathbb{Z}_q^{K_e}$ and

$$\mathbf{R}_{\mathsf{ID}^\star,i} = \begin{cases} \mathsf{T}_{\mathsf{flip}}^{2d-1,k+2}(r_{\mathsf{ID}^\star,i}) \in \mathbb{Z}_q^{(2d+k)\times(k+2)} & \text{if } i \in [t] \\ \mathsf{T}_{\mathsf{flip}}^{d,k+2}(r_{\mathsf{ID}^\star,i}) \in \mathbb{Z}_q^{(d+k+1)\times(k+2)} & \text{if } i \in [t+1, t+\gamma\tau] \end{cases},$$

$$\mathbf{R}_{\mathsf{ID}^\star} = \begin{bmatrix} \mathbf{R}_{\mathsf{ID}^\star,1} \\ \vdots \\ \mathbf{R}_{\mathsf{ID}^\star,t+\gamma\tau} \end{bmatrix} \in \mathbb{Z}_q^{K_e \times (k+2)}. \tag{3}$$

Then, run

$$[\mathbf{b}_1 | \cdots | \mathbf{b}_{t+\gamma\tau} \mid \mathbf{b}'] \leftarrow 2 \cdot \mathsf{ReRand}\left(2^{-1}[\mathbf{I}_{K_e} \mid \mathbf{R}_{\mathsf{ID}^\star}], \mathbf{v}, \alpha q, \frac{\alpha'}{2\alpha}\right) \tag{4}$$

and output the challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, b' + \mathsf{m}^\star)$.

We will show that the ReRand algorithm can be applied properly. Since there is a restriction on the maximum singular value of the ReRand algorithm's input matrix, we will evaluate it. We have

$$s_1([\mathbf{I}_{K_e} \mid \mathbf{R}_{\mathsf{ID}^\star}])^2 \le s_1(\mathbf{R}_{\mathsf{ID}^\star})^2 + 1 \le \sum_{i=1}^{t+\gamma\tau} s_1(\mathbf{R}_{\mathsf{ID}^\star,i})^2 + 1$$

and

$$s_1(\mathbf{R}_{\mathsf{ID}^\star,i})^2 = \max_{\|\mathbf{h}\|=1} \|\mathsf{T}^{2d-1,k+2}(r_{\mathsf{ID}^\star,i})\|\mathbf{h}^2$$

$$
\begin{aligned}
&= \max_{\|\mathbf{h}\|=1} \|\mathsf{T}^{2d-1,k+2}(r_{\mathsf{ID}^\star,i})\mathsf{T}^{k+2,1}(h)\|^2 \\
&= \max_{\|\mathbf{h}\|=1} \|\mathsf{T}^{2d+k,1}(r_{\mathsf{ID}^\star,i}h)\|^2 \\
&\leq \|\mathbf{r}_{\mathsf{ID}^\star,i}\|^2 \\
&\leq \sigma^2(2d-1)
\end{aligned}
$$

for each $i \in [t]$. By a similar argument for each $i \in [t+1, t+\gamma\tau]$, it follows that if $\frac{\alpha'}{2\alpha} > \sqrt{\sigma^2((2d-1)t + d\gamma\tau) + 1}$ holds, the ReRand algorithm can be applied properly.

We will show that the challenge ciphertext is statistically indistinguishable between Game_3 and Game_4. Let $\mathbf{e} = [\mathbf{e}_1^\top | \cdots | \mathbf{e}_{t+\gamma\tau}^\top]^\top \in \mathbb{Z}_q^{K_e}$ and $\mathbf{A} = [\mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_1) | \cdots | \mathsf{T}_{\mathsf{flip}}^{n+d-1,d+k+1}(a_{t+\gamma\tau})] \in \mathbb{Z}_q^{(n+2d+k-1)\times K_e}$. By Eq. (2), we have

$$
\begin{aligned}
\mathbf{A}^\top\mathbf{s} + \mathbf{e} &= \begin{bmatrix} \mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_1)^\top \\ \vdots \\ \mathsf{T}_{\mathsf{flip}}^{n+d-1,d+k+1}(a_{t+\gamma\tau})^\top \end{bmatrix} \mathbf{s} + \begin{bmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_{t+\gamma\tau} \end{bmatrix} \\
&= [\mathbf{v}_1^\top | \cdots | \mathbf{v}_{t+\gamma\tau}^\top]^\top \\
&= \mathbf{v}. \qquad (5)
\end{aligned}
$$

Let $\mathbf{U} = \mathsf{T}_{\mathsf{flip}}^{n+2d-2,k+2}(u_{\mathsf{ID}^\star}) \in \mathbb{Z}_q^{(n+2d+k-1)\times(k+2)}$. By Eq. (3), we have

$$
\begin{aligned}
\mathbf{A}\mathbf{R}_{\mathsf{ID}^\star} &= \sum_{i=1}^{t} \mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_i)\mathbf{R}_{\mathsf{ID}^\star,i} + \sum_{i=t+1}^{t+\gamma\tau} \mathsf{T}_{\mathsf{flip}}^{n+d-1,d+k+1}(a_i)\mathbf{R}_{\mathsf{ID}^\star,i} \\
&= \sum_{i=1}^{t} \mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_i)\mathsf{T}_{\mathsf{flip}}^{2d-1,k+2}(r_{\mathsf{ID}^\star,i}) \\
&\quad + \sum_{i=t+1}^{t+\gamma\tau} \mathsf{T}_{\mathsf{flip}}^{n+d+1,d+k+1}(a_i)\mathsf{T}_{\mathsf{flip}}^{d,k+2}(r_{\mathsf{ID}^\star,i}) \\
&= \mathsf{T}_{\mathsf{flip}}^{n+2d-2,k+2}\left(\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID}^\star,i}\right) \\
&= \mathbf{U}_{\mathsf{ID}^\star}. \qquad (6)
\end{aligned}
$$

With respect to the challenge ciphertext in Game_4, Eq. (5), Eq. (6), and the property of the ReRand algorithm in Lemma 5 ensure that

$$
\begin{aligned}
[\mathbf{b}_1^\top | \cdots | \mathbf{b}_{t+\gamma\tau}^\top \mid \mathbf{b}'^\top]^\top &= 2\left(2^{-1}(\mathbf{A} \cdot [\mathbf{I}_{K_e} \mid \mathbf{R}_{\mathsf{ID}^\star}])^\top\mathbf{s} + \mathbf{e}'\right) \\
&= [\mathbf{A} \mid \mathbf{U}_{\mathsf{ID}^\star}]^\top\mathbf{s} + 2\mathbf{e}' \qquad (7)
\end{aligned}
$$

and the distribution of $\mathbf{e}'$ is statistically indistinguishable from $D_{\mathbb{Z}_q^{K_e+(k+2)},\alpha' q}$. By Lemma 7 and Eq. (7), the challenge ciphertext in Game_4 $(b_i)_{i=1}^{t+\gamma\tau}$ and b' can

be written as

$$b_i = \begin{cases} a_i \odot_{2d+k} s + 2e_i & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s + 2e_i & \text{if } i \in [t+1, t+\gamma\tau] \end{cases}$$
$$b' = u^\star_{\mathsf{ID}} \odot_{k+2} s + 2e',$$

where the distribution of e_i for each $i \in [t]$, e_i for each $i \in [t+1, t+\gamma\tau]$, and e' are statistically indistinguishable from $D^{<2d+k}_{\mathbb{Z}_q,\alpha' q}[X]$, $D^{<d+k+1}_{\mathbb{Z}_q,\alpha' q}[X]$, and $D^{<k+2}_{\mathbb{Z}_q,\alpha' q}[X]$, respectively.

Thus, the challenge ciphertexts of Game_3 and Game_4 are statistically indistinguishable, and $|\Pr[E_4] - \Pr[E_3]| = \mathsf{negl}(n)$ holds.

Game_5: We change how to compute the challenge ciphertext of $\mathsf{coin} = 0$ from Game_4. Namely, we change how to compute $(v_i)_{i=1}^{t+\gamma\tau}$ in Eq. (1). In Game_5, first sample $z_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<2d+k}[X]$ and $e_i \leftarrow D^{<2d+k}_{\mathbb{Z}_q,\alpha q}[X]$ for each $i \in [t]$, and $z_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<d+k+1}[X]$ and $e_i \leftarrow D^{<d+k+1}_{\mathbb{Z}_q,\alpha q}[X]$ for each $i \in [t+1, t+\gamma\tau]$. Then, compute $v_i = z_i + e_i$ for each $i \in [t+\gamma\tau]$, run ReRand algorithm as Eq. (4), and output the challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, b' + \mathsf{m}^\star)$.

We will show that $|\Pr[E_5] - \Pr[E_4]| = \mathsf{Adv}^{\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}}_{\mathcal{B},\mathbf{QRO}_{L_{\mathcal{ID}}+\lceil\log(t+\gamma\tau)\rceil+1,\kappa}}(n)$ holds. We construct a reduction algorithm $\mathcal{B}$ which solves $\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}$ relative to the QROM using $\mathcal{A}$. $\mathcal{B}$ receives $(a_i)_{i=1}^{t+\gamma\tau}$ and $(z_i + e_i)_{i=1}^{t+\gamma\tau}$, where $z_i \in \mathbb{Z}_q^{<2d+k}[X]$ and $e_i \leftarrow D^{<2d+k}_{\mathbb{Z}_q,\alpha q}[X]$ for each $i \in [t]$ and $z_i \in \mathbb{Z}_q^{<d+k+1}[X]$ and $e_i \leftarrow D^{<d+k+1}_{\mathbb{Z}_q,\alpha q}[X]$ for each $i \in [t+1, t+\gamma\tau]$.

The task of $\mathcal{B}$ is to distinguish whether z_i is uniform or

$$z_i = \begin{cases} a_i \odot_{2d+k} s & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s & \text{if } i \in [t+1, t+\gamma\tau], \end{cases} \tag{8}$$

where $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$, $a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n}[X]$ for each $i \in [t]$, and $a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+d-1}[X]$ for each $i \in [t+1, t+\gamma\tau]$.

$\mathcal{B}$ sends $\mathsf{mpk} = (a_i)_{i=1}^{t+\gamma\tau}$ to $\mathcal{A}$. Let $\widehat{\mathsf{H}} \xleftarrow{\mathrm{U}} \mathsf{Func}(\{0,1\}^{\leq L_{\mathcal{ID}}+\lceil\log(t+\gamma\tau)\rceil+1}, \{0,1\}^\kappa)$ be a hash function chosen by $\mathcal{B}$ at the beginning of the game. Upon a secret key reveal query $\mathsf{ID} \in \mathcal{ID}$ by $\mathcal{A}$, $\mathcal{B}$ returns $r_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|i))$ for each $i \in [t+\gamma\tau]$ to $\mathcal{A}$. Upon a quantum random oracle query $\sum_{\mathsf{ID},y} \alpha_{\mathsf{ID},y} |\mathsf{ID}\rangle |y\rangle$ by $\mathcal{A}$, $\mathcal{B}$ returns $\sum_{\mathsf{ID}\,y} \alpha_{\mathsf{ID},y} |\mathsf{ID}\rangle |\mathsf{H}(\mathsf{ID}) \oplus y\rangle$, where $\mathsf{H}(\mathsf{ID}) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i}$. $\mathcal{B}$ picks $\mathsf{coin} \xleftarrow{\mathrm{U}} \{0,1\}$, and if $\mathsf{coin} = 1$, send a uniformly random ciphertext to $\mathcal{A}$. Otherwise, let $\mathbf{v} = [\mathbf{w}_1^\top + \mathbf{e}_1^\top | \cdots | \mathbf{w}_{t+\gamma\tau}^\top + \mathbf{e}_{t+\gamma\tau}^\top]^\top$ and run ReRand algorithm as Eq. (4). Then, send the challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, b' + \mathsf{m}^\star)$ to $\mathcal{A}$.

$\mathcal{A}$ returns $\widehat{\mathsf{coin}}$ as a geuss value of coin to $\mathcal{B}$. If $\mathsf{coin} = \widehat{\mathsf{coin}}$ holds, $\mathcal{B}$ outputs 1. Otherwise, outputs 0. If $(z_i)_{i=1}^{t+\gamma\tau}$ is obtained as Eq. (8), the view of $\mathcal{A}$ corresponds to Game_4. Otherwise, it corresponds to Game_5. Therefore, it holds that $|\Pr[E_5] - \Pr[E_4]| = \mathsf{Adv}^{\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}}_{\mathcal{B},\mathbf{QRO}_{L_{\mathcal{ID}}+\lceil\log(t+\gamma\tau)\rceil+1,\kappa}}(n)$.

Game_6: We change how to compute the challenge ciphertext of $\mathsf{coin} = 0$ from Game_5. In Game_6, first sample $(v_i)_{i=1}^{t+\gamma\tau} \xleftarrow{\mathrm{U}} (\mathbb{Z}_q^{<2d+k}[X])^t \times (\mathbb{Z}_q^{<d+k+1}[X])^{\gamma\tau}$, $e_i \leftarrow D_{\mathbb{Z}_q,\alpha q}^{<2d+k}[X]$ for each $i \in [t]$, $e_i \leftarrow D_{\mathbb{Z}_q,\alpha q}^{<d+k+1}[X]$ for each $i \in [t+1, t+\gamma\tau]$, and $e' \leftarrow D_{\mathbb{Z}_q,\alpha' q}^{<k+2}[X]$. Let $K_e = (2d+k)t + (d+k+1)\gamma\tau$, $\mathbf{v} = [\mathbf{v}_1^\top | \cdots | \mathbf{v}_{t+\gamma\tau}^\top]^\top$, $\mathbf{e} = [\mathbf{e}_1^\top | \cdots | \mathbf{e}_{t+\gamma\tau}^\top \mid \mathbf{e}'^\top]^\top$, and $\mathbf{R}_{\mathsf{ID}^\star}$ as specified in Eq. (3) Then, compute

$$[\mathbf{b}_1^\top | \cdots | \mathbf{b}_{t+\gamma\tau}^\top \mid \mathbf{b}'^\top]^\top = [\mathbf{I}_{K_e} \mid \mathbf{R}_{\mathsf{ID}^\star}]^\top \mathbf{v} + 2\mathbf{e}$$

and output the challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, b' + \mathsf{m}^\star)$.

As mentioned in Game_4, by Lemma 5, the challenge ciphertext of Game_5 and Game_6 are statistically indistinguishable. Therefore, it holds that $|\Pr[E_6] - \Pr[E_5]| = \mathsf{negl}(n)$.

Note that b_i can be written as $b_i = v_i + 2e_i$. Also, by Lemma 7, b' can be written as

$$b' = \sum_{i=1}^{t+\gamma\tau} r_{\mathsf{ID}^\star,i} \odot_{k+2} v_i + 2e'. \tag{9}$$

Game_7: We change how to compute the challenge ciphertext of $\mathsf{coin} = 0$ from Game_6. In Game_7, the challenge ciphertext when $\mathsf{coin} = 0$ is $((b_i)_{i=1}^{t+\gamma\tau}, b') \xleftarrow{\mathrm{U}} \mathcal{CT}$.

By the definition of IBE's security game, $\mathcal{A}$ cannot obtain $(r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau}$ by making the secret key reveal query. $\sum_{i=1}^{t+\gamma\tau} r_{\mathsf{ID},i} \odot_{k+2} v_i$ in the right hand side of Eq. (9) is statistically indistinguishable from a uniform polynomial since $\sum_{i=1}^{t} r_{\mathsf{ID}^\star,i} \cdot v_i \in \mathbb{Z}_q^{<4d+k-2}[X]$ is distributed statistically close to uniform by Lemma 4. Therefore, the challenge ciphertext of Game_6 is statistically indistinguishable from that of Game_7 and $|\Pr[E_7] - \Pr[E_6]| = \mathsf{negl}(n)$ holds.

In Game_7, both the challenge ciphertexts of $\mathsf{coin} = 0$ and $\mathsf{coin} = 1$ are random polynomials in $\mathcal{CT}$ and $\Pr[E_7] = \frac{1}{2}$ holds. Thus, we have

$$\begin{aligned}
\mathrm{Adv}^{\mathrm{IBE}}_{\text{LVV-IBE},\mathcal{A}}(n) &= |\Pr[E_0] - \frac{1}{2}| \\
&\leq \sum_{i=0}^{6} |\Pr[E_i] - \Pr[E_{i+1}]| + |\Pr[E_7] - \frac{1}{2}| \\
&\leq \mathsf{Adv}^{\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}}_{\mathcal{B},\mathbf{QRO}_{L_{\mathcal{ID}}+\lceil\log(t+\gamma\tau)\rceil+1,\kappa}}(n) + (Q_{\mathsf{H}}^2 + Q_{\mathsf{ID}}) \cdot \mathsf{negl}(n).
\end{aligned}$$

□

4 Revocable Identity-based Encryption

In this section, we review the definition of RIBE by following Katsumata et al.'s one [15] and Takayasu's one [30].

Syntax. A time space, a plaintext space, a ciphertext space, and an identity space are denoted by $\mathcal{T}$, $\mathcal{M}$, $\mathcal{CT}$, and $\mathcal{ID}$, respectively. Let $\mathsf{RL}_\mathsf{T} \subset \mathcal{ID}$ be a key revocation list for a time period $\mathsf{T} \in \mathcal{T}$. A key revocation algorithm of RIBE is

to add newly revoked identities to the revocation list. Users on the list are not deleted. An RIBE scheme Π consists of the following six algorithms.

$\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$**:** Setup algorithm takes a security parameter 1^λ as input, and outputs a master public key mpk and a master secret key msk.

$\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}) \to \mathsf{sk}_{\mathsf{ID}}$**:** SKGen algorithm takes mpk, msk, and an identity $\mathsf{ID} \in \mathcal{ID}$ as input, and outputs a secret key $\mathsf{sk}_{\mathsf{ID}}$ for the identity ID.

$\mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL}_{\mathsf{T}}) \to \mathsf{ku}_{\mathsf{T}}$**:** KeyUp algorithm takes mpk, msk, a time period $\mathsf{T} \in \mathcal{T}$, and a revocation list $\mathsf{RL}_{\mathsf{T}} \subset \mathcal{ID}$ for the time period T as input, and outputs a key update ku_{T} for the time period T.

$\mathsf{DKGen}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ku}_{\mathsf{T}}) \to \mathsf{dk}_{\mathsf{ID},\mathsf{T}} \ / \ \perp$**:** DKGen algorithm takes mpk, $\mathsf{sk}_{\mathsf{ID}}$, and ku_{T} as input. If the identity ID has not been revoked by T, this algorithm outputs a decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ for ID and T. Otherwise, this algorithm outputs $\perp$.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{T}, \mathsf{m}) \to \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$**:** Encrypt algorithm takes mpk, ID, T, and a plaintext $\mathsf{m} \in \mathcal{M}$ as input, and outputs a ciphertext $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} \in \mathcal{CT}$ for ID and T.

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}) \to \mathsf{m}'$**:** Decrypt algorithm takes mpk, $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$, and $\mathsf{ct}_{\mathsf{ID},\mathsf{T}}$ as input, and outputs a decryption result m'.

Correctness. A ciphertext $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} \in \mathcal{CT}$ for an identity ID and a time period T has to be decrypted correctly by a decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ for ID and T if ID has not been revoked by T. We consider all the possible situations of creating the decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$. Namely, for all $\lambda \in \mathbb{N}$, $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{ID} \in \mathcal{ID}$, $\mathsf{T} \in \mathcal{T}$, $\mathsf{m} \in \mathcal{M}$, and $\mathsf{RL}_{\mathsf{T}} \subset \mathcal{ID} \setminus \{\mathsf{ID}\}$, we require m' obtained by running the following algorithms to satisfy $\mathsf{m}' = \mathsf{m}$. (1) $\mathsf{sk}_{\mathsf{ID}} \leftarrow \mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID})$, (2) $\mathsf{ku}_{\mathsf{T}} \leftarrow \mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL}_{\mathsf{T}})$, (3) $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} \leftarrow \mathsf{DKGen}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ku}_{\mathsf{T}})$, (4) $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} \leftarrow \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{T}, \mathsf{m})$, and (5) $\mathsf{m}' \leftarrow \mathsf{Decrypt}(\mathsf{mpk}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}})$.

Security. The security of RIBE is defined via a security game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. This game has a global counter T_{cu} which denotes the current time period initialized with 1.

In the beginning of the security game, $\mathcal{C}$ runs $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, initializes a list SKList to $(\mathsf{ID} = \mathsf{kgc}, \mathsf{msk})$, and sets a decryption key $\mathsf{ku}_1 \leftarrow \mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T} = 1, \mathsf{RL}_1 = \phi)$ for $\mathsf{T} = 1$. Then, $\mathcal{C}$ sends mpk and ku_1 to $\mathcal{A}$. $\mathcal{A}$ may adaptively make the following four queries.

Secret Key Generation Query: Upon a query $\mathsf{ID} \in \mathcal{ID}$ by $\mathcal{A}$, $\mathcal{C}$ checks if $(\mathsf{ID}, *) \in \mathsf{SKList}$ and returns $\perp$ to $\mathcal{A}$ if this is the case. If not, $\mathcal{C}$ runs $\mathsf{sk}_{\mathsf{ID}} \leftarrow \mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID})$, adds $(\mathsf{ID}, \mathsf{sk}_{\mathsf{ID}})$ to SKList, and returns nothing to $\mathcal{A}$.
We require that all identities in the following queries except the challenge query are "activated". In other words, $\mathsf{sk}_{\mathsf{ID}}$ is generated via this query and hence $(\mathsf{ID}, \mathsf{sk}_{\mathsf{ID}}) \in \mathsf{SKList}$.

Secret Key Reveal Query: Upon a query $\mathsf{ID} \in \mathcal{ID}$ by $\mathcal{A}$, $\mathcal{C}$ finds $\mathsf{sk}_{\mathsf{ID}}$ in SKList and returns it to $\mathcal{A}$ until the challenge query. After the challenge query, $\mathcal{C}$ checks if $\mathsf{T}_{\mathsf{cu}} \geq \mathsf{T}^\star$ and $\mathsf{ID} \notin \mathsf{RL}_{\mathsf{T}^\star}$, then $\mathsf{ID} \neq \mathsf{ID}^\star$. If this is *not* the case, $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ finds $\mathsf{sk}_{\mathsf{ID}}$ in SKList and returns it.

Revoke & Key Update Query: Upon a query $\mathsf{RL} \subseteq \mathcal{ID}$ by $\mathcal{A}$, $\mathcal{C}$ checks if $\mathsf{RL}_{\mathsf{T}_{\mathsf{cu}}} \subseteq \mathsf{RL}$ until the challenge query. After the challenge query, $\mathcal{C}$ also checks if $\mathsf{T}_{\mathsf{cu}} = \mathsf{T}^\star - 1$ holds and $\mathcal{A}$ has already made the secret key reveal query on $\mathsf{ID}^\star$, then $\mathsf{ID}^\star \in \mathsf{RL}_{\mathsf{T}}$. If these conditions are *not* satisfied, $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ updates $\mathsf{T}_{\mathsf{cu}} \leftarrow \mathsf{T}_{\mathsf{cu}} + 1$ and $\mathsf{RL}_{\mathsf{T}_{\mathsf{cu}}} \leftarrow \mathsf{RL}$, runs $\mathsf{ku}_{\mathsf{T}_{\mathsf{cu}}} \leftarrow \mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL}_{\mathsf{T}_{\mathsf{cu}}})$, and returns $\mathsf{ku}_{\mathsf{T}_{\mathsf{cu}}}$.

Challenge Query: $\mathcal{A}$ is allowed to make this query only once in this game. Upon a query $(\mathsf{m}^\star, \mathsf{ID}^\star, \mathsf{T}^\star)$ by $\mathcal{A}$, $\mathcal{C}$ checks if $\mathsf{T}^\star \leq \mathsf{T}_{\mathsf{cu}}$ holds and $\mathsf{sk}_{\mathsf{ID}^\star}$ has been revealed to $\mathcal{A}$, then $\mathsf{ID} \in \mathsf{RL}_{\mathsf{T}^\star}$. If this is *not* the case, $\mathcal{C}$ returns $\perp$. Otherwise, $\mathcal{C}$ picks $\mathsf{coin} \xleftarrow{\mathrm{U}} \{0,1\}$. If $\mathsf{coin} = 0$, $\mathcal{C}$ returns $\mathsf{ct}^\star \leftarrow \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}^\star, \mathsf{T}^\star, \mathsf{m}^\star)$ to $\mathcal{A}$. If $\mathsf{coin} = 1$, $\mathcal{C}$ returns $\mathsf{ct}^\star \xleftarrow{\mathrm{U}} \mathcal{CT}$ to $\mathcal{A}$.

At some point in this game, $\mathcal{A}$ outputs $\widehat{\mathsf{coin}} \in \{0,1\}$ as a guess value of coin and terminates this game.

We say that $\mathcal{A}$ wins if $\widehat{\mathsf{coin}} = \mathsf{coin}$ holds. Let $\mathrm{Adv}^{\mathrm{RIBE}}_{\Pi,\mathcal{A}}(\lambda) = |\Pr[\widehat{\mathsf{coin}} = \mathsf{coin}] - \frac{1}{2}|$ be $\mathcal{A}$'s advantage in this game. We say that an RIBE scheme Π satisfies the adaptive anonymity if $\mathrm{Adv}^{\mathrm{RIBE}}_{\Pi,\mathcal{A}}(\lambda) = \mathsf{negl}(\lambda)$ holds for all PPT adversary $\mathcal{A}$.

5 Our RIBE Scheme

In this section, we propose an RIBE scheme. In advance, we prepare parameters, binary tree data structures, and the KUNode algorithm [25] to describe the proposed scheme. In Section 5.1, we propose our RIBE scheme. In Section 5.2, we prove the correctness of the scheme and set the parameters.

Here, we define notation to describe our RIBE scheme. Let q be a prime number, and $n = \Theta(\lambda)$, d, t, k, γ, τ, $L_{\mathcal{ID}}$, $L_{\mathcal{T}}$, and T be positive integers. Let α, α', σ be positive real numbers. The plaintext space, the identity space, the ciphertext space, and the time period space are defined as $\mathcal{M} = \{0,1\}^{k+2}$, $\mathcal{ID} = 0||\{0,1\}^{L_{\mathcal{ID}}}$, $\mathcal{CT} = (\mathbb{Z}_q^{<2d+k}[X])^t \times (\mathbb{Z}_q^{<d+k+1}[X])^{\gamma\tau} \times (\mathbb{Z}_q^{<k+2}[X])^{L_{\mathcal{ID}}+1}$, and $\mathcal{T} = \{0,1\}^{L_{\mathcal{T}}}$, respectively by following Takayasu [30]. For $\mathsf{ID} \in \mathcal{ID}$ and $\ell \in [0, L_{\mathcal{ID}}]$, let $\mathsf{ID}[0:\ell]$ be the first $\ell+1$ bits of ID. A hash function $\mathsf{H} : \{0,1\}^{\leq L_{\mathcal{ID}}+L_{\mathcal{T}}+1} \to \mathbb{Z}_q^{<n+2d-2}[X]$ will be modeled as a random oracle in the security proof.

We use a binary tree BT which has $2^{L_{\mathcal{ID}}}$ leaf nodes to manage users' identities. BT's nodes of depth ℓ are assigned $\ell+1$ bits whose first bit is 0. Especially, the root node is assigned 0. For a node assigned a bit sequence θ, the left and right child nodes are assigned $\theta\|0$ and $\theta\|1$, respectively. We note that each leaf node is assigned some identity $\mathsf{ID} \in \mathcal{ID}$. We use the KUNode algorithm [25] to realize a key revocation mechanism as known lattice-based RIBE schemes [15,30,31,32,33]. The KUNode algorithm takes a set of leaf nodes $\mathsf{RL}_{\mathsf{T}} = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_R\}$ as input and outputs a set of nodes $\mathcal{KU}_{\mathsf{T}} = \{\theta_1, \ldots \theta_r\}$ such that

- If $\mathsf{ID} \notin \mathsf{RL}_{\mathsf{T}}$ holds, there exists a unique node $\mathsf{ID}[0:\ell] \in \mathcal{KU}_{\mathsf{T}}$ for some $\ell \in [0, L_{\mathcal{ID}}]$.

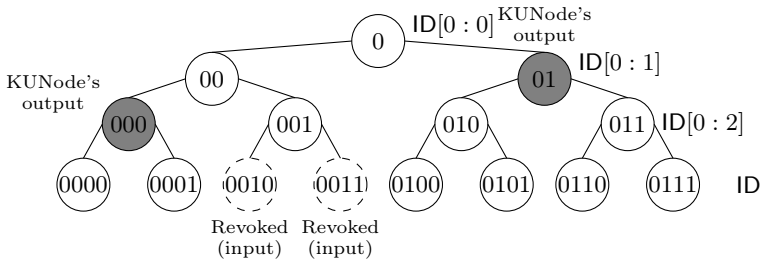

Fig. 1. Example of how identities are managed and the KUNode algorithm works

– If $\mathsf{ID} \in \mathsf{RL}_\mathsf{T}$ holds, there is no node $\mathsf{ID}[0:\ell] \in \mathcal{KU}_\mathsf{T}$ for all $\ell \in [0, L_{\mathcal{ID}}]$.

Moreover, $|\mathcal{KU}_\mathsf{T}| = O(|\mathsf{RL}_\mathsf{T}|(L_{\mathcal{ID}} - \log|\mathsf{RL}_\mathsf{T}|))$ holds.

Figure 1 illustrates how identities are managed and the KUNode algorithm works. In Figure 1, let $L_{\mathcal{ID}} = 3$. The algorithm takes a revoked identities list $\{0010, 0011\}$ as input and outputs a node list $\{01, 000\}$. For each non-revoked identity, we can find a unique node which is in the output and on the path to the corresponding leaf node.

5.1 Construction

We describe our RIBE scheme Π.

$\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$**:** Run $((a_i)_{i=1}^{t+\gamma\tau}, (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}) \leftarrow \mathsf{TrapGen}(1^n)$ and output $\mathsf{mpk} = (a_i)_{i=1}^{t+\gamma\tau}$ and $\mathsf{msk} = (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}$.

$\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}) \to \mathsf{sk}_\mathsf{ID}$**:** Let $u_\mathsf{ID} = \mathsf{H}(\mathsf{ID}\|0)$. Output $\mathsf{sk}_\mathsf{ID} = (r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau} \leftarrow \mathsf{SamplePre}(\mathsf{mpk}, \mathsf{msk}, u_\mathsf{ID}, \sigma)$. By Lemma 6, it holds that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i} = u_\mathsf{ID}$.

$\mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL}_\mathsf{T}) \to \mathsf{ku}_\mathsf{T}$**:** First, run the KUNode algorithm with input a key revocation list $\mathsf{RL}_\mathsf{T} \subset \mathcal{ID}$ and obtain $\mathcal{KU}_\mathsf{T} = \{\theta_1, \dots \theta_r\}$. Then, for each node $\theta_j \in \mathcal{KU}_\mathsf{T}$, run $(r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau} \leftarrow \mathsf{SamplePre}(\mathsf{mpk}, \mathsf{msk}, u_{\mathsf{T},\theta_j}, \sigma)$, where $u_{\mathsf{T},\theta_j} = \mathsf{H}(\theta_j\|\mathsf{T})$. Finally, output $\mathsf{ku}_\mathsf{T} = (\mathcal{KU}_\mathsf{T}, ((r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau})_{\theta_j \in \mathcal{KU}_\mathsf{T}})$. By Lemma 6, it holds that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\theta_j,i} = u_{\mathsf{T},\theta_j}$.

$\mathsf{DKGen}(\mathsf{mpk}, \mathsf{sk}_\mathsf{ID}, \mathsf{ku}_\mathsf{T}) \to \mathsf{dk}_{\mathsf{ID},\mathsf{T}} \,/\, \perp$**:** DKGen algorithm takes mpk, $\mathsf{sk}_\mathsf{ID} = (r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau}$, and $\mathsf{ku}_\mathsf{T} = (\mathcal{KU}_\mathsf{T} = \{\theta_1, \dots, \theta_r\}, ((r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau})_{\theta_j \in \mathcal{KU}_\mathsf{T}})$ as input. Then, find $\theta_j \in \mathcal{KU}_\mathsf{T}$ such that $\mathsf{ID}[0:\ell] = \theta_j$ for some $\ell \in [0, L_{\mathcal{ID}}]$. If such θ_j does not exist, output $\perp$. Otherwise, output a decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} = (d_{\mathsf{ID},\mathsf{T},i})_{i=1}^{t+\gamma\tau} = (r_{\mathsf{ID},i} + r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau}$. By Lemma 6, it holds that $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = \sum_{i=1}^{t+\gamma\tau} a_i (r_{\mathsf{ID},i} + r_{\mathsf{T},\theta_j,i}) = u_\mathsf{ID} + u_{\mathsf{T},\theta_j}$.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{T}, \mathsf{m}) \to \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$**:** Sample $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$, $e_i \leftarrow D_{\mathbb{Z}_q,\alpha' q}^{<2d+k}[X]$ for each $i \in [t]$, $e_i \leftarrow D_{\mathbb{Z}_q,\alpha' q}^{<d+k+1}[X]$ for each $i \in [t+1, t+\gamma\tau]$, and $e'_\ell \leftarrow$

$D^{<k+2}_{\mathbb{Z}_q,\alpha' q}[X]$ for $\ell \in [0, L_{\mathcal{ID}}]$. Then, compute $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} = ((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}})$;

$$b_i = \begin{cases} a_i \odot_{2d+k} s + 2e_i, & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s + 2e_i, & \text{if } i \in [t+1, t+\gamma\tau] \end{cases},$$
$$b'_\ell = \mathsf{m} + (u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}) \odot_{k+2} s + 2e'_\ell.$$

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}) \to \mathsf{m}'$**:** Find $\ell \in [0, L_{\mathcal{ID}}]$ such that $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}$ and output

$$\mathsf{m}' = \left(b'_\ell - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \mod q \right) \mod 2.$$

5.2 Correctness and Parameter Settings

The following lemma states that our scheme satisfies the correctness with overwhelming probability.

Theorem 3. *For a positive real $\alpha' < (8\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$ and a positive integer $K = t(2d-1) + \gamma\tau d$, our RIBE scheme satisfies the correctness with overwhelming probability in n.*

Proof Overview of Theorem 3. Before giving the complete proof, we first briefly sketch our proof overview.

By the property of the KUNode algorithm, each non-revoked user can find a unique node $\theta_j \in \mathcal{KU}_{\mathsf{T}}$ such that $\mathsf{ID}[0:\ell] = \theta_j$ for some $\ell \in [0, L_{\mathcal{ID}}]$. Therefore, the DKGen algorithm does not output $\perp$. When the $\mathsf{Decrypt}$ algorithm operates as specified, by Lemma 7 and the fact that $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = \sum_{i=1}^{t+\gamma\tau} a_i (r_{\mathsf{ID},i} + r_{\mathsf{T},\mathsf{ID}[0:\ell],i}) = u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}$ holds, we have

$$\begin{aligned} & b'_\ell - \sum_{i=1}^{t+\gamma\tau} b_i \odot d_{\mathsf{ID},\mathsf{T},i} \\ &= \mathsf{m} + (u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}) \odot s + 2e'_\ell - \sum_{i=1}^{t+\gamma\tau} (a_i \odot s) \odot d_{\mathsf{ID},\mathsf{T},i} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot d_{\mathsf{ID},\mathsf{T},i} \\ &= \mathsf{m} + \cancel{(u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}) \odot s} - \cancel{\sum_{i=1}^{t+\gamma\tau} (a_i d_{\mathsf{ID},\mathsf{T},i}) \odot s} + \underbrace{2 \left(e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot d_{\mathsf{ID},\mathsf{T},i} \right)}_{\text{error terms}}. \end{aligned}$$

Since the error terms are small by Lemma 2, we can recover the plaintext m.

Proof of Theorem 3. Hereafter, we provide the complete of Theorem 3 and parameter restrictions.

Proof. By the property of the KUNode algorithm, each non-revoked user can find a unique node $\theta_j \in \mathcal{KU}_{\mathsf{T}}$ such that $\mathsf{ID}[0:\ell] = \theta_j$ for some $\ell \in [0, L_{\mathcal{ID}}]$.

Therefore, the DKGen algorithm does not output $\perp$. Since $b_i = a_i \odot_{2d+k} s + 2e_i$ holds for each $i \in [t]$ and $b_i = a_i \odot_{d+k+1} s + 2e_i$ holds for each $i \in [t+1, t+\gamma\tau]$, when the $\mathsf{Decrypt}$ algorithm operates as specified, we have

$$\begin{aligned}
&b'_\ell - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&= \mathsf{m} + (u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}) \odot_{k+2} s + 2e'_\ell - \sum_{i=1}^{t} (a_i \odot_{2d+k} s) \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&\quad - \sum_{i=t+1}^{t+\gamma\tau} (a_i \odot_{d+k+1} s) \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}.
\end{aligned}$$

Then, by Lemma 7 and the fact that $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}$ holds as we explained in the DKGen algorithm, we have

$$\begin{aligned}
&\mathsf{m} + (u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}) \odot_{k+2} s + 2e'_\ell - \sum_{i=1}^{t} (a_i \odot_{2d+k} s) \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&\quad - \sum_{i=t+1}^{t+\gamma\tau} (a_i \odot_{d+k+1} s) \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&= \mathsf{m} + \cancel{(u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}) \odot_{k+2} s} + 2e'_\ell \\
&\quad - \cancel{\sum_{i=1}^{t+\gamma\tau} (a_i d_{\mathsf{ID},\mathsf{T},i}) \odot_{k+2} s} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&= \mathsf{m} + \underbrace{2 \left(e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \right)}_{\text{error terms}}.
\end{aligned}$$

If $\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty < \frac{q}{8}$ holds, the decryption of our RIBE scheme satisfies the correctness. Let

$$\begin{aligned}
&\mathbf{A} = [\mathsf{T}^{n,2d-1}(a_1) | \cdots | \mathsf{T}^{n,2d-1}(a_t) | \mathsf{T}^{n+d-1,d}(a_{t+1}) | \cdots | \mathsf{T}^{n+d-1,d}(a_{t+\gamma\tau})], \\
&\mathbf{r}_{\mathsf{ID}} = [\mathbf{r}_{\mathsf{ID},1}^\top | \cdots | \mathbf{r}_{\mathsf{ID},t+\gamma\tau}^\top]^\top, \qquad \mathbf{r}_{\mathsf{T},\mathsf{ID}[0:\ell]} = [\mathbf{r}_{\mathsf{T},\mathsf{ID}[0:\ell],1}^\top | \cdots | \mathbf{r}_{\mathsf{T},\mathsf{ID}[0:\ell],t+\gamma\tau}^\top]^\top.
\end{aligned}$$

By Lemma 6, the property of the $\mathsf{SamplePre}$ algorithm ensures that $\mathbf{r}_{\mathsf{ID}}$ and $\mathbf{r}_{\mathsf{T},\mathsf{ID}[0:\ell]}$ are distributed statistically close to $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A})}$ and $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{T},\mathsf{ID}[0:\ell]}}(\mathbf{A})}$, respectively. Therefore, by Lemma 2, it holds that

$$\begin{aligned}
&\|r_{\mathsf{ID},i}\|_\infty \le \omega(\sqrt{\log n})\sigma, \qquad &&\|r_{\mathsf{T},\mathsf{ID}[0:\ell],i}\|_\infty \le \omega(\sqrt{\log n})\sigma \\
&\|e_i\|_\infty \le \omega(\sqrt{\log n})\alpha' q, \qquad &&\|e'_\ell\|_\infty \le \omega(\sqrt{\log n})\alpha' q
\end{aligned}$$

with overwhelming probability in n. We have

$$\begin{aligned}
&\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty \\
&\leq \|e'_\ell\|_\infty + \|\sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty \\
&\leq \omega(\sqrt{\log n})\alpha' q + K(\sqrt{2}\omega(\sqrt{\log n})\sigma)(\omega(\sqrt{\log n})\alpha' q),
\end{aligned}$$

where $K = t(2d-1) + d\gamma\tau$. Thus, we have $\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty < \frac{q}{8}$ if $\alpha' < (8\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$. □

To guarantee the correctness and the adaptive anonymity of our RIBE scheme, parameters have to satisfy the following restrictions.

- For the correctness, $\alpha' < (8\sqrt{2}\omega(\log n)\sigma K + 1)^{-1}$ holds.
- By Lemma 6, $q = \mathsf{poly}(n)$, $d \leq n$, $\frac{dt}{n} = \Omega(\log n)$, $\sigma = \omega(\log^2 n)\sqrt{ndt}$, and $\gamma = \frac{n+2d-2}{d}$ hold to apply $\mathsf{TrapGen}$ and $\mathsf{SamplePre}$ algorithms properly.
- By Lemma 4, $d \leq n$, $\sigma = \omega(1)$, $q = \mathsf{poly}(n)$, $q = \omega(\sqrt{\log n})\sigma$, and $\frac{dt}{n} = \Omega(\log n)$ hold so that the master public key is statistically indistinguishable from uniform.
- By Lemma 6, $\sigma > 16\sqrt{\log 2(2d-1)/\pi}$ holds to apply $\mathsf{Sample}\mathbb{Z}$ algorithm properly.
- By Lemma 5, $\frac{\alpha'}{2\alpha} > \sqrt{2\sigma^2((2d-1)t + d\gamma\tau)(L_{\mathcal{ID}}+1)+1}$ and $\alpha q > \omega(\sqrt{\log(t(2d+k) + \gamma\tau d + (K+2)(L_{\mathcal{ID}}+1))})$ hold to apply ReRand algorithm properly.
- $\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z},\alpha q}}$ assumption holds. In other words, by Lemma 9, $q = \Omega(\alpha^{-1}n^{c+1})$ and $\mathsf{PLWE}^{(f)}_{\mathbb{Z}_q,\bar{\alpha}q}$ assumption holds for a constant $c > 0$, a polynomial $f \in \mathcal{E}(T, \mathbf{d}, n+2d+k)$ of degree $m \in [2d+k, n]$ such that $\mathrm{EF}(f) = O(n^c)$, $\bar{\alpha} = \Omega(\sqrt{m}/q)$, and $1 \geq \bar{\alpha} \geq \frac{2\sqrt{n+2d+k}}{qT}$ by Lemma 9.

We set the parameters as follows:

$$\begin{aligned}
&d = \Theta(n),\ k = \Theta(n),\ t = \log n,\ \gamma = \frac{n+2d-2}{d},\ L_{\mathcal{ID}} = \Theta(n),\ \sigma = n^{1+\mu_0}, \\
&q = n^{4.5+4\mu_0+c}\sqrt{L_{\mathcal{ID}}},\ \tau = \lceil \log q \rceil,\ \alpha' = (n^{2+2\mu_0})^{-1},\ \alpha = \left(n^{3.5+4\mu_0}\sqrt{L_{\mathcal{ID}}}\right)^{-1},
\end{aligned}$$

where $\mu_0 > 0$ can be set arbitrarily small and $c > 0$ is a parameter of the PLWE assumption.

5.3 Tight Adaptive Anonymity in the QROM

The following theorem states that our RIBE scheme Π in Section 5 satisfies the tight adaptive anonymity in the QROM.

Theorem 4. *Our RIBE scheme* Π *in Section 5 satisfies the adaptive anonymity in the QROM under the parameter settings and the* MPLWE *assumption. In particular, for any quantum adversary* $\mathcal{A}$ *making at most* Q_{H} *queries to* $|\mathsf{H}\rangle$ *and* Q_{ID} *secret key reveal queries, there exists a quantum 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*

$$\mathrm{Adv}^{\mathrm{RIBE}}_{\Pi,\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z}_q},\alpha q}}_{\mathcal{B},\mathbf{QRO}_{L_{\mathcal{ID}}+L_{\mathcal{T}}+\lceil\log(t+\gamma\tau)\rceil+1,\kappa}}(\lambda)+(Q_{\mathsf{H}}^2+Q_{\mathsf{ID}}+\sum_{\mathsf{T}\in\mathcal{T}}\#\mathsf{ku}_{\mathsf{T}})\cdot\mathsf{negl}(\lambda)$$

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* κ *denotes the length of randomness for* $\mathsf{Sample}\mathbb{Z}$*,* $\sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}$ *denotes the number of key updates created during the security game, and*

$$\mathbf{d} = \begin{cases} 2d+k & (\text{if } i \in [t]) \\ d+k+1 & (\text{if } i \in [t+1, t+\gamma\tau]). \end{cases}$$

Proof Overview of Theorem 4. Before giving the complete proof, we first briefly sketch our proof overview. Let $\mathsf{ct}^\star = ((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}})$ be a challenge ciphertext for $\mathsf{coin} = 0$. In the first step, we show that $\mathsf{ct}^\star$ for $\mathsf{coin} = 0$ is computationally indistinguishable if we replace $(b_i)_{i=1}^{t+\gamma\tau}$ with a set of uniform polynomials. In the second step, we show that $\mathsf{ct}^\star$ for $\mathsf{coin} = 0$ is statistically indistinguishable if we replace $(b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}}$ with a set of uniform polynomials.

First, we explain an overview of the first step. We do not run the $\mathsf{TrapGen}$ algorithm but sample $(a_i)_{i=1}^{t+\gamma\tau} \xleftarrow{\mathrm{U}} (\mathbb{Z}_q^{2d-1}[X])^t \times (\mathbb{Z}_q^d[X])^{\gamma\tau}$ and send $\mathsf{mpk} = (a_i)_{i=1}^{t+\gamma\tau}$ to $\mathcal{A}$ at the beginning of the game. The property of the $\mathsf{TrapGen}$ algorithm (Lemma 6) ensures that the change is statistically indistinguishable. To answer $\mathcal{A}$'s quantum random oracle query $\sum_{\mathsf{ID},y} \alpha_{\mathsf{ID},y} |\mathsf{ID}\rangle |y\rangle$, we first choose a hash function $\widehat{\mathsf{H}} \xleftarrow{\mathrm{U}} \mathsf{Func}(\{0,1\}^{\leq L_{\mathcal{ID}}+\mathcal{T}+\lceil\log(t+\gamma\tau)\rceil+1}, \{0,1\}^\kappa)$, where κ is the length of a random seed for the $\mathsf{Sample}\mathbb{Z}$ algorithm. To program $\mathsf{H}(\mathsf{ID}\|0)$ (resp. $\mathsf{H}(\theta_j\|\mathsf{T})$), we use $\widehat{\mathsf{H}}(\mathsf{ID}\|0\|i)$ (resp. $\widehat{\mathsf{H}}(\theta_j\|\mathsf{T}\|i)$) as an input random seed and run $\mathbf{r}_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|0\|i))$ (resp. $\mathbf{r}_{\mathsf{T},\theta_j,i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\theta_j\|\mathsf{T}\|i))$) for each $i \in [t+\gamma\tau]$. Then, we set $\mathsf{H}(\mathsf{ID}\|0) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i}$ (resp. $\mathsf{H}(\theta_j\|\mathsf{T}) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\theta_j,i}$). Lemma 4 ensures that the change is statistically indistinguishable. To create $\mathsf{sk}_{\mathsf{ID}} = (r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau}$ (resp. $(r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau} \in \mathsf{ku}_{\mathsf{T}}$), we use the above $\mathbf{r}_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|0\|i))$ (resp. $\mathbf{r}_{\mathsf{T},\theta_j,i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\theta_j\|\mathsf{T}\|i))$) for each $i \in [t+\gamma\tau]$. Lemma 4 and the property of the $\mathsf{SamplePre}$ algorithm (Lemma 6) ensure that the change is statistically indistinguishable. To answer the challenge query on $(\mathsf{m}^\star, \mathsf{ID}^\star, \mathsf{T}^\star)$, we replace $(b_i)_{i=1}^{t+\gamma\tau}$ with a set of uniform polynomials if $\mathsf{coin} = 0$. The MPLWE assumption ensures that the change is computationally indistinguishable. Finally, we use $\mathsf{sk}_{\mathsf{ID}^\star} = (r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau}$ and $(r_{\mathsf{T}^\star,\mathsf{ID}^\star[0:\ell],i})_{i=1}^{t+\gamma\tau}$, and set b'_ℓ for $\ell \in [0, L_{\mathcal{ID}}]$ by computing

$$b'_\ell = \sum_{i=1}^{t+\gamma\tau} (r_{\mathsf{ID}^\star,i} + r_{\mathsf{T},\mathsf{ID}^\star[0:\ell],i}) \odot_{k+2} b_i + 2e'_\ell.$$

The property of the ReRand algorithm (Lemma 5) ensures that the change is statistically indistinguishable. Thus, we can replace $(b_i)_{i=1}^{t+\gamma\tau}$ with a set of uniform polynomials.

Next, we explain an overview of the second step. For this purpose, we divide $\mathcal{A}$'s attack strategy into two types depending on whether $\mathcal{A}$ receives $\mathsf{sk}_{\mathsf{ID}^\star}$ by making a secret key reveal query. If $\mathcal{A}$ receives $\mathsf{sk}_{\mathsf{ID}^\star}$, the security definition of RIBE ensures that $\mathsf{ID}^\star$ is revoked by $\mathsf{T}^\star$. Then, the property of the KUNode algorithm ensures that $\mathcal{A}$ cannot receive $(r_{\mathsf{T}^\star,\mathsf{ID}^\star[0:\ell],i})_{i=1}^{t+\gamma\tau}$ for $\ell \in [0, L_{\mathcal{ID}}]$ by making revoke and key update queries. Thus, each $\sum_{i=1}^{t+\gamma\tau} r_{\mathsf{T},\mathsf{ID}^\star[0:\ell],i} \odot_{k+2} b_i + 2e'_\ell$ for $\ell \in [0, L_{\mathcal{ID}}]$ is indistinguishable from uniform due to the entropy of each $(r_{\mathsf{T}^\star,\mathsf{ID}^\star[0:\ell],i})_{i=1}^{t+\gamma\tau}$. Therefore, we can replace $(b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}}$ with a set of uniform polynomials. If $\mathcal{A}$ does not receive $\mathsf{sk}_{\mathsf{ID}^\star}$, the property of the KUNode algorithm ensures that there is $(r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell^\star],i})_{i=1}^{t+\gamma\tau}$ for a unique $\ell^\star \in [0, L_{\mathcal{ID}}]$ which $\mathcal{A}$ receives by making a revoke and key update query. In other words, $\mathcal{A}$ cannot receive $(r_{\mathsf{T}^\star,\mathsf{ID}^\star[0:\ell],i})_{i=1}^{t+\gamma\tau}$ for $\ell \in [0, L_{\mathcal{ID}}] \setminus \{\ell^\star\}$. Thus, each $\sum_{i=1}^{t+\gamma\tau} r_{\mathsf{T},\mathsf{ID}^\star[0:\ell],i} \odot_{k+2} b_i + 2e'_\ell$ for $\ell \in [0, L_{\mathcal{ID}}] \setminus \{\ell^\star\}$ is indistinguishable from uniform due to the entropy of each $(r_{\mathsf{T}^\star,\mathsf{ID}^\star[0:\ell],i})_{i=1}^{t+\gamma\tau}$. Therefore, we can replace $(b'_\ell)_{\ell \in [0,L_{\mathcal{ID}}]\setminus\{\ell^\star\}}$ with a set of uniform polynomials. Finally, $\sum_{i=1}^{t+\gamma\tau} r_{\mathsf{ID}^\star,i} \odot_{k+2} b_i + 2e'_{\ell^\star}$ is indistinguishable from uniform due to the entropy of $\mathsf{sk}_{\mathsf{ID}^\star} = (r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau}$. Therefore, we can also replace $b'_{\ell^\star}$ with a set of uniform polynomials.

Proof of Theorem 4. Hereafter, we provide the complete proof of Theorem 4.

Proof. We show the tight adaptive anonymity of our RIBE scheme via the following security games. Let E_i denote an event that $\mathcal{A}$ wins in game i.

Game_0: Game_0 is the original security game. The challenger $\mathcal{C}$ chooses a hash function $\mathsf{H} : \{0,1\}^{\leq L_{\mathcal{ID}}+L_{\mathcal{T}}+1} \to \mathbb{Z}_q^{<n+2d-2}[X]$ at the beginning of the game. Upon a quantum random oracle query $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y} |\mathsf{ID}\|\mathsf{T}\rangle |y\rangle$ by the adversary $\mathcal{A}$, $\mathcal{C}$ returns $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y} |\mathsf{ID}\|\mathsf{T}\rangle |\mathsf{H}(\mathsf{ID}\|\mathsf{T}) \oplus y\rangle$.

Game_1: We change how to answer the quantum random oracle queries from Game_0. In Game_1, $\mathcal{C}$ chooses a function $\widehat{\mathsf{H}} \xleftarrow{\mathrm{U}} \mathsf{Func}(\{0,1\}^{\leq L_{\mathcal{ID}}+L_{\mathcal{T}}+\lceil \log(t+\gamma\tau)\rceil+1}, \{0,1\}^\kappa)$ at the beginning of the game. With respect to $\mathsf{H}(\mathsf{ID}\|0)$, sample coefficient vectors $\mathbf{r}_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|0\|i))$ for each $i \in [t+\gamma\tau]$ and compute $\mathsf{H}(\mathsf{ID}\|0) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i}$. With respect to $\mathsf{H}(\theta_j\|\mathsf{T})$, sample coefficient vectors $\mathbf{r}_{\mathsf{T},\theta_j,i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\theta_j\|\mathsf{T}\|i))$ for each $i \in [t+\gamma\tau]$ and compute $\mathsf{H}(\theta_j\|\mathsf{T}) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\theta_j,i}$. Here, $\mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|0\|i))$ and $\mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\theta_j\|\mathsf{T}\|i))$ denote running $\mathsf{Sample}\mathbb{Z}(\sigma)$ with $\widehat{\mathsf{H}}(\mathsf{ID}\|0\|i)$ and $\widehat{\mathsf{H}}(\theta_j\|\mathsf{T}\|i)$ as input random seeds, respectively.

By Lemma 4, $\mathsf{H}(\mathsf{ID}\|0)$ and $\mathsf{H}(\theta_j\|\mathsf{T})$ are statistically indistinguishable from uniform. Therefore, Lemma 1 ensures that $|\Pr[E_0] - \Pr[E_1]| = \mathsf{negl}(n) + 4Q_{\mathsf{H}}^2\sqrt{\mathsf{negl}(n)} = Q_{\mathsf{H}}^2 \cdot \mathsf{negl}(n)$, where Q_{H} is the number of random oracle queries.

Game_2: We change how to generate a secret key $(r_{\mathsf{ID},i})_{i=1}^{t+\gamma\tau}$ and a key update $(r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau}$ from Game_1. In Game_2, we do not use $\mathsf{SamplePre}$ algorithm. Instead, upon a secret key reveal query of ID, return $\mathbf{r}_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|0\|i))$ for

each $i \in [t+\gamma\tau]$ to $\mathcal{A}$. Similarly, upon a key update query of (θ_j, T), return $\mathbf{r}_{\mathsf{T},\theta_j,i} \leftarrow \mathsf{SampleZ}(\sigma; \widehat{\mathsf{H}}(\theta_j \| \mathsf{T} \| i))$ for each $i \in [t+\gamma\tau]$.

Let $\mathbf{A} = [\mathsf{T}^{n,2d-1}(a_1)| \cdots |\mathsf{T}^{d,n+d-1}(a_{t+\gamma\tau})]$. By Lemma 6, the property of the $\mathsf{SamplePre}$ algorithm ensures that $\mathbf{r}_{\mathsf{ID}} = [\mathbf{r}_{\mathsf{ID},1}^\top | \cdots | \mathbf{r}_{\mathsf{ID},t+\gamma\tau}^\top]^\top$ of Game_1 is statistically indistinguishable from the discrete Gaussian distribution $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A}),\sigma}$. Moreover, by Lemma 4, $\mathbf{r}_{\mathsf{ID}} = [\mathbf{r}_{\mathsf{ID},1}^\top | \cdots | \mathbf{r}_{\mathsf{ID},t+\gamma\tau}^\top]^\top$ of Game_2 is also statistically indistinguishable from $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID}}}(\mathbf{A}),\sigma}$. Similarly, the distributions of $\mathbf{r}_{\mathsf{T},\theta_j} = [\mathbf{r}_{\mathsf{T},\theta_j,1}^\top | \cdots | \mathbf{r}_{\mathsf{T},\theta_j,t+\gamma\tau}^\top]^\top$ in Game_1 and Game_2 are statistically indistinguishable from $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{T},\theta_j}}(\mathbf{A}),\sigma}$. Since $\mathcal{A}$ obtains $\sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}$ key updates and at most Q_{ID} secret keys during the game, we have $|\Pr[E_2] - \Pr[E_1]| = (Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}) \cdot \mathsf{negl}(n)$.

Game_3: We change how to generate the master public key from Game_2. In Game_3, the master public key is chosen by running $(a_i)_{i=1}^{t+\gamma\tau} \xleftarrow{\mathrm{U}} (\mathbb{Z}_q^n[X])^t \times (\mathbb{Z}_q^{n+d-1}[X])^{\gamma\tau}$.

By Lemma 6, the property of the $\mathsf{TrapGen}$ algorithm ensures that mpk of Game_2 is statistically indistinguishable from uniform, therefore $|\Pr[E_3] - \Pr[E_2]| = \mathsf{negl}(n)$ holds.

Game_4: We change how to compute the challenge ciphertext of $\mathsf{coin} = 0$ from Game_3. Let $K_e = t(2d+k) + \gamma\tau(d+k+1)$. In Game_4, first, sample $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$, $e_i \leftarrow D_{\mathbb{Z}_q,\alpha q}^{<2d+k}[X]$ for each $i \in [t]$, and $e_i \leftarrow D_{\mathbb{Z}_q,\alpha q}^{<d+k+1}[X]$ for each $i \in [t+1, t+\gamma\tau]$. Then, compute

$$v_i = \begin{cases} a_i \odot_{2d+k} s + e_i & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s + e_i & \text{if } i \in [t+1, t+\gamma\tau]. \end{cases} \tag{10}$$

By Eq. (10) and Lemma 7, we have

$$\mathbf{v}_i = \begin{cases} \mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_i)^\top \mathbf{s} + \mathbf{e}_i & \text{if } i \in [t] \\ \mathsf{T}_{\mathsf{flip}}^{n+d-1,d+k+1}(a_i)^\top \mathbf{s} + \mathbf{e}_i & \text{if } i \in [t+1, t+\gamma\tau]. \end{cases} \tag{11}$$

Let $\mathbf{v} = [\mathbf{v}_1^\top | \cdots | \mathbf{v}_{t+\gamma\tau}^\top]^\top \in \mathbb{Z}_q^{K_e}$ and

$$\begin{aligned} &\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell,i} \\ &= \begin{cases} \mathsf{T}_{\mathsf{flip}}^{2d-1,k+2}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i}) \in \mathbb{Z}_q^{(2d+k)\times(k+2)} & \text{if } i \in [t] \\ \mathsf{T}_{\mathsf{flip}}^{d,k+2}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i}) \in \mathbb{Z}_q^{(d+k+1)\times(k+2)} & \text{if } i \in [t+1, t+\gamma\tau] \end{cases} \\ &\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell} = \begin{bmatrix} \mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell,1} \\ \vdots \\ \mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell,t+\gamma\tau} \end{bmatrix} \in \mathbb{Z}_q^{K_e\times(k+2)} \quad (\ell \in [0, L_{\mathcal{ID}}]). \end{aligned} \tag{12}$$

Then, run

$$[\mathbf{b}_0| \cdots |\mathbf{b}_{t+\gamma\tau}|\mathbf{b}'_1| \cdots |\mathbf{b}'_{L_{\mathcal{ID}}}]$$

$$\leftarrow 2 \cdot \mathsf{ReRand}\left(2^{-1}[\mathbf{I}_{K_e} \mid \mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,0}|\cdots|\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,L_{\mathcal{ID}}}], \mathbf{v}, \alpha q, \frac{\alpha'}{2\alpha}\right) \tag{13}$$

and output the challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell + \mathsf{m}^\star)_{\ell=0}^{L_{\mathcal{ID}}})$.

We will show that the ReRand algorithm can be applied properly. There is a restriction on the maximum singular value of the ReRand algorithm's input matrix, therefore we will evaluate it. We have

$$\begin{aligned} s_1([\mathbf{I}_{K_e} \mid \mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,0}|\cdots|\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,L_{\mathcal{ID}}}])^2 &\le \sum_{\ell=0}^{L_{\mathcal{ID}}} s_1(\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell})^2 + 1 \\ &\le \sum_{\ell=0}^{L_{\mathcal{ID}}} \sum_{i=1}^{t+\gamma\tau} s_1(\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell,i})^2 + 1 \end{aligned}$$

and

$$\begin{aligned} s_1(\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell,i})^2 &= \max_{\|\mathbf{h}\|=1} \|\mathsf{T}^{2d-1,k+2}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i})\|\mathbf{h}^2 \\ &= \max_{\|\mathbf{h}\|=1} \|\mathsf{T}^{2d-1,k+2}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i})\mathsf{T}^{k+2,1}(h)\|^2 \\ &= \max_{\|\mathbf{h}\|=1} \|\mathsf{T}^{2d+k,1}((r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i})h)\|^2 \\ &\le \|\mathbf{r}_{\mathsf{ID}^\star,i}\|^2 + \|\mathbf{r}_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i}\|^2 \\ &\le 2\sigma^2(2d-1) \end{aligned}$$

for each $i \in [t]$. By a similar argument for each $i \in [t+1, t+\gamma\tau]$, it follows that if $\frac{\alpha'}{2\alpha} > \sqrt{2\sigma^2((2d-1)t + d\gamma\tau)(L_{\mathcal{ID}}+1)+1}$ holds, ReRand algorithm can be applied properly.

We will show that the challenge ciphertext is statistically indistinguishable between Game_3 and Game_4. Let $\mathbf{e} = [\mathbf{e}_1^\top|\cdots|\mathbf{e}_{t+\gamma\tau}^\top]^\top \in \mathbb{Z}_q^{K_e}$ and $\mathbf{A} = [\mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_1)|\cdots|\mathsf{T}_{\mathsf{flip}}^{n+d-1,d+k+1}(a_{t+\gamma\tau})] \in \mathbb{Z}_q^{(n+2d+k-1)\times K_e}$. By Eq. (11), we have

$$\begin{aligned} \mathbf{A}^\top\mathbf{s} + \mathbf{e} &= \begin{bmatrix} \mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_1)^\top \\ \vdots \\ \mathsf{T}_{\mathsf{flip}}^{n+d-1,d+k+1}(a_{t+\gamma\tau})^\top \end{bmatrix}\mathbf{s} + \begin{bmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_{t+\gamma\tau} \end{bmatrix} \\ &= [\mathbf{v}_1^\top|\cdots|\mathbf{v}_{t+\gamma\tau}^\top]^\top = \mathbf{v}. \end{aligned} \tag{14}$$

Let

$$\begin{aligned} \mathbf{U}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell} &= \mathsf{T}_{\mathsf{flip}}^{n+2d-2,k+2}(u_{\mathsf{ID}^\star} + u_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell]}) \\ &\in \mathbb{Z}_q^{(n+2d+k-1)\times(k+2)} \quad (\ell \in [0, L_{\mathcal{ID}}]). \end{aligned}$$

By Eq. (12), we have

$$\mathbf{A}\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell} = \sum_{i=1}^{t} \mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_i)\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell,i} + \sum_{i=t+1}^{t+\gamma\tau} \mathsf{T}_{\mathsf{flip}}^{n+d-1,d+k+1}(a_i)\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell,i}$$

$$
\begin{aligned}
&= \sum_{i=1}^{t} \mathsf{T}_{\mathsf{flip}}^{n,2d+k}(a_i)\mathsf{T}_{\mathsf{flip}}^{2d-1,k+2}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i}) \\
&\quad + \sum_{i=t+1}^{t+\gamma\tau} \mathsf{T}_{\mathsf{flip}}^{n+d+1,d+k+1}(a_i)\mathsf{T}_{\mathsf{flip}}^{d,k+2}(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i}) \\
&= \mathsf{T}_{\mathsf{flip}}^{n+2d-2,k+2}\left(\sum_{i=1}^{t+\gamma\tau} a_i(r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i})\right) \\
&= \mathbf{U}_{\mathsf{ID}^\star,\mathsf{T}^\star,\ell} \qquad (15)
\end{aligned}
$$

for each $\ell \in [0, L_{\mathcal{ID}}]$. Eq. (13), Eq. (14), Eq. (15), and the property of the ReRand algorithm in Lemma 5 ensure that

$$
\begin{aligned}
&[\mathbf{b}_1|\cdots|\mathbf{b}_{t+\gamma\tau}|\mathbf{b}'_0|\cdots|\mathbf{b}'_{L_{\mathcal{ID}}}] \\
&= 2\left(2^{-1}\left(\mathbf{A}\cdot[\mathbf{I}_{K_e} \mid \mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,0}|\cdots|\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,L_{\mathcal{ID}}}]\right)^\top \mathbf{s} + \mathbf{e}'\right) \\
&= [\mathbf{A} \mid \mathbf{U}_{\mathsf{ID}^\star,\mathsf{T}^\star,0}|\cdots|\mathbf{U}_{\mathsf{ID}^\star,\mathsf{T}^\star,L_{\mathcal{ID}}}]^\top \mathbf{s} + 2\mathbf{e}' \qquad (16)
\end{aligned}
$$

and the distribution of $\mathbf{e}'$ is statistically indistinguishable from $D_{\mathbb{Z}_q^{K_e+(k+2)(L_{\mathcal{ID}}+1)},\alpha' q}$. By Lemma 7 and Eq. (16), the challenge ciphertext in Game_4 $(b_i)_{i=1}^{t+\gamma\tau}$ and $(b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}}$ can be written as

$$
\begin{aligned}
b_i &= \begin{cases} a_i \odot_{2d+k} s + 2e_i & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s + 2e_i & \text{if } i \in [t+1, t+\gamma\tau] \end{cases} \\
b'_\ell &= (u_{\mathsf{ID}^\star} + u_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell]}) \odot_{k+2} s + 2e'_\ell \quad (\ell \in [0, L_{\mathcal{ID}}]),
\end{aligned}
$$

where the distribution of e_i for each $i \in [t]$, e_i for each $i \in [t+1, t+\gamma\tau]$, and e'_ℓ for each $\ell \in [0, L_{\mathcal{ID}}]$ are statistically indistinguishable from $D^{<2d+k}_{\mathbb{Z}_q,\alpha' q}[X]$, $D^{<d+k+1}_{\mathbb{Z}_q,\alpha' q}[X]$, and $D^{<k+2}_{\mathbb{Z}_q,\alpha' q}[X]$, respectively.

Thus, the challenge ciphertexts of Game_3 and Game_4 are statistically indistinguishable, thus $|\Pr[E_4] - \Pr[E_3]| = \mathsf{negl}(n)$ holds.

Game_5: We change how to compute the challenge ciphertext of $\mathsf{coin} = 0$ from Game_4. Namely, we change how to compute $(v_i)_{i=1}^{t+\gamma\tau}$ in Eq. (10). In Game_5, first sample $z_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<2d+k}[X]$ and $e_i \leftarrow D^{<2d+k}_{\mathbb{Z}_q,\alpha q}[X]$ for each $i \in [t]$, and $z_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<d+k+1}[X]$ and $e_i \leftarrow D^{<d+k+1}_{\mathbb{Z}_q,\alpha q}[X]$ for each $i \in [t+1, t+\gamma\tau]$. Then, compute $v_i = z_i + e_i$ for each $i \in [t+\gamma\tau]$, run ReRand algorithm as Eq. (13), and output the challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell + \mathsf{m}^\star)_{\ell=0}^{L_{\mathcal{ID}}})$.

We will show that $|\Pr[E_5] - \Pr[E_4]| = \mathsf{Adv}^{\mathsf{MPLWE}_{q,n,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}}_{\mathcal{B},\mathbf{QRO}_{L_{\mathcal{ID}}+L_{\mathcal{T}}+\lceil\log(t+\gamma\tau)\rceil+1,\kappa}}(n)$ holds. We construct a reduction algorithm $\mathcal{B}$ which solves $\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}$ relative to the QROM using $\mathcal{A}$. $\mathcal{B}$ receives $(a_i)_{i=1}^{t+\gamma\tau}$ and $(z_i + e_i)_{i=1}^{t+\gamma\tau}$, where $z_i \in \mathbb{Z}_q^{<2d+k}[X], e_i \leftarrow D^{<2d+k}_{\mathbb{Z}_q,\alpha q}[X]$ for each $i \in [t]$ and $z_i \in \mathbb{Z}_q^{<d+k+1}[X], e_i \leftarrow D^{<d+k+1}_{\mathbb{Z}_q,\alpha q}[X]$ for each $i \in [t+1, t+\gamma\tau]$.

The task of $\mathcal{B}$ is to distinguish whether z_i is uniform or

$$z_i = \begin{cases} a_i \odot_{2d+k} s & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s & \text{if } i \in [t+1, t+\gamma\tau], \end{cases} \tag{17}$$

where $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$, $a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n}[X]$ for each $i \in [t]$, and $a_i \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+d-1}[X]$ for each $i \in [t+1, t+\gamma\tau]$.

$\mathcal{B}$ sends $\mathsf{mpk} = (a_i)_{i=1}^{t+\gamma\tau}$ to $\mathcal{A}$. Let $\widehat{\mathsf{H}} \xleftarrow{\mathrm{U}} \mathsf{Func}(\{0,1\}^{\leq L_{\mathcal{ID}}+L_{\mathcal{T}}+\lceil\log(t+\gamma\tau)\rceil+1}, \{0,1\}^{\kappa})$ be a hash function chosen by $\mathcal{B}$ at the beginning of the game. Upon a secret key reveal query $\mathsf{ID} \in \mathcal{ID}$ by $\mathcal{A}$, $\mathcal{B}$ returns $r_{\mathsf{ID},i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\mathsf{ID}\|0\|i))$ for each $i \in [t+\gamma\tau]$ to $\mathcal{A}$. Upon a revoke and key update query $\mathsf{RL}_{\mathsf{T}} \subset \mathcal{ID}$ by $\mathcal{A}$, $\mathcal{B}$ runs the KUNode algorithm and obtains $\mathcal{KU}_{\mathsf{T}} = \{\theta_1, \ldots, \theta_r\}$. Then, $\mathcal{B}$ returns $r_{\mathsf{T},\theta_j,i} \leftarrow \mathsf{Sample}\mathbb{Z}(\sigma; \widehat{\mathsf{H}}(\theta_j\|\mathsf{T}\|i))$ for each $(i, \theta_j) \in [t+\gamma\tau] \times \mathcal{KU}_{\mathsf{T}}$ to $\mathcal{A}$. Upon a quantum random oracle query $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y} |\mathsf{ID}\|\mathsf{T}\rangle |y\rangle$ by $\mathcal{A}$, $\mathcal{B}$ returns $\sum_{\mathsf{ID}\|\mathsf{T},y} \alpha_{\mathsf{ID}\|\mathsf{T},y} |\mathsf{ID}\|\mathsf{T}\rangle |\mathsf{H}(\mathsf{ID}\|\mathsf{T}) \oplus y\rangle$, where $\mathsf{H}(\mathsf{ID}\|\mathsf{T} = 0) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},i}$ and $\mathsf{H}(\mathsf{ID}\|\mathsf{T} > 1) = \sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\mathsf{ID},i}$. $\mathcal{B}$ picks $\mathsf{coin} \xleftarrow{\mathrm{U}} \{0,1\}$, and if $\mathsf{coin} = 1$, send a uniformly random ciphertext to $\mathcal{A}$. Otherwise, let $\mathbf{v} = [\mathbf{w}_1^\top + \mathbf{e}_1^\top | \cdots | \mathbf{w}_{t+\gamma\tau}^\top + \mathbf{e}_{t+\gamma\tau}^\top]^\top$ and run ReRand algorithm as Eq. (13). Then, send the challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell + \mathsf{m}^\star)_{\ell=0}^{L_{\mathcal{ID}}})$ to $\mathcal{A}$.

$\mathcal{A}$ returns $\widehat{\mathsf{coin}}$ as a geuss value of coin to $\mathcal{B}$. If $\mathsf{coin} = \widehat{\mathsf{coin}}$, $\mathcal{B}$ outputs 1. Otherwise, outputs 0. If $(z_i)_{i=1}^{t+\gamma\tau}$ is obtained as Eq. (17), the view of $\mathcal{A}$ corresponds to Game_4. Otherwise, it corresponds to Game_5. Therefore, it holds that $|\Pr[E_5] - \Pr[E_4]| = \mathsf{Adv}^{\mathsf{MPLWE}_{q,n,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}}_{\mathcal{B},\mathbf{QRO}_{L_{\mathcal{ID}}+L_{\mathcal{T}}+\lceil\log(t+\gamma\tau)\rceil+1,\kappa}}(n)$.

Game_6: We change how to compute the challenge ciphertext of $\mathsf{coin} = 0$ from Game_5. In Game_6, first sample $(v_i)_{i=1}^{t+\gamma\tau} \xleftarrow{\mathrm{U}} (\mathbb{Z}_q^{<2d+k}[X])^t \times (\mathbb{Z}_q^{<d+k+1}[X])^{\gamma\tau}$, $e_i \leftarrow D_{\mathbb{Z}_q,\alpha' q}^{<2d+k}[X]$ for each $i \in [t]$, $e_i \leftarrow D_{\mathbb{Z}_q,\alpha' q}^{<d+k+1}[X]$ for each $i \in [t+1, t+\gamma\tau]$, and $e'_\ell \leftarrow D_{\mathbb{Z}_q,\alpha' q}^{<k+2}[X]$ for each $\ell \in [0, L_{\mathcal{ID}}]$. Let $K_e = t(2d+k) + \gamma\tau(d+k+1)$, $\mathbf{v} = [\mathbf{v}_1^\top | \cdots | \mathbf{v}_{t+\gamma\tau}^\top]^\top \in \mathbb{Z}_q^{K_e}$, $\mathbf{e} = [\mathbf{e}_1^\top | \cdots | \mathbf{e}_{t+\gamma\tau}^\top | \mathbf{e}_0'^\top | \cdots | \mathbf{e}_{L_{\mathcal{ID}}}'^\top]^\top \in \mathbb{Z}_q^{K_e+(L_{\mathcal{ID}}+1)(k+2)}$, and $\mathbf{R}_{\mathsf{ID}^\star,\mathsf{T},\ell} \in \mathbb{Z}_q^{K_e \times (k+2)}$ as specified in Eq. (12). Then, compute

$$\begin{aligned} &[\mathbf{b}_1^\top | \cdots | \mathbf{b}_{t+\gamma\tau}^\top | \mathbf{b}_0'^\top | \cdots | \mathbf{b}_{L_{\mathcal{ID}}}'^\top]^\top \\ &= [\mathbf{I}_{K_e} \mid \mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,0} | \cdots | \mathbf{R}_{\mathsf{ID}^\star,\mathsf{T}^\star,L_{\mathcal{ID}}}]^\top \mathbf{v} + 2\mathbf{e} \end{aligned}$$

and output the challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell + \mathsf{m}^\star)_{\ell=0}^{L_{\mathcal{ID}}})$.

As mentioned in Game_4, by Lemma 5, the challenge ciphertext of Game_5 and Game_6 are statistically indistinguishable. Therefore, it holds that $|\Pr[E_6] - \Pr[E_5]| = \mathsf{negl}(n)$.

Note that b_i can be written as $b_i = v_i + 2e_i$. Also, by Lemma 7, b'_ℓ can be written as

$$b'_\ell = \sum_{i=1}^{t+\gamma\tau} (r_{\mathsf{ID}^\star,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i}) \odot_{k+2} v_i + 2e'_\ell. \tag{18}$$

Game_7: We change how to compute the challenge ciphertext of $\mathsf{coin} = 0$ from Game_6. In Game_7, the challenge ciphertext when $\mathsf{coin} = 0$ is $((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}}) \xleftarrow{\mathrm{U}} \mathcal{CT}$. We will show that the challenge ciphertext of Game_6 and Game_7 is statistically indistinguishable.

If $\mathsf{ID}^\star \in \mathsf{RL}_{\mathsf{T}^\star}$, $\mathcal{A}$ cannot obtain $(r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i})_{i=1}^{t+\gamma\tau}$ in the key update $\mathsf{ku}_{\mathsf{T}^\star}$ for each $\ell \in [0, L_{\mathcal{ID}}]$ by the property of KUNode algorithm. For each $\ell \in [0, L_{\mathcal{ID}}]$, a statistical distance between a distribution of

$$\left((v_i)_{i=1}^{t+\gamma\tau}, \sum_{i=1}^{t+\gamma\tau} r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i} \odot_{k+2} v_i\right)$$

in Eq. (18) and a uniform distribution is $\mathsf{negl}(n)$ since

$$\left((v_i)_{i=1}^{t+\gamma\tau}, \sum_{i=1}^{t} r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i} \cdot v_i \in \mathbb{Z}_q^{<4d+k-2}[X]\right)$$

is distributed statistically close to uniform by Lemma 4. Therefore, a statistical distance between a distribution of

$$\left((v_i)_{i=1}^{t+\gamma\tau}, \left(\sum_{i=1}^{t+\gamma\tau} r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i} \odot_{k+2} v_i\right)_{\ell=0}^{L_{\mathcal{ID}}}\right)$$

and a uniform distribution is $(L_{\mathcal{ID}} + 1) \cdot \mathsf{negl}(n) = \mathsf{negl}(n)$. Thus, challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}})$ in Game_6 is statistically indistinguishable from the challenge ciphertext in Game_7.

If $\mathsf{ID}^\star \notin \mathsf{RL}_{\mathsf{T}^\star}$, by the definition of RIBE's security game, $\mathcal{A}$ cannot obtain $\mathsf{sk}_{\mathsf{ID}^\star} = (r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau}$ by making the secret key reveal query. Furthermore, the property of the KUNode algorithm ensures that $\mathcal{A}$ receives the key update $(r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell'],i})_{i=1}^{t+\gamma\tau}$ for only one $\ell' \in [0, L_{\mathcal{ID}}]$. By a discussion similar to that of $\mathsf{ID}^\star \in \mathsf{RL}_{\mathsf{T}^\star}$, for $\ell \in [0, L_{\mathcal{ID}}] \setminus \{\ell'\}$, a statistical distance between a distribution of $\left((v_i)_{i=1}^{t+\gamma\tau}, \sum_{i=1}^{t+\gamma\tau} r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i} \odot_{k+2} v_i\right)$ and a uniform distribution is $\mathsf{negl}(n)$. Similarly, a statistical distance between a distribution of $\left((v_i)_{i=1}^{t+\gamma\tau}, \sum_{i=1}^{t+\gamma\tau} r_{\mathsf{ID}^\star,i} \odot_{k+2} v_i\right)$ and a uniform distribution is $\mathsf{negl}(n)$. Therefore, the statistical distance between a distribution of

$$\left((v_i)_{i=1}^{t+\gamma\tau}, \sum_{i=1}^{t+\gamma\tau} r_{\mathsf{ID}^\star,i} \odot_{k+2} v_i, \left(\sum_{i=1}^{t+\gamma\tau} r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i} \odot_{k+2} v_i\right)_{\ell\in[0,L_{\mathcal{ID}}]\setminus\{\ell'\}}\right)$$

and a uniform distribution is $(L_{\mathcal{ID}} + 1) \cdot \mathsf{negl}(n) = \mathsf{negl}(n)$. Thus, challenge ciphertext $((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}})$ in Game_6 is statistically indistinguishable from the challenge ciphertext in Game_7. Therefore, $|\Pr[E_7] - \Pr[E_6]| = \mathsf{negl}(n)$ holds.

In Game_7, both the challenge ciphertexts of $\mathsf{coin} = 0$ and $\mathsf{coin} = 1$ are random samples in $\mathcal{CT}$ and $\Pr[E_7] = \frac{1}{2}$ holds. Thus, we have

$$\mathrm{Adv}^{\mathrm{RIBE}}_{\Pi,\mathcal{A}}(n) = |\Pr[E_0] - \frac{1}{2}|$$

$$\leq \sum_{i=0}^{6} |\Pr[E_i] - \Pr[E_{i+1}]| + |\Pr[E_7] - \frac{1}{2}|$$
$$\leq \mathsf{Adv}^{\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z}_q,\alpha q}}}_{\mathcal{B},\mathbf{QRO}_{L_{\mathcal{ID}}+L_{\mathcal{T}}+\lceil \log(t+\gamma\tau)\rceil+1,\kappa}}(n) + (Q_{\mathsf{H}}^2 + Q_{\mathsf{ID}} + \sum_{\mathsf{T}\in\mathcal{T}} \#\mathsf{ku}_{\mathsf{T}}) \cdot \mathsf{negl}(n).$$

□

6 Our RIBE Scheme with Bounded DKER

In this section, we propose an RIBE scheme achieving bounded decryption key exposure resistance (DKER). We give some backgrounds and preliminaries on RIBE with bounded DKER in Section 6.1 and Section 6.2, respectively. We propose our construction and prove its adaptive anonymity in Section 6.3 and Section 6.4, respectively.

6.1 Background

Seo and Emura [28] introduced a security notion called decryption key exposure resistance (DKER). DKER is a stronger security notion than the simplest notion defined by Boldyreva et al. [5]. DKER ensures an RIBE scheme is secure even when the decryption key of the target identity $\mathsf{ID}^\star$ is revealed. It is believed that an adaptive-identity secure RIBE scheme with DKER based on LWE can be constructed, but no concrete construction has been proposed so far. [4] Moreover, all previous adaptive-identity RIBE schemes achieving DKER do not satisfy the anonymity. However, a selective-identity RIBE scheme that satisfies DKER and the anonymity can be obtained by applying Katsumata et al.'s generic construction [15] to our RIBE scheme and the selective-identity hierarchical IBE scheme on MPLWE [20]. Takayasu and Watanabe [31,32] introduced a weaker security notion called bounded DKER. Bounded DKER is a variant of DKER and there is a-priori number Q_D and an adversary is allowed to make the decryption key reveal query of $\mathsf{ID}^\star$ at most Q_D. As discussed in [31,32], bounded DKER is enough to be secure against exposure of the decryption key in practice because it rarely happens so many times. Takayasu's RIBE scheme [30] can be transformed into a scheme with the anonymity and bounded DKER. However, an adaptive-identity RIBE scheme with the anonymity and bounded DKER based on MPLWE has not been constructed. In this paper, we propose an RIBE scheme with bounded DKER based on the MPLWE assumption. Table 3 compares Takayasu's RIBE with bounded DKER and our scheme. Our scheme achieves a shorter master public key and a secret key compared to Takayasu's RIBE.

[4] Wang et al. [33] claimed to construct the adaptive-identity hierarchical RIBE scheme on LWE in the ROM. However, this scheme is based on Agrawal et al.'s [3] hierarchical IBE scheme on LWE which is selective-identity secure, therefore, the security proof is doubtful.

6.2 Preliminaries on RIBE with Bounded DKER

We give some preliminaries on RIBE with Bounded DKER.

Cover Free Family. We use the following result of the cover free family to construct an RIBE scheme achieving the bounded DKER.

Definition 8 ([11]). *Let α, G, W, Q be positive integers and $\mathcal{F} = \{\mathcal{F}_i\}_{i=1}^{\alpha}$ be a family of subsets of $[G]$, where $|\mathcal{F}_i| = W$ for each $i \in [\alpha]$. If $\bigcup_{j=1}^{Q} \mathcal{F}_{i_j} \not\supset \mathcal{F}_{i_{Q+1}}$ holds for any $\mathcal{F}_{i_1}, \ldots, \mathcal{F}_{i_{Q+1}} \in \mathcal{F}$ such that $\mathcal{F}_{i_k} \neq \mathcal{F}_{i_\ell}$ for any distinct $k, \ell \in [Q+1]$, $\mathcal{F}$ is termed as W-uniform Q-cover-free.*

Lemma 10 ([18]). *There is a deterministic polynomial time algorithm* $\mathsf{CFF.Gen}$ *which takes positive integers α and Q as input, and outputs a positive integer G and a W-uniform Q-cover-free family $\mathcal{F} = \{\mathcal{F}_i\}_{i=1}^{\alpha}$ over $[G]$, where $G \leq 16Q^2 \log \alpha$ and $W = \frac{G}{4Q}$.*

Anonymous RIBE achieving Bounded DKER. Takayasu and Watanabe [31] formalized bounded DKER which is a weaker security notion than the full DKER. In RIBE with bounded DKER, an adversary $\mathcal{A}$ is allowed to make the decryption key reveal queries on the target identity $\mathsf{ID}^\star$ at most Q_D times for a-priori positive integer Q_D as well as the queries described in Section 4.

Decryption Key Reveal Query: Until the challenge query, upon a query $(\mathsf{ID}, \mathsf{T}) \in \mathcal{ID} \times \mathcal{T}$ by $\mathcal{A}$, $\mathcal{C}$ checks (1) $\mathsf{T} \leq \mathsf{T}_{\mathsf{cu}}$ and (2) $\mathsf{ID} \notin \mathsf{RL}_{\mathsf{T}}$. After the challenge query, $\mathcal{C}$ also checks (3) $(\mathsf{ID}, \mathsf{T}) \neq (\mathsf{ID}^\star, \mathsf{T}^\star)$ and (4) $\mathsf{T}_{\mathsf{cu}} \geq \mathsf{T}^\star$, $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}}$ has been revealed to $\mathcal{A}$ Q_D times by the decryption key reveal queries, and $\mathsf{ID} \neq \mathsf{ID}^\star$. If the all conditions are satisfied, $\mathcal{C}$ finds $\mathsf{sk}_{\mathsf{ID}}$ from SKList and returns $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} \leftarrow \mathsf{DKGen}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ku}_{\mathsf{T}})$ to $\mathcal{A}$. Otherwise, returns $\perp$ to $\mathcal{A}$.

To capture this query, we change several queries described in Section 4. Upon the revoke & key update query by $\mathcal{A}$, $\mathcal{C}$ also checks $\mathsf{T}_{\mathsf{cu}} = \mathsf{T}^\star - 1$, $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}}$ has been revealed to $\mathcal{A}$ Q_D times by the decryption key reveal queries, and $\mathsf{ID}^\star \in \mathsf{RL}$. Upon the challenge query by $\mathcal{A}$, $\mathcal{C}$ also checks (1) $\mathsf{T}^\star \leq \mathsf{T}_{\mathsf{cu}}$ and $\mathcal{A}$ has made a decryption key reveal query $(\mathsf{ID}^\star, \mathsf{T}^\star)$, and (2) $\mathsf{T}^\star \leq \mathsf{T}_{\mathsf{cu}}$, $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}}$ has been revealed to $\mathcal{A}$ more than Q_D times, and $\mathsf{ID}^\star \in \mathsf{RL}_{\mathsf{T}^\star}$.

We note that our RIBE scheme in Section 5 does not satisfy (bounded) DKER. $\mathcal{A}$ can obtain $\mathsf{ID}^\star$'s decryption key $(d_{\mathsf{ID},\mathsf{T},i})_{i=1}^{t+\gamma\tau} = (r_{\mathsf{ID},i} + r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau}$ and the key update $(r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau}$ if $\mathsf{ID}^\star$ has not been revoked by $\mathsf{T}^\star$. Therefore, $\mathcal{A}$ can retrieve $\mathsf{ID}^\star$'s secret key by computing $(r_{\mathsf{ID}^\star,i})_{i=1}^{t+\gamma\tau} = (d_{\mathsf{ID},\mathsf{T},i} - r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau}$.

6.3 Construction

In this section, we propose our RIBE scheme with bounded DKER.

Let G be a positive integer. A hash function $\mathsf{H} : \{0,1\}^{\leq L_{\mathcal{ID}} + L_{\mathcal{T}} + \lceil \log G \rceil + 1} \to \mathbb{Z}_q^{<n+2d-2}[X]$ will be modeled as a random oracle in a security proof. Other notations are the same as in Section 5. Our bounded DKER RIBE scheme consists of the following algorithms.

Table 3. Comparison among adaptively secure RIBE schemes with bounded DKER based on LWE and MPLWE in the (Q)ROM

Scheme	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{ct}\rvert$	$\lvert\mathsf{sk}_{\mathsf{ID}}\rvert$
Takayasu-RIBE [30] (with Bounded DKER)	$O(n^2 \log^2 n)$	$O(L_{\mathcal{ID}} n \log n)$	$O(Gn^2 \log^2 n)$
Our Scheme	$O(n \log^2 n)$	$O(L_{\mathcal{ID}} n \log n)$	$O(Gn \log^2 n)$

Scheme	Anonymity	Reduction loss	Model	Assumption
Takayasu-RIBE [30] (with Bounded DKER)	✓	$O(1)$	QROM	LWE
Our Scheme	✓	$O(1)$	QROM	MPLWE

n denotes the security parameter. $\lvert\mathsf{mpk}\rvert$, $\lvert\mathsf{ct}\rvert$, and $\lvert\mathsf{sk}_{\mathsf{ID}}\rvert$ denote the size of a master public key, a ciphertext for a n-bit plaintext, and a secret key, respectively. $L_{\mathcal{ID}} = O(n)$ denotes the length of an identity. Let $G = \mathsf{poly}(n)$ be a positive integer proportional to Q_D, where Q_D is the bounded number of the decryption key reveal queries.

$\mathsf{Setup}(1^n) \to (\mathsf{mpk}, \mathsf{msk})$**:** Run $((a_i)_{i=1}^{t+\gamma\tau}, (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}) \leftarrow \mathsf{TrapGen}(1^n)$ and output $\mathsf{mpk} = (a_i)_{i=1}^{t+\gamma\tau}$ and $\mathsf{msk} = (w_{i,j})_{(i,j)=(1,1)}^{(t,\gamma\tau)}$.

$\mathsf{SKGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID}) \to \mathsf{sk}_{\mathsf{ID}}$**:** For $g \in [G]$, run $((r_{\mathsf{ID},g,i})_{i=1}^{t+\gamma\tau})_{g=1}^{G} \leftarrow \mathsf{SamplePre}(\mathsf{mpk}, \mathsf{msk}, u_{\mathsf{ID},g}, \sigma)$, where $u_{\mathsf{ID},g} = \mathsf{H}(\mathsf{ID} \| g \| 0)$, and output $\mathsf{sk}_{\mathsf{ID}} = ((r_{\mathsf{ID},g,i})_{i=1}^{t+\gamma\tau})_{g=1}^{G}$. By Lemma 6, it holds that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{ID},g,i} = u_{\mathsf{ID},g}$.

$\mathsf{KeyUp}(\mathsf{mpk}, \mathsf{msk}, \mathsf{T}, \mathsf{RL}_{\mathsf{T}}) \to \mathsf{ku}_{\mathsf{T}}$**:** First, run the KUNode algorithm with input a key revocation list $\mathsf{RL}_{\mathsf{T}} \subset \mathcal{ID}$ and obtain $\mathcal{KU}_{\mathsf{T}} = \{\theta_1, \ldots \theta_r\}$. Then, for each node $\theta_j \in \mathcal{KU}_{\mathsf{T}}$, run $(r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau} \leftarrow \mathsf{SamplePre}(\mathsf{mpk}, \mathsf{msk}, u_{\mathsf{T},\theta_j}, \sigma)$, where $u_{\mathsf{T},\theta_j} = \mathsf{H}(\theta_j \| 0 \| \mathsf{T})$. Finally, output $\mathsf{ku}_{\mathsf{T}} = (\theta_j, (r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau})_{\theta_j \in \mathcal{KU}_{\mathsf{T}}}$ for the time period T. By Lemma 6, it holds that $\sum_{i=1}^{t+\gamma\tau} a_i r_{\mathsf{T},\theta_j,i} = u_{\mathsf{T},\theta_j}$.

$\mathsf{DKGen}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{ku}_{\mathsf{T}}) \to \mathsf{dk}_{\mathsf{ID},\mathsf{T}} \,/\, \perp$**:** DKGen algorithm takes mpk, $\mathsf{sk}_{\mathsf{ID}} = ((r_{\mathsf{ID},g,i})_{i=1}^{t+\gamma\tau})_{g \in \mathcal{F}_{\mathsf{T}}}$, and $\mathsf{ku}_{\mathsf{T}} = (\mathcal{KU}_{\mathsf{T}} = \{\theta_1, \ldots, \theta_r\}, ((r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau})_{\theta_j \in \mathcal{KU}_{\mathsf{T}}})$ as input. Then, find $\theta_j \in \mathcal{KU}_{\mathsf{T}}$ such that $\mathsf{ID}[0:\ell] = \theta_j$ for some $\ell \in [0, L_{\mathcal{ID}}]$. If such θ_j does not exist, output $\perp$. Otherwise, output a decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}} = (d_{\mathsf{ID},\mathsf{T},i})_{i=1}^{t+\gamma\tau} = (\sum_{g \in \mathcal{F}_{\mathsf{T}}} r_{\mathsf{ID},g,i} + r_{\mathsf{T},\theta_j,i})_{i=1}^{t+\gamma\tau}$ for $(\mathsf{ID}, \mathsf{T})$. By Lemma 6, it holds that $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = \sum_{i=1}^{t+\gamma\tau} a_i (\sum_{g \in \mathcal{F}_{\mathsf{T}}} r_{\mathsf{ID},g,i} + r_{\mathsf{T},\theta_j,i}) = \sum_{g \in \mathcal{F}_{\mathsf{T}}} u_{\mathsf{ID},g} + u_{\mathsf{T},\theta_j}$.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{T}, \mathsf{m}) \to \mathsf{ct}_{\mathsf{ID},\mathsf{T}}$**:** Sample $s \xleftarrow{\mathrm{U}} \mathbb{Z}_q^{<n+2d+k-1}[X]$, $\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q^{2d+k},\alpha' q}$ for each $i \in [t]$, $\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q^{d+k+1},\alpha' q}$ for each $i \in [t+1, t+\gamma\tau]$, and $\mathbf{e}'_\ell \leftarrow D_{\mathbb{Z}_q^{k+2},\alpha' q}$ for $\ell \in [0, L_{\mathcal{ID}}]$. Then, compute

$$b_i = \begin{cases} a_i \odot_{2d+k} s + 2e_i & \text{if } i \in [t] \\ a_i \odot_{d+k+1} s + 2e_i & \text{if } i \in [t+1, t+\gamma\tau] \end{cases}$$

$$b'_\ell = \mathsf{m} + \left(\sum_{g \in \mathcal{F}_{\mathsf{T}}} u_{\mathsf{ID},g} + u_{\mathsf{T},\mathsf{ID}[0:\ell]} \right) \odot_{k+2} s + 2e'_\ell \quad (\ell \in [0, L_{\mathcal{ID}}])$$

and output $\mathsf{ct}_{\mathsf{ID},\mathsf{T}} = ((b_i)_{i=1}^{t+\gamma\tau}, (b'_\ell)_{\ell=0}^{L_{\mathcal{ID}}})$.

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{dk}_{\mathsf{ID},\mathsf{T}}, \mathsf{ct}_{\mathsf{ID},\mathsf{T}}) \to \mathsf{m}'$**:** Find $\ell \in [0, L_{\mathcal{ID}}]$ such that $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = u_{\mathsf{ID}} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}$. Then, output

$$\mathsf{m}' = \left(b'_\ell - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \mod q \right) \mod 2.$$

The following lemma states that our scheme satisfies the correctness with overwhelming probability.

Theorem 5. *For a positive real number $\alpha' < (8\sqrt{W+1}\omega(\log n)\sigma K + 1)^{-1}$ and a positive integer $K = t(2d-1) + \gamma\tau d$, the scheme satisfies the correctness with overwhelming probability in n.*

Proof. By the property of the KUNode algorithm, each non-revoked user can find a unique node $\theta_j \in \mathcal{KU}_{\mathsf{T}}$ such that $\mathsf{ID}[0:\ell] = \theta_j$ for some $\ell \in [0, L_{\mathcal{ID}}]$. Therefore, the DKGen algorithm does not output $\perp$. Since $b_i = a_i \odot_{2d+k} s + 2e_i$ holds for each $i \in [t]$ and $b_i = a_i \odot_{d+k+1} s + 2e_i$ holds for each $i \in [t+1, t+\gamma\tau]$, when the $\mathsf{Decrypt}$ algorithm operates as specified, we have

$$\begin{aligned}
&b'_\ell - \sum_{i=1}^{t+\gamma\tau} b_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&= \mathsf{m} + \left(\sum_{g \in \mathcal{F}_{\mathsf{T}}} u_{\mathsf{ID},g} + u_{\mathsf{T},\mathsf{ID}[0:\ell]} \right) \odot_{k+2} s + 2e'_\ell - \sum_{i=1}^{t} (a_i \odot_{2d+k} s) \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&\quad - \sum_{i=t+1}^{t+\gamma\tau} (a_i \odot_{d+k+1} s) \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}.
\end{aligned}$$

Then, by Lemma 7 and the fact that $\sum_{i=1}^{t+\gamma\tau} a_i d_{\mathsf{ID},\mathsf{T},i} = \sum_{g \in \mathcal{F}_{\mathsf{T}}} u_{\mathsf{ID},g} + u_{\mathsf{T},\mathsf{ID}[0:\ell]}$ holds as we explained in the DKGen algorithm, we have

$$\begin{aligned}
&\mathsf{m} + \left(\sum_{g \in \mathcal{F}_{\mathsf{T}}} u_{\mathsf{ID},g} + u_{\mathsf{T},\mathsf{ID}[0:\ell]} \right) \odot_{k+2} s + 2e'_\ell - \sum_{i=1}^{t} (a_i \odot_{2d+k} s) \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&\quad - \sum_{i=t+1}^{t+\gamma\tau} (a_i \odot_{d+k+1} s) \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} - 2 \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&= \mathsf{m} + \cancel{\left(\sum_{g \in \mathcal{F}_{\mathsf{T}}} u_{\mathsf{ID},g} + u_{\mathsf{T},\mathsf{ID}[0:\ell]} \right)} \odot_{k+2} s + 2e'_\ell
\end{aligned}$$

$$
\begin{aligned}
&\cancel{-\sum_{i=1}^{t+\gamma\tau}(a_i d_{\mathsf{ID},\mathsf{T},i}) \odot_{k+2} s} - 2\sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i} \\
&= \mathsf{m} + \underbrace{2\left(e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\right)}_{\text{error terms}}.
\end{aligned}
$$

If $\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty < \frac{q}{8}$, the decryption of the scheme satisfies the correctness. Let

$$
\begin{aligned}
&\mathbf{A} = [\mathsf{T}^{n,2d-1}(a_1)|\cdots|\mathsf{T}^{n,2d-1}(a_t)|\mathsf{T}^{n+d-1,d}(a_{t+1})|\cdots|\mathsf{T}^{n+d-1,d}(a_{t+\gamma\tau})], \\
&\mathbf{r}_{\mathsf{ID},g} = [\mathbf{r}_{\mathsf{ID},g,1}^\top|\cdots|\mathbf{r}_{\mathsf{ID},g,t+\gamma\tau}^\top]^\top, \qquad \mathbf{r}_{\mathsf{T},\mathsf{ID}[0:\ell]} = [\mathbf{r}_{\mathsf{T},\mathsf{ID}[0:\ell],1}^\top|\cdots|\mathbf{r}_{\mathsf{T},\mathsf{ID}[0:\ell],t+\gamma\tau}^\top]^\top.
\end{aligned}
$$

By Lemma 6, $\mathbf{r}_{\mathsf{ID},g}$ and $\mathbf{r}_{\mathsf{T},\mathsf{ID}[0:\ell]}$ are distributed statistically close to $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{ID},g}}(\mathbf{A})}$ and $D_{\Lambda^\perp_{\mathbf{u}_{\mathsf{T},\mathsf{ID}[0:\ell]}}(\mathbf{A})}$, respectively. Therefore, by Lemma 2, for each $g \in \mathcal{F}_\mathsf{T}$ and $\ell \in [0, L_{\mathcal{ID}}]$, it holds that

$$
\begin{aligned}
&\|r_{\mathsf{ID},g,i}\|_\infty \le \omega(\sqrt{\log n})\sigma, \qquad \|r_{\mathsf{T},\mathsf{ID}[0:\ell],i}\|_\infty \le \omega(\sqrt{\log n})\sigma \\
&\|e_i\|_\infty \le \omega(\sqrt{\log n})\alpha' q, \qquad \|e'_\ell\|_\infty \le \omega(\sqrt{\log n})\alpha' q
\end{aligned}
$$

with overwhelming probability in n. We have

$$
\begin{aligned}
&\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty \\
&\le \|e'_\ell\|_\infty + \|\sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty \\
&\le \|e'_\ell\|_\infty + \|\sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{T},\mathsf{ID}[0:\ell],i}\|_\infty + \sum_{g\in\mathcal{F}_\mathsf{T}} \|\sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} r_{\mathsf{ID},g,i}\|_\infty \\
&\le \omega(\sqrt{\log n})\alpha' q + K(\sqrt{W+1}\omega(\sqrt{\log n})\sigma)(\omega(\sqrt{\log n})\alpha' q),
\end{aligned}
$$

where $K = t(2d-1) + d\gamma\tau$. Thus, we have $\|e'_\ell - \sum_{i=1}^{t+\gamma\tau} e_i \odot_{k+2} d_{\mathsf{ID},\mathsf{T},i}\|_\infty < \frac{q}{8}$ if $\alpha' < (8\sqrt{W+1}\omega(\log n)\sigma K + 1)^{-1}$ holds. □

To guarantee the correctness and the adaptive anonymity of the scheme, parameters have to satisfy the following restrictions.

- For the correctness, $\alpha' < (8\sqrt{W+1}\omega(\log n)\sigma K + 1)^{-1}$ holds.
- By Lemma 6, $q = \mathsf{poly}(n)$, $d \le n$, $\frac{dt}{n} = \Omega(\log n)$, $\sigma = \omega(\log^2 n)\sqrt{ndt}$, and $\gamma = \frac{n+2d-2}{d}$ hold to apply $\mathsf{TrapGen}$ and $\mathsf{SamplePre}$ algorithms properly.
- By Lemma 4, $d \le n$, $\sigma = \omega(1)$, $q = \mathsf{poly}(n)$, $q = \omega(\sqrt{\log n})\sigma$, and $\frac{dt}{n} = \Omega(\log n)$ hold to the public key is statistically indistinguishable from uniform.
- By Lemma 6, $\sigma > 16\sqrt{\log 2(2d-1)/\pi}$ holds to apply $\mathsf{Sample}\mathbb{Z}$ algorithm properly.

- By Lemma 5, $\frac{\alpha'}{2\alpha} > \sqrt{2\sigma^2((2d-1)t + d\gamma\tau)(L_{\mathcal{ID}}+1)+1}$ and $\alpha q > \omega(\sqrt{\log(t(2d+k)+\gamma\tau d+(K+2)(L_{\mathcal{ID}}+1))})$ holds to apply ReRand algorithm properly.
- $\mathsf{MPLWE}_{q,n+2d+k,\mathbf{d},D_{\mathbb{Z},\alpha q}}$ assumption holds. In other words, by Lemma 9, $q = \Omega(\alpha^{-1}n^{c+1})$ and $\mathsf{PLWE}^{(f)}_{\mathbb{Z}_q,\bar{\alpha}q}$ assumption holds for a constant $c > 0$, a polynomial $f \in \mathcal{E}(T, \mathbf{d}, n+2d+k)$ of degree $m \in [2d+k, n]$ such that $\mathrm{EF}(f) = O(n^c)$, $\bar{\alpha} = \Omega(\sqrt{m}/q)$, and $1 \geq \bar{\alpha} \geq \frac{2\sqrt{n+2d+k}}{qT}$ by Lemma 9.

To satisfy these restrictions, we set

$$
\begin{aligned}
&d = \Theta(n),\ k = \Theta(n),\ t = \log n,\ \gamma = \frac{n+2d-2}{d},\ L_{\mathcal{ID}} = \Theta(n),\ \sigma = n^{1+\mu_2},\\
&q = \sqrt{WL_{\mathcal{ID}}}n^{4.5+4\mu_2+c},\ \tau = \lceil \log q \rceil,\\
&\alpha' = (\sqrt{W}n^{2+2\mu_2})^{-1},\ \alpha = (\sqrt{WL_{\mathcal{ID}}}n^{3.5+4\mu_2})^{-1},
\end{aligned}
$$

where $\mu_2 > 0$ can be set arbitrarily small and $c > 0$ is a parameter of the PLWE assumption.

6.4 Security

A security proof is also almost the same as that of Theorem 4. The only difference is the discussion in Game_7 because Eq. (18) is replaced by the following equation.

$$
b'_\ell = \sum_{i=1}^{t+\gamma\tau} \left(\sum_{g \in \mathcal{F}_{\mathsf{T}}} r_{\mathsf{ID}^\star,g,i} + r_{\mathsf{T}^\star,\mathsf{ID}^\star[\ell],i} \right) \odot_{k+2} v_i + 2e'_\ell
$$

If $\mathsf{ID}^\star \in \mathsf{RL}_{\mathsf{T}^\star}$, by the same discussion in Game_7 of the security proof of Theorem 4, the challenge ciphertext is statistically indistinguishable from uniform. If $\mathsf{ID}^\star \notin \mathsf{RL}_{\mathsf{T}^\star}$, even when an adversary $\mathcal{A}$ obtains at most Q_D decryption keys $\mathsf{dk}_{\mathsf{ID}^\star,\mathsf{T}^\star}$ for $\mathsf{T} \neq \mathsf{T}^\star$, Lemma 10 ensures that at least one $r_{\mathsf{ID}^\star,g,i}$ in $(r_{\mathsf{ID}^\star,g,i})_{g\in\mathcal{F}_{\mathsf{T}}}$ is not revealed to $\mathcal{A}$. Therefore, by a similar discussion in Game_7 the proof of Theorem 4, the challenge ciphertext is statistically indistinguishable from uniform.

7 Conclusion

In this paper, we prove the tight adaptive anonymity of LVV-IBE in the QROM and propose an RIBE scheme achieving tight adaptive anonymity in the QROM. Moreover, we also propose an RIBE scheme achieving bounded DKER as well as tight adaptive anonymity in the QROM.

Acknowledgement. This research was partially supported by JST CREST Grant Number JPMJCR2113, Japan, and JSPS KAKENHI Grant Number JP24K02939, Japan.

References

1. Abla, P.: Identity-based encryption from LWE with more compact master public key. In: Oswald, E. (ed.) CT-RSA 2024. LNCS, vol. 14643, pp. 319–353. Springer, Heidelberg (May 2024). https://doi.org/10.1007/978-3-031-58868-6_13
2. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (May / Jun 2010). https://doi.org/10.1007/978-3-642-13190-5_28
3. Agrawal, S., Boneh, D., Boyen, X.: Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 98–115. Springer, Heidelberg (Aug 2010). https://doi.org/10.1007/978-3-642-14623-7_6
4. Bai, S., Das, D., Hiromasa, R., Rosca, M., Sakzad, A., Stehlé, D., Steinfeld, R., Zhang, Z.: MPSign: A signature from small-secret middle-product learning with errors. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 66–93. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45388-6_3
5. Boldyreva, A., Goyal, V., Kumar, V.: Identity-based encryption with efficient revocation. In: Ning, P., Syverson, P.F., Jha, S. (eds.) ACM CCS 2008. pp. 417–426. ACM Press (Oct 2008). https://doi.org/10.1145/1455770.1455823
6. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (Dec 2011). https://doi.org/10.1007/978-3-642-25385-0_3
7. Boyen, X., Li, Q.: Towards tightly secure lattice short signature and id-based encryption. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 404–434. Springer, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53890-6_14
8. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. Journal of Cryptology **25**(4), 601–639 (Oct 2012). https://doi.org/10.1007/s00145-011-9105-2
9. Chen, J., Lim, H.W., Ling, S., Wang, H., Nguyen, K.: Revocable identity-based encryption from lattices. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 12. LNCS, vol. 7372, pp. 390–403. Springer, Heidelberg (Jul 2012)
10. Das, D., Au, M.H., Zhang, Z.: Ring signatures based on middle-product learning with errors problems. In: Buchmann, J., Nitaj, A., eddine Rachidi, T. (eds.) AFRICACRYPT 19. LNCS, vol. 11627, pp. 139–156. Springer, Heidelberg (Jul 2019). https://doi.org/10.1007/978-3-030-23696-0_8
11. Erdös, P., Frankel, P., Furedi, Z.: Families of finite sets in which no set is covered by the union of r others. Israeli Journal of Mathematics **51**, 79–89 (1985)
12. Fan, J., Lu, X., Au, M.H.: Adaptively secure identity-based encryption from middle-product learning with errors. In: Simpson, L., Baee, M.A.R. (eds.) ACISP 23. LNCS, vol. 13915, pp. 320–340. Springer, Heidelberg (Jul 2023). https://doi.org/10.1007/978-3-031-35486-1_15
13. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC. pp. 197–206. ACM Press (May 2008). https://doi.org/10.1145/1374376.1374407
14. Hiromasa, R.: Digital signatures from the middle-product LWE. In: Baek, J., Susilo, W., Kim, J. (eds.) ProvSec 2018. LNCS, vol. 11192, pp. 239–257. Springer, Heidelberg (Oct 2018). https://doi.org/10.1007/978-3-030-01446-9_14

15. Katsumata, S., Matsuda, T., Takayasu, A.: Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. In: Lin, D., Sako, K. (eds.) PKC 2019, Part II. LNCS, vol. 11443, pp. 441–471. Springer, Heidelberg (Apr 2019). https://doi.org/10.1007/978-3-030-17259-6_15
16. Katsumata, S., Yamada, S.: Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 682–712. Springer, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53890-6_23
17. Katsumata, S., Yamada, S., Yamakawa, T.: Tighter security proofs for GPV-IBE in the quantum random oracle model. Journal of Cryptology **34**(1), 5 (Jan 2021). https://doi.org/10.1007/s00145-020-09371-y
18. Kumar, R., Rajagopalan, S., Sahai, A.: Coding constructions for blacklisting problems without computational assumptions. In: Wiener, M.J. (ed.) CRYPTO'99. LNCS, vol. 1666, pp. 609–623. Springer, Heidelberg (Aug 1999). https://doi.org/10.1007/3-540-48405-1_38
19. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. DCC **75**(3), 565–599 (2015). https://doi.org/10.1007/s10623-014-9938-4
20. Le, H.Q., Duong, D.H., Susilo, W., Pieprzyk, J.: Trapdoor delegation and HIBE from middle-product LWE in standard model. In: Conti, M., Zhou, J., Casalicchio, E., Spognardi, A. (eds.) ACNS 20, Part I. LNCS, vol. 12146, pp. 130–149. Springer, Heidelberg (Oct 2020). https://doi.org/10.1007/978-3-030-57808-4_7
21. Lin, H., Sun, S., Wang, M., Liu, J.K., Wang, W.: Shorter linkable ring signature based on middle-product learning with errors problem. The Computer Journal **66**(12), 2974–2989 (2022). https://doi.org/10.1093/comjnl/bxac141
22. Lombardi, A., Vaikuntanathan, V., Vuong, T.D.: Lattice trapdoors and IBE from middle-product LWE. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019, Part I. LNCS, vol. 11891, pp. 24–54. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-36030-6_2
23. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (May / Jun 2010). https://doi.org/10.1007/978-3-642-13190-5_1
24. Ma, X., Lin, D.: Generic constructions of revocable identity-based encryption. In: Liu, Z., Yung, M. (eds.) Inscrypt 2019. pp. 381–396. LNCS, Springer (December 2020)
25. Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (Aug 2001). https://doi.org/10.1007/3-540-44647-8_3
26. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC. pp. 84–93. ACM Press (May 2005). https://doi.org/10.1145/1060590.1060603
27. Rosca, M., Sakzad, A., Stehlé, D., Steinfeld, R.: Middle-product learning with errors. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 283–297. Springer, Heidelberg (Aug 2017). https://doi.org/10.1007/978-3-319-63697-9_10
28. Seo, J.H., Emura, K.: Revocable identity-based encryption revisited: Security model and construction. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 216–234. Springer, Heidelberg (Feb / Mar 2013). https://doi.org/10.1007/978-3-642-36362-7_14

29. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 617–635. Springer, Heidelberg (Dec 2009). https://doi.org/10.1007/978-3-642-10366-7_36
30. Takayasu, A.: Adaptively secure lattice-based revocable IBE in the QROM: compact parameters, tight security, and anonymity. DCC **89**(8), 1965–1992 (2021). https://doi.org/10.1007/s10623-021-00895-3
31. Takayasu, A., Watanabe, Y.: Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance. In: Pieprzyk, J., Suriadi, S. (eds.) ACISP 17, Part I. LNCS, vol. 10342, pp. 184–204. Springer, Heidelberg (Jul 2017)
32. Takayasu, A., Watanabe, Y.: Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more. Theoretical Computer Science **849**, 64–98 (2021). https://doi.org/10.1016/J.TCS.2020.10.010, https://doi.org/10.1016/j.tcs.2020.10.010
33. Wang, S., Zhang, J., He, J., Wang, H., Li, C.: Simplified revocable hierarchical identity-based encryption from lattices. In: Mu, Y., Deng, R.H., Huang, X. (eds.) CANS 19. LNCS, vol. 11829, pp. 99–119. Springer, Heidelberg (Oct 2019). https://doi.org/10.1007/978-3-030-31578-8_6
34. Yamada, S.: Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 32–62. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49896-5_2
35. Yamada, S.: Asymptotically compact adaptively secure lattice IBEs and verifiable random functions via generalized partitioning techniques. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 161–193. Springer, Heidelberg (Aug 2017). https://doi.org/10.1007/978-3-319-63697-9_6
36. Yamakawa, T., Zhandry, M.: Classical vs quantum random oracles. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part II. LNCS, vol. 12697, pp. 568–597. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77886-6_20
37. Yang, N., Yang, S., Zhao, Y., Wu, W.: Inner product encryption from middle-product learning with errors. In: Chen, X., Huang, X., Kutyłowski, M. (eds.) SocialSec 2022. CCIS, vol. 1663, pp. 94–113. Springer Nature (October 2022)
38. Yang, N., Yang, S., Zhao, Y., Wu, W., Wang, X.: Inner product encryption from middle-product learning with errors. Computer Standards & Interfaces **87**(C) (2024)
39. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 758–775. Springer, Heidelberg (Aug 2012). https://doi.org/10.1007/978-3-642-32009-5_44