Compact and Tightly Secure (Anonymous) IBE from Module LWE in the QROM

Toi Tomita[1] and Junji Shikata[1]

[1]Yokohama National University, Japan
{tomita-toi-sk, shikata-junji-rb}@ynu.ac.jp

October 30, 2024

Abstract

We present a new compact and tightly secure (anonymous) identity-based encryption (IBE) scheme based on structured lattices. This is the first IBE scheme that is (asymptotically) as compact as the most practical NTRU-based schemes and tightly secure under the module learning with errors (MLWE) assumption, known as the standard lattice assumption, in the (quantum) random oracle model. In particular, our IBE scheme is the most compact lattice-based scheme (except for NTRU-based schemes). We design our IBE scheme by instantiating the framework of Gentry, Peikert, and Vaikuntanathan (STOC'08) using the compact trapdoor proposed by Yu, Jia, and Wang (CRYPTO'23). The tightness of our IBE scheme is achieved by extending the proof technique of Katsumata et al. (ASIACRYPT'18, JoC'21) to the hermit normal form setting. To achieve this, we developed some new results on module lattices that may be of independent interest.

1 Introduction

1.1 Background

Identity-based encryption (IBE), introduced by Shamir [Sha84], is a generalization of public key encryption (PKE). Unlike traditional PKE, IBE allows senders to encrypt messages using a master public key mpk and an arbitrary string id, such as the recipient's username or email address. This means IBEs do not require a Public Key Infrastructure (PKI). In addition, when communicating with multiple users, an IBE only needs one mpk, whereas a PKE requires as many public keys as there are users. Because of these advantages, IBE has been discussed in the context of several practical applications [AKG+07, BRTM08, DSDSAL08, TWZL08, ZC11, HSM13, MSW15]. Since the first IBE scheme was proposed in 2001 [BF01, Coc01], it has been improved in various ways [BGK08, Wat09, BKP14, DG17]. However, these traditional schemes are vulnerable to quantum attacks due to Shor's algorithm [Sho99].

In 2008, Gentry, Peikert, and Vaikuntanathan [GPV08] proposed the first post-quantum IBE scheme (GPV-IBE) based on standard unstructured lattices. The GPV-IBE is secure under the learning with error (LWE) assumption [Reg05] in the random oracle model (ROM). Since then, there have been several studies on lattice-based IBEs from different perspectives, including extending to the quantum ROM (QROM) [Zha12, KYY18, KYY21], removing the random oracle [ABB10a, CHKP10, KY16, BL16, Yam17, ALWW21], and adding security properties [ABB10b, AP12, NY19, KMT19, EKW19]. However, these constructions only indicate improvements on the theoretical side. In particular, these IBE schemes are still inefficient even when instantiated on structured lattices such as the ML-KEM [SAB+22] and the ML-DSA [LDK+22]. On the practical side, Ducas, Lyubashevsky, and Prest [DLP14] proposed the first practical lattice-based IBE scheme (DLP-IBE) based on NTRU lattices, and then several works [MSO17, CKKS19, ZMS+24] optimized the

DLP-IBE. As for implementations on structured lattices (not NTRU lattices), Bert et al. [BFRS18, BEP+21] provided (relatively) efficient implementations.

Unfortunately, even the DLP-IBE [DLP14] and its variants [MSO17, CKKS19, ZMS+24] have several efficiency challenges. One of these is the tightness of the security reduction. The efficiency of cryptographic schemes depends on the tightness of the security reduction. In general, we say that the security of a cryptographic scheme under a given computational assumption is tight if breaking the scheme's security is as hard as solving the assumption. More precisely, suppose that we have proved that if there is an adversary who can break the security of the scheme with advantage ϵ and running time T, we can break the underlying assumption with advantage ϵ' and running time T'. We then obtain the inequality $\epsilon/T \leq L \cdot \epsilon'/T'$, where L is the reduction loss of the scheme. The scheme is tightly secure if $L = O(1)$. If the scheme is not tightly secure, we need to set the parameters larger to ensure the concrete security of the scheme. The DLP-IBE is not tightly secure because the reduction loss depends on the number of adversary queries. Several tightly secure lattice-based IBE schemes have also been proposed [BL16, BL18, LLW20, KYY18, KYY21, KTY23], but none is as efficient as the DLP-IBE. From the above, the natural question is:

Can we construct a compact and tightly secure IBE scheme from lattices?

1.2 Our Contributions

In this paper, we answer the above questions in the affirmative by proposing the first IBE scheme that is (asymptotically) as compact as the DLP-IBE and tightly secure under the module LWE (MLWE) assumption, known as the standard lattice assumption, in (Q)ROM. Furthermore, our IBE scheme also satisfies anonymity, by ensuring that the ciphertext does not reveal any information about the identity as well as the message. In Table 1, we summarize our results and a comparison with previous lattice-based (anonymous) IBE schemes in the (Q)ROM. For a fair and clear comparison, we calculate the parameters of the module variants of some previous schemes. As can be seen from Table 1, our scheme is the first IBE scheme that is

Table 1: Comparison of lattice-based (anonymous) IBE schemes in the module setting. mpk, sk, and ct denote the master public key, a secret key, and a ciphertext, respectively. n, k, q, and $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n+1)$ denote the degree, the dimension, the modulus, and the ring of the underlying assumptions. MNTRU is an abbreviation for module NTRU. Q_{H} and Q_{id} denote the numbers of (quantum) random oracle and secret key queries, respectively. ϵ denotes the advantage of the scheme. † Its security losses are based on the results of the previous work [GPV08] because the security proof is omitted in their paper.

Scheme	# of $\mathcal{R}_q^k$ vectors in the mpk	# of $\mathcal{R}_q^k$ vectors in sk/ct	Assumption	Security loss
[GPV08]	$O(k \log q)$	$O(\log q)$	MLWE	$O(Q_{\mathsf{H}})$
[Zha12]	$O(k \log q)$	$O(\log q)$	MLWE	$O\left(\frac{(Q_{\mathsf{H}}+Q_{\mathsf{id}})^4}{\epsilon}\right)$
[DLP14]	$O(1)$	$O(1)$	MNTRU	$O(Q_{\mathsf{H}})$
[KYY21]	$O(k \log q)$	$O(\log q)$	MLWE	$O(1)$
[JHTW24]†	$O(k \log q)$	$O(\log q)$	MLWE	$O(Q_{\mathsf{H}})$
Ours	$O(k)$	$O(1)$	MLWE	$O(1)$

(asymptotically) as compact as the most practical NTRU-based schemes and tightly secure under the standard lattice assumption. In particular, our IBE scheme is the most compact lattice-based scheme (except for NTRU-based schemes).

Technical Overview. Here, we briefly summarize the spirit of our construction and security proof. Our proposed scheme is a GPV-IBE [GPV08] instantiated by Yu et al.'s compact preimage sampling [YJW23]. Hence, we first briefly describe the GPV-IBE.

GPV-IBE over module lattices. Let $\mathcal{R} = \mathbb{Z}_q[X]/(X^n + 1)$ and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$ be rings. In the GPV-IBE, a master public key is a fat matrix $\mathbf{A} \in \mathcal{R}_q^{k \times \ell}$ and a master secret key is its trapdoor $\mathsf{td}_{\mathbf{A}}$, which enables one to sample a short preimage $\mathbf{x} \in \mathcal{R}_q^\ell$ such that $\mathbf{A}\mathbf{x} = \mathbf{y} \bmod q$ given an arbitrary vector $\mathbf{y} \in \mathcal{R}_q^k$. A secret key $\mathsf{sk}_{\mathsf{id}}$ for an identity $\mathsf{id} \in \{0,1\}^*$ is a short vector $\mathbf{x}_{\mathsf{id}} \in \mathcal{R}^\ell$ such that $\mathbf{A}\mathbf{x}_{\mathsf{id}} = \mathbf{y}_{\mathsf{id}} \bmod q$, where $\mathbf{y}_{\mathsf{id}} = \mathsf{H}(\mathsf{id})$ for a hash function $\mathsf{H} : \{0,1\}^* \to \mathcal{R}_q^k$. A ciphertext for a message $\mathsf{M} \in \{0,1\}$ and an identity id consists of $\mathbf{c}_1 = \mathbf{A}^\top \mathbf{r} + \mathbf{e}_1 \in \mathcal{R}_q^\ell$ and $c_2 = \mathbf{y}_{\mathsf{id}}^\top \mathbf{r} + e_2 + \mathsf{M} \cdot \lfloor q/2 \rceil \in \mathcal{R}_q$ and , where $\mathbf{r} \in \mathcal{R}_q^k$ is a uniform random vector, $\mathbf{e}_1 \in \mathcal{R}^\ell$ and $e_2 \in \mathcal{R}$ are small noise term.

Tight proof by Katsumata et al. [KYY18, KYY21]. Katsumata et al. showed that GPV-IBE has tight security in the (Q)ROM. We outline the security proof in the ROM. To answer a random oracle query on id, the reduction algorithm chooses a random short vector $\mathbf{x}_{\mathsf{id}} \in \mathcal{R}^\ell$ and sets $\mathbf{y}_{\mathsf{id}} = \mathbf{A}\mathbf{x}_{\mathsf{id}} \bmod q$. If $\mathbf{x}_{\mathsf{id}}$ has sufficient entropy, $\mathbf{y}_{\mathsf{id}}$ is uniformly distributed over $\mathcal{R}_q^k$. Using this fact, the reduction algorithm returns $\mathbf{y}_{\mathsf{id}}$ for the random oracle query and $\mathbf{x}_{\mathsf{id}}$ for the secret key query. Note that the reduction algorithm knows a secret key $\mathbf{x}_{\mathsf{id}^*}$ for a target identity id^*. Thus, the reduction algorithm can simulate the challenge ciphertext by generating $\mathbf{c}_1^* = \mathbf{A}^\top \mathbf{r} + \mathbf{e}_1$ and $c_2^* = \mathbf{z}_{\mathsf{id}^*}^\top \mathbf{c}_1^* + \mathsf{M} \cdot \lfloor q/2 \rceil$. It is important to note that we no longer need the LWE instance $(\mathbf{y}_{\mathsf{id}^*}, \mathbf{y}_{\mathsf{id}^*}^\top \mathbf{r} + e_2)$ to simulate the challenge ciphertext. The actual proof uses the noise re-randomization technique by Katsumata and Yamada [KY16] to simulate the distribution of c_2^* (especially the noise term e_2).

More compact scheme via approximate preimage sampling. At the heart of the GPV-IBE is the preimage sampling technique, which is also a source of non-compactness. This is because the width of the matrix $\mathbf{A}$ must be $\ell = O(k \log_2 q)$ to realize preimage sampling. To improve the compactness, Chen et al. [CGM19] introduced the relaxed notion of preimage sampling, called *approximate preimage sampling*. With approximate preimage sampling, instead of sampling an exact preimage $\mathbf{x}$ such that $\mathbf{A}\mathbf{x} = \mathbf{y} \bmod q$, sample an approximate preimage $\mathbf{x} \in \mathcal{R}^\ell$ such that $\mathbf{A}\mathbf{x} = \mathbf{y} - \mathbf{z} \bmod q$, where $\mathbf{z} \in \mathcal{R}^k$ is a short error vector. Recently, Yu, Jia, and Wang [YJW23] developed a compact framework for approximate preimage sampling that uses *a nearly square matrix* instead of the short and fat one used in [CGM19].

To construct an efficient IBE scheme, we instantiate the GPV-IBE using Yu et al.'s approximate preimage sampling. Very recently and concurrently, Izabachène et al. [IPR23][1] and Jia et al. [JHTW24] proposed compact IBE schemes by using the approximate preimage sampling. The design idea of our scheme is similar to their schemes. Namely, to encrypt a message M under an identity id, we use a short random vector $\mathbf{r} \in \mathcal{R}^k$ instead of a uniform random vector. This is to keep the error term $\mathbf{z}^\top \mathbf{r}$ that appears during decryption small, where $\mathbf{z}$ is an approximate error.

Attempt: Apply the Katsumata et al. security proof directly. We try to apply the proof techniques of Katsumata et al. to the above compact scheme. Mostly, their proof technique can be applied, but there is one part where it cannot. This is the part that simulates the c^* of the challenge ciphertext. In their proof, they use a secret key $\mathbf{x}_{\mathsf{id}^*}$, which is an exact preimage vector, and the noise re-randomization technique of Katsumata and Yamada [KY16] to approximately simulate c^*. In our scheme, $\mathbf{x}_{\mathsf{id}^*}$ is an approximate preimage vector rather than an exact preimage vector. Then, when we try to simulate c^*, we have

$$
\begin{aligned}
c_2^* &= \mathbf{x}_{\mathsf{id}^*}^\top \mathbf{c}_1^* + \mathsf{M} \cdot \lfloor q/2 \rceil \\
&= \mathbf{x}_{\mathsf{id}^*}^\top (\mathbf{A}^\top \mathbf{r} + \mathbf{e}_1) + \mathsf{M} \cdot \lfloor q/2 \rceil \\
&= (\mathbf{A}\mathbf{x}_{\mathsf{id}^*})^\top \mathbf{r} + \mathbf{x}_{\mathsf{id}^*}^\top \mathbf{e}_1 + \mathsf{M} \cdot \lfloor q/2 \rceil \\
&= \mathbf{y}_{\mathsf{id}^*}^\top \mathbf{r} - \boxed{\mathbf{z}^\top \mathbf{r}} + \mathbf{z}_{\mathsf{id}^*}^\top \mathbf{e}_1 + \mathsf{M} \cdot \lfloor q/2 \rceil.
\end{aligned}
$$

Unfortunately, the noise re-randomization technique cannot account for this additional error term $\mathbf{z}^\top \mathbf{r}$ that *appears by evaluating* $\mathbf{A}\mathbf{r}_{\mathsf{id}^*}$. Therefore, we must use a different approach to complete the proof.

Solution: MLWE with an adaptive hint. To overcome the above problem, we use the module LWE with an adaptive hint, instead of the noise re-randomization technique. This assumption is an extension of MLWE

[1] Their proposed scheme is *selectively* secure in the *standard model*.

with error-leakage, introduced by Döttling et al [DKL+23]. Roughly speaking, this assumption says that the MLWE assumption holds even if a hint of the secret $\mathbf{r}$ and the noise $\mathbf{e}_1$ are adaptively given. We show a reduction from the (standard) MLWE problem to this variant. This allows us to exactly simulate c_2^* by using an approximate preimage vector $\mathbf{x}_{\mathsf{id}^*}$ and a hint without the noise re-randomization. Therefore, we can complete the proof.

Finally, we note that the above proof naturally fits in the QROM setting similar to [KYY18, KYY21]. Thus, the proof in the classical ROM can be almost automatically converted into the one in the QROM. Our proof technique can also be seen as an extension of the [KYY18, KYY21]'s proof technique to the Hermit normal form (HNF) setting. Furthermore, our proof technique is somewhat general since it can be applied to any approximate trapdoor sampling, e.g., [CGM19, JHTW24, JRS24], by appropriately setting parameters.

Comparison with the previous version in PQCrypto 2024. Here, we highlight the new contributions of the current paper, beyond the previous version [TS24] published in PQCrypto 2024.

The main difference from the PQCrypto 2024 version is that it uses module lattices instead of ideal ones. Module lattices offer a flexible trade-off between efficiency and scalability compared to ideal lattices. To this end, we develop three new results on module lattices that may be of independent interest. The first result is a tight reduction of the MLWE problem to a variant of MLWE where a hint about the secret and the noise is given adaptively. The second insight is a new Gaussian regularity lemma over rings. The third result is a compact approximate trapdoor over module lattices. These results are summarised in Section 3.

Organization. This paper is organized as follows. In Section 2, we first recall the notations, cryptographic definitions, and related lemmas. In Section 3, we show new results over module lattices. In Section 4, we present the description of our IBE scheme. In Section 5, we give a security proof of our IBE scheme in the ROM. In Section 6, we provide security proof of our IBE scheme in the QROM.

2 Preliminaries

Notations. Let λ denote the security parameter throughout the paper. We denote by $[n]$ the set $\{1, \ldots, n\}$ for any positive integer. For a finite set $\mathcal{S}$, let $\mathcal{U}(\mathcal{S})$ be the uniform distribution over $\mathcal{S}$ and let $s \leftarrow\$ \mathcal{S}$ denote the operation of sampling a from $\mathcal{S}$ uniformly at random. For a probability distribution or random variable $\mathcal{X}$, let $x \leftarrow\$ \mathcal{X}$ denote the operation of sampling x according to $\mathcal{X}$. Let $\mathcal{X}$ and $\mathcal{Y}$ be two random variables over some finite set $\mathcal{S}_X$ and $\mathcal{S}_Y$, respectively. The statistical distance $\Delta(\mathcal{X}, \mathcal{Y})$ between $\mathcal{X}$ and $\mathcal{Y}$ is defined as $\Delta(X, Y) \coloneqq \frac{1}{2}\sum_{s \in \mathcal{S}_X \cup \mathcal{S}_Y} |\Pr[X = s] - \Pr[Y = s]|$. We say that $\mathcal{X}$ and $\mathcal{Y}$ are statistically close and denote as $\mathcal{X} \approx_s \mathcal{Y}$ when $\Delta(X, Y) = \mathsf{negl}(\lambda)$. For two distributions $\mathcal{X}$ and $\mathcal{Y}$, we denote the convolution of $\mathcal{X}$ and $\mathcal{Y}$ by $\mathcal{X} * \mathcal{Y}$. That is, $\mathcal{X} * \mathcal{Y} = \{x + y : x \leftarrow\$ \mathcal{X}, y \leftarrow\$ \mathcal{Y}\}$.

2.1 Linear Algebra, Lattices, and Gaussian

Linear Algebra. Any matrix $\mathbf{M} \in \mathbb{R}^{n\times m}$ can be written as $\mathbf{M} = \mathbf{U}\mathbf{D}\mathbf{V}^\top$, where $\mathbf{U} \in \mathbb{R}^{n\times n}$ and $\mathbf{V} \in \mathbb{R}^{m\times m}$ are orthogonal matrices and $\mathbf{D} \in \mathbb{R}^{n\times m}$ is an upper diagonal matrix (singular value decomposition). The entries of $\mathbf{D}$ are called the singular values of $\mathbf{M}$ and we denote the smallest singular value by $\sigma_{\mathsf{min}}(\mathbf{M})$ and the largest singular value by $\sigma_{\mathsf{max}}(\mathbf{M})$. The largest singular value $\sigma_{\mathsf{max}}(\mathbf{M})$ is equal to the Euclidean spectral norm $\|\mathbf{M}\|_2 \coloneqq \max_{\|\mathbf{x}\|_2=1} \|\mathbf{M}\mathbf{x}\|_2$. We will use the following bound for the largest singular value of a short matrix.

Lemma 2.1 ([Lan23, Lemma 1])**.** Let $n, m \in \mathbb{N}$, $\beta > 0$ be a positive real, and $\mathbf{M} \in \mathbb{R}^{n\times m}$ be a matrix such that $\|\mathbf{M}\|_\infty \leq \beta$. Then, it holds that $\sigma_{\mathsf{max}}(\mathbf{M}) \leq \beta\sqrt{n}$.

Lattices. A lattice $\Lambda \subseteq \mathbb{R}^n$ is the set of all integer-linear combinations of a set of linearly independent basis vectors, i.e, for any lattice Λ, there exists a full-rank matrix $\mathbf{B}^{n\times m}$ such that $\Lambda = \Lambda(\mathbf{B}) = \{\mathbf{B}\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^m\}$. We call m the rank of Λ and $\mathbf{B}$ a basis of Λ, and we say that Λ is full-rank if $m = n$. The dual of a lattice Λ

is $\Lambda^* \coloneqq \{ \mathbf{w} \in \mathbb{R}^n \mid \forall \mathbf{v} \in \Lambda : \mathbf{v}^\top \mathbf{w} \in \mathbb{Z} \}$. Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ for some $n, m, q \in \mathbb{N}$, we can define the following q-ary lattices:

$$\Lambda_q(\mathbf{A}) \coloneqq \{ \mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}^\top \mathbf{s} \bmod q \text{ for some } \mathbf{s} \in \mathbb{Z}^n \},$$
$$\Lambda_q^\perp(\mathbf{A}) \coloneqq \{ \mathbf{y} \in \mathbb{Z}^m : \mathbf{A}\mathbf{y} = \mathbf{0} \bmod q \}.$$

In this paper, we will deal with lattices of the form $\mathcal{R}^k$ and $\mathcal{R}_q^k$, where $\mathcal{R} \coloneqq \mathbb{Z}[X]/(X^n + 1)$ and $\mathcal{R}_q \coloneqq \mathcal{R}/q\mathcal{R}$ for $q \in \mathbb{N}$ are rings. The ring $\mathcal{R}$ becomes a lattice through the coefficient embedding $\psi : \mathcal{R} \to \mathbb{Z}^n$ that maps every $a = \sum_{i=0}^{n-1} a_i X^i \in \mathcal{R}$ to its coefficient vector $\psi(a) = (a_0, \ldots, a_{n-1})^\top \in \mathbb{Z}^n$. We extend ψ component-wise to vectors and matrices over $\mathcal{R}$. The embedding also induces a norm on the ring elements $\mathbf{a} \in \mathcal{R}^k$. That is, we define $\|\mathbf{a}\|_\infty \coloneqq \|\psi(\mathbf{a})\|_\infty$. The multiplication in $\mathcal{R}$ translates into a matrix-vector multiplication once embedded with ψ. For all $a, b \in \mathcal{R}$, we can write $\psi(a \cdot b)$ as $\mathsf{Rot}(a) \cdot \psi(b)$, where $\mathsf{Rot}(a)$ is defined as

$$\mathsf{Rot}(a) = (\psi(a), \psi(aX), \ldots, \psi(aX^{n-1})) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & -a_{n-1} \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix} \in \mathbb{Z}^{n \times n},$$

which is itself a nega-circulant matrix. We also extend Rot component-wise to vectors and matrices over $\mathcal{R}$. Let $\mathbf{I}_{\mathbb{Z},k} \in \mathbb{Z}^{k \times k}$ and $\mathbf{I}_{\mathcal{R},k} \in \mathcal{R}^{k \times k}$ be identity matrices on $\mathbb{Z}$ and $\mathcal{R}$, respectively.

Gaussian. Let $\mathbf{\Sigma} \in \mathbb{R}^{n \times n}$ be a positive definite matrix, we define the Gaussian function $\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{x}) \coloneqq \exp(-\pi \mathbf{x}^\top \mathbf{\Sigma}^{-1} \mathbf{x})$ for any $\mathbf{x} \in \mathbb{R}^n$. For a lattice $\Lambda \subseteq \mathbb{R}^n$, we define the discrete Gaussian distribution

$$\mathcal{D}_{\Lambda, \sqrt{\mathbf{\Sigma}}}(\mathbf{x}) \coloneqq \frac{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{x})}{\rho_{\sqrt{\mathbf{\Sigma}}}(\Lambda)}$$

for any $\mathbf{x} \in \mathbb{R}^n$, where $\rho_{\sqrt{\mathbf{\Sigma}}}(\Lambda) \coloneqq \sum_{\mathbf{y} \in \Lambda} \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{y})$. When $\mathbf{\Sigma} = \sigma^2 \mathbf{I}_{\mathbb{Z},n}$ for a positive real $\sigma \in \mathbb{R}$, we use σ as subscript instead of $\sqrt{\mathbf{\Sigma}}$. For a ring $\mathcal{R}$, we write $\mathcal{D}_{\mathcal{R}, \sqrt{\mathbf{\Sigma}}}$ for the distribution that samples $z \in \mathcal{R}$ with probability $\rho_{\psi(\mathcal{R}),\sigma}(\psi(z))$. As coined by [MR07], we define the smoothing parameter of a lattice Λ, parameterized by $\epsilon > 0$, by

$$\eta_\epsilon(\Lambda) \coloneqq \min \{ s > 0 \mid \rho_{1/s}(\Lambda^* \setminus \{ \mathbf{0} \}) \leq \epsilon \}.$$

We will use the following properties of discrete Gaussian distributions and the smoothing parameter.

Lemma 2.2 ([Lyu12])**.** It holds that

$$\Pr_{z \leftarrow\$ \mathcal{D}_{\mathcal{R},\sigma}} [\|z\|_\infty > \sqrt{\lambda}\sigma] = \mathsf{negl}(\lambda).$$

Lemma 2.3 ([Pei08, Lemma 3.5])**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice with basis $\mathbf{B}$, and let $\epsilon \in (0, 1)$. Then, it holds that

$$\eta_\epsilon(\Lambda) \leq \frac{\sqrt{\ln(2n(1 + 1/\epsilon))/\pi}}{\lambda_1^\infty(\Lambda^*)},$$

where $\lambda_1^\infty(\Lambda^*)$ is the infinity norm of the shortest vector of Λ^*.

Lemma 2.4 ([MKMS21, Lemma 9])**.** Let $n \geq 4$ be a power of 2 such that $X^n + 1$ splits into n linear factors modulo prime p and $\mathcal{R}_p = \mathbb{Z}_p[X]/(X^n + 1)$. Then, it holds that

$$\lambda_1^\infty(\Lambda_p(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A})) \geq \frac{1}{\sqrt{n}} \cdot p^{1 - \frac{k}{k+\ell} - \frac{\epsilon}{k}}$$

except for a fraction of at most $2^n / p^{\epsilon n}$ of all $\mathbf{A} \in \mathcal{R}_p^{k \times \ell}$.

Lemma 2.5 ([AGJ+24, Lemma 2.6]). Let $k, \ell, q \in \mathbb{N}$, and $\mathbf{A} \in \mathcal{R}_q^{k\times\ell}$ such that $\mathbf{A}\mathcal{R}_q^{\ell} = \mathcal{R}_q^k$. Then, let $\epsilon > 0$ be a negligible in λ and $\mathbf{\Sigma} \in \mathbb{R}^{n\ell\times n\ell}$ such that $\mathbf{\Sigma} - \eta_\epsilon(\Lambda_q^\perp(\mathbf{A}))^2 \cdot \mathbf{I}_{\mathbb{Z},n\ell}$ is positive semi-definite. Then, it holds that

$$\{\, \mathbf{u} : \mathbf{x} \leftarrow\!\$\, \mathcal{D}^{\ell}_{\mathcal{R},\sqrt{\mathbf{\Sigma}}}, \mathbf{u} \coloneqq \mathbf{A}\mathbf{x} \bmod q \,\} \approx_s \{\, \mathbf{u} : \mathbf{u} \leftarrow\!\$\, \mathcal{R}_q^k \,\}.$$

Lemma 2.6 ([DKL+23, Theorem 2], simplified by [Lan23]). Let $k \in \mathbb{N}$, $\beta > 0$ be a positive real, and $\epsilon > 0$ be negligible in λ. Let $\mathbf{z} \in \mathcal{R}^k$ be a vector such that $\|\mathbf{z}\|_\infty \leq \beta$. Further let $\sigma_0, \tau_0 \in \mathbb{R}$ and $s, t \geq 2\sqrt{2}$ be positive reals such that $\sigma_0 \geq \eta_\epsilon(\mathcal{R}^m)$, $\tau_0 \geq \eta_\epsilon(\mathcal{R})$, and

$$t\tau_0 \geq \frac{\sqrt{(s^2+1)(s^2+2)}}{s}\sigma_0\beta.$$

Then, for $\sigma \coloneqq \sqrt{(s^2+1)}\sigma_0$, $\tau \coloneqq \sqrt{(t^2+1)}\tau_0$, and $\sigma^* \coloneqq s/2 \cdot \sigma_0$, there exists an efficiently sampleable distribution $\mathcal{F}$ on $\mathcal{R}^m \times \mathcal{R}$ such that

$$\left\{ (\mathbf{r}_1, \mathbf{z}^\top \mathbf{r}_1 + r_2) : \begin{array}{l} \mathbf{r}_1 \leftarrow\!\$\, \mathcal{D}^k_{\mathcal{R},\sigma}, \\ r_2 \leftarrow\!\$\, \mathcal{D}_{\mathcal{R},\tau} \end{array} \right\} \approx_s \left\{ (\mathbf{r} + \mathbf{f}_1, f_2) : \begin{array}{l} \mathbf{r} \leftarrow\!\$\, \mathcal{D}^k_{\mathcal{R},\sigma^*}, \\ (\mathbf{f}_1, f_2) \leftarrow\!\$\, \mathcal{F} \end{array} \right\}.$$

Approximate Trapdoor. Chen et al. [YJW23] proposed a compact approximate trapdoor for *integer* or *ideal* lattices. We recall their results.

Lemma 2.7 ([YJW23, Theorem 2]). Let $n, p, q, Q \in \mathbb{N}$ such that $Q = pq$. There exists a probabilistic polynomial time (PPT) algorithm $\mathsf{AppSampPre}\mathbb{Z}(\cdot,\cdot,\cdot,\cdot)$ satisfying the following: Let $\mathbf{A} \in \mathbb{Z}_Q^{n\times 3n}$ and $\mathbf{T} \in \mathbb{Z}^{3n\times n}$ be matrices such that $\mathbf{A}\mathbf{T} = p \cdot \mathbf{I}_{\mathbb{Z},n} \bmod Q$, $\mathsf{Approx}\mathbb{Z}.\mathbf{A}^{-1}(\cdot)$ denote $\mathsf{AppSampPre}\mathbb{Z}(\mathbf{A}, \mathbf{T}, \cdot, \sigma_1)$. Then, it holds that

$$\left\{ (\mathbf{A}, \mathbf{x}, \mathbf{y}, \mathbf{z}) : \begin{array}{l} \mathbf{y} \leftarrow\!\$\, \mathbb{Z}_Q^n, \\ \mathbf{x} \leftarrow\!\$\, \mathsf{Approx}\mathbb{Z}.\mathbf{A}^{-1}(\mathbf{y}), \\ \mathbf{z} \coloneqq \mathbf{y} - \mathbf{A}\mathbf{x} \bmod Q \end{array} \right\} \approx_s \left\{ (\mathbf{A}, \mathbf{x}, \mathbf{y}, \mathbf{z}) : \begin{array}{l} \mathbf{x} \leftarrow\!\$\, \mathcal{D}^{3n}_{\mathbb{Z},\sigma_1}, \\ \mathbf{z} \leftarrow\!\$\, \mathbb{Z}_p^n, \\ \mathbf{y} \coloneqq \mathbf{A}\mathbf{x} + \mathbf{z} \bmod Q \end{array} \right\}$$

for any $\sigma_1^2 \geq (q^2+1) \cdot (\sigma_{\mathsf{max}}(\mathbf{T})^2 + 1) \cdot \eta_\epsilon(\mathbb{Z}^n)$.

Module Learning with Errors. We recall the module learning with errors (MLWE) assumption.

Definition 2.8 (Module Learning with Errors (MLWE) [LS15]). Let $k, \ell, q \in \mathbb{N}$ and χ be an error distribution on $\mathcal{R}$. We say that the module learning with errors (MLWE) problem $\mathsf{MLWE}_{k,\ell,q,\chi}$ is hard if for any PPT algorithm $\mathcal{A}$, it holds that

$$\mathsf{Adv}^{\mathsf{MLWE}}_{k,\ell,q,\chi}(\lambda, \mathcal{A}) \coloneqq |\Pr[\mathcal{A}(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}) = 1] - \Pr[\mathcal{A}(\mathbf{A}, \mathbf{u}) = 1]| = \mathsf{negl}(\lambda),$$

where $\mathbf{A} \leftarrow\!\$\, \mathcal{R}_q^{k\times\ell}$, $\mathbf{s} \leftarrow\!\$\, \chi^\ell$, $\mathbf{e} \leftarrow\!\$\, \chi^k$, and $\mathbf{u} \leftarrow\!\$\, \mathcal{R}_q^k$. We write $\mathsf{MLWE}_{k,\ell,q,\sigma}$ as a shorthand for $\mathsf{MLWE}_{k,\ell,q,\chi}$ when $\chi = \mathcal{D}_{\mathcal{R},\sigma}$.

Lemma 2.9 (Hardness of MLWE [LS15]). For any integers k, ℓ, and q and real σ such that $q \leq \mathsf{poly}(\ell n)$, $k \leq \mathsf{poly}(\ell)$, and $\sigma \geq \sqrt{\ell} \cdot \omega(\sqrt{\log n})$, the $\mathsf{MLWE}_{k,\ell,q,\sigma}$ problem is as hard as the worst-case lattice generalized-independent-vector-problem in dimension $N = k\ell$ with approximation factor $\sqrt{8N\ell} \cdot \omega(\sqrt{\log n}) \cdot q/\sigma$.

2.2 Identity-Based Encryption

Here, we review the definition of identity-based encryption (IBE) by following [BF01, KYY21].

Syntax. An IBE scheme Π consists of the following four PPT algorithms.

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{msk}, \mathsf{mpk})$: The setup algorithm takes the security parameter λ as input and outputs a master secret key msk and a master public key mpk. It is assumed that the descriptions of the message space $\mathcal{M}$ and the identity space $\mathcal{ID}$ are implicitly included in mpk.
- $\mathsf{KGen}(\mathsf{msk}, \mathsf{mpk}, \mathsf{id}) \to \mathsf{sk}$: The key-generation algorithm takes the master secret key msk, the master public key mpk, and an identity $\mathsf{id} \in \mathcal{ID}$ as input, and outputs a secret key $\mathsf{sk}_{\mathsf{id}}$. It is assumed that id is implicitly included in $\mathsf{sk}_{\mathsf{id}}$.
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mathsf{M}) \to \mathsf{ct}$: The encryption algorithm takes the master public key mpk, an identity $\mathsf{id} \in \mathcal{ID}$, and a message $\mathsf{M} \in \mathcal{M}$, and outputs a ciphertext ct.
- $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) \to \mathsf{M}$: The decryption algorithm takes a secret key $\mathsf{sk}_{\mathsf{id}}$ and a ciphertext ct and outputs a message M.

Correctness. We require that for all all $\lambda \in \mathbb{N}$, $\mathsf{id} \in \mathcal{ID}$, and $\mathsf{M} \in \mathcal{M}$, it holds that

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) = \mathsf{M} : \begin{array}{l} (\mathsf{mpk}, \mathsf{msk}) \leftarrow\$\ \mathsf{Setup}(1^\lambda) \\ \mathsf{sk}_{\mathsf{id}} \leftarrow\$\ \mathsf{KGen}(\mathsf{msk}, \mathsf{mpk}, \mathsf{id}) \\ \mathsf{ct} \leftarrow\$\ \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mathsf{M}) \end{array}\right] = 1 - \mathsf{negl}(\lambda).$$

Security. Let Π be an IBE scheme. The adaptive-identity anonymity is defined via a game between an adversary $\mathcal{A}$ and the challenger $\mathcal{C}$.

1. Setup Phase: $\mathcal{C}$ first runs $(\mathsf{msk}, \mathsf{mpk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and gives mpk to $\mathcal{A}$. It then prepares a set $\mathcal{Q}_{\mathsf{sk}} := \emptyset$.
2. Query Phase: $\mathcal{A}$ may adaptively make the following two types of queries to $\mathcal{C}$:

   Key generation query: Upon a query $\mathsf{id} \in \mathcal{ID}$ from $\mathcal{A}$, $\mathcal{C}$ checks if $(\mathsf{id}, *) \notin \mathcal{Q}_{\mathsf{sk}}$, and returns $\perp$ to $\mathcal{A}$ if this is not the case. Otherwise, $\mathcal{C}$ computes $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KGen}(\mathsf{msk}, \mathsf{mpk}, \mathsf{id})$, stores $(\mathsf{id}, \mathsf{sk}_{\mathsf{id}})$ in $\mathcal{Q}_{\mathsf{sk}}$, and returns it to $\mathcal{A}$.

   Challenge query: $\mathcal{A}$ is allowed to make this query only once. Upon a query $(\mathsf{id}^*, \mathsf{M}) \in \mathcal{ID} \times \mathcal{M}$ from $\mathcal{A}$, $\mathcal{C}$ checks if $(\mathsf{id}^*, *) \notin \mathcal{Q}_{\mathsf{sk}}$, and returns $\perp$ to $\mathcal{A}$ if this is not the case. Otherwise, $\mathcal{C}$ stores $(\mathsf{id}^*, \perp)$ in $\mathcal{Q}_{\mathsf{sk}}$ and chooses $\mathsf{coin} \leftarrow\$\ \{0, 1\}$. If $\mathsf{coin} = 0$, it runs $\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*, \mathsf{M}^*)$. Otherwise, it randomly samples ct^* from a ciphertext space. Finally, $\mathcal{C}$ returns ct^* to $\mathcal{A}$.
3. Guess Phase: At some point, $\mathcal{A}$ outputs a guess $\widehat{\mathsf{coin}} \in \{0, 1\}$ for coin and terminates.

The above completes the description of the game. In this game, the advantage of $\mathcal{A}$ is defined as

$$\mathsf{Adv}_{\Pi}^{\mathsf{IBE}}(\lambda, \mathcal{A}) := |\Pr[\widehat{\mathsf{coin}} = \mathsf{coin}] - 1/2|.$$

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

3 New Results on Module Lattices

In this section, we present our new results on module lattices, which are employed in the security proof of our IBE scheme and may be of independent interest.

3.1 Module-LWE with an Adaptive Hint

Here, we introduce a variant of the MLWE assumption which allows an adversary to *adaptively* learn both the leakages of the MLWE secret and error. This assumption extends MLWE with error-leakage (elMLWE), introduced in [DKL+23].

Definition 3.1 (MLWE with an Adaptive Hint (ahMLWE))**.** Let $k, \ell, q \in \mathbb{N}$, $\beta > 0$ be a positive real, and χ and χ' be error distributions on $\mathcal{R}$. The MLWE with adaptive hint (ahMLWE) problem $\mathsf{ahMLWE}_{k,\ell,q,\chi,\chi',\beta}$ is defined via the following experiment, where $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is a two-stage PPT algorithm.

1. The challenger $\mathcal{C}$ samples $\mathbf{A} \leftarrow\$ \mathcal{R}_q^{k\times\ell}$ and provides $\mathbf{A}$ to $\mathcal{A}_1$.
2. $\mathcal{A}_1$ sends $\mathbf{z} \in \mathcal{R}^{k+\ell}$ such that $\|\mathbf{z}\|_\infty \le \beta$ to $\mathcal{C}$.
3. $\mathcal{C}$ samples $\mathbf{s} \leftarrow\$ \chi^\ell$, $\mathbf{e} \leftarrow\$ \chi^k$, and $e' \leftarrow\$ \chi'$ and sets $h \coloneqq \mathbf{z}^\top \begin{pmatrix}\mathbf{s}\\ \mathbf{e}\end{pmatrix} + e' \bmod q$.
4. $\mathcal{C}$ chooses a random bit $b \leftarrow\$ \{0,1\}$.
5. If $b = 0$, $\mathcal{C}$ sets $\mathbf{u} \coloneqq \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$, otherwise, $\mathcal{C}$ samples $\mathbf{u} \leftarrow\$ \mathcal{R}_q^k$.
6. $\mathcal{C}$ now runs $\mathcal{A}_2$ on input $(\mathbf{A}, \mathbf{u}, h)$, upon which $\mathcal{A}_2$ outputs a bit b'.

We say that $\mathsf{ahMLWE}_{k,\ell,q,\chi,\chi',\beta}$ is hard if every PPT algorithm $\mathcal{A}$, it holds that

$$\mathsf{Adv}^{\mathsf{ahMLWE}}_{k,\ell,q,\chi,\chi',\beta}(\lambda, \mathcal{A}) \coloneqq \Pr[b = b'] = \frac{1}{2} + \mathsf{negl}(\lambda)$$

in the above experiment. We may write $\mathsf{ahMLWE}_{k,\ell,q,\sigma,\sigma',\beta}$ as a shorthand for $\mathsf{ahMLWE}_{k,\ell,q,\chi,\chi',\beta}$ when $\chi = \mathcal{D}_{\mathcal{R},\sigma}$ and $\chi = \mathcal{D}_{\mathcal{R},\sigma'}$.

We prove that the standard MLWE implies the ahMLWE tightly with only a small parameter loss for suitable discrete Gaussian distributions.

Theorem 3.2 (Hardness of ahMLWE)**.** Let $\beta > 0$ be a parameter and $\epsilon > 0$ be negligible in λ. Let $\sigma_0, \sigma, \sigma^*, \tau_0, \tau \in \mathbb{R}$ and $s, t \ge 2\sqrt{2}$ be positive reals such that as in the statement in Lemma 2.6. Then, assuming that $\mathsf{MLWE}_{k,\ell,q,\sigma^*}$ is hard, $\mathsf{ahMLWE}_{k,\ell,q,\sigma,\tau,\beta}$ is also hard.

More precisely, for any PPT algorithm $\mathcal{A}$, there exists a PPT algorithm $\mathcal{B}$ such that

$$\mathsf{Adv}^{\mathsf{ahMLWE}}_{k,\ell,q,\sigma,\tau,\beta}(\lambda, \mathcal{A}) = \mathsf{Adv}^{\mathsf{MLWE}}_{k,\ell,q,\sigma^*}(\lambda, \mathcal{B}) + \mathsf{negl}(\lambda).$$

Proof. The proof is almost identical to that of [DKL+23, Theorem 3]. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a PPT algorithm against the ahMLWE assumption and $\mathcal{F}$ be a distribution on $\mathcal{R}^{\ell+k} \times \mathcal{R}$ as in the statement in Lemma 2.6. We will construct the algorithm $\mathcal{B}$ as follows:

- Given an MLWE sample $(\mathbf{A}, \mathbf{u})$, provide $\mathbf{A}$ to $\mathcal{A}_1$, which outputs vectors $\mathbf{z}_0$ and $\mathbf{z}_1$.
- Sample $(\mathbf{f}_1, f_2) \leftarrow\$ \mathcal{F}$.
- Compute $\mathbf{u}' \coloneqq \mathbf{u} + (\mathbf{A}\|\mathbf{I}_{\mathcal{R},k})\mathbf{f}_1$ and $h \coloneqq f_2$.
- Run $\mathcal{A}_2$ on input $(\mathbf{A}, \mathbf{u}, \mathbf{h})$ and output whatever $\mathcal{A}_2$ outputs.

If $(\mathbf{A}, \mathbf{u})$ is a well-formed $\mathsf{MLWE}_{k,\ell,q,\sigma^*}$ sample, it holds that $\mathbf{u} = \mathbf{A}\mathbf{s} + \mathbf{e}$, where $\mathbf{s} \leftarrow\$ \mathcal{D}^\ell_{\mathcal{R},\sigma^*}$ and $\mathbf{e} \leftarrow\$ \mathcal{D}^k_{\mathcal{R},\sigma^*}$. Consequently, by Lemma 2.6, it holds that

$$(\mathbf{A}, \mathbf{u}', \mathbf{h}) \equiv \left(\mathbf{A}, (\mathbf{A}\|\mathbf{I}_{\mathcal{R},k})\left(\begin{pmatrix}\mathbf{s}\\ \mathbf{e}\end{pmatrix} + \mathbf{f}_1\right), f_2\right)$$

$$\approx_s (\mathbf{A}, (\mathbf{A}\|\mathbf{I}_{\mathcal{R},k})\mathbf{r}_1, \mathbf{z}^\top \mathbf{r}_1 + r_2),$$

where $\mathbf{r}_1 \leftarrow\$ \mathcal{D}^{k+\ell}_{\mathcal{R},\sigma}$ and $\mathbf{r}_2 \leftarrow\$ \mathcal{D}_{\mathcal{R},\tau}$. In this case, the sample computed by $\mathcal{B}$ is statistically close to a sample of $\mathsf{ahMLWE}_{k,\ell,q,\sigma,\tau,\beta}$ for $b = 0$.

On the other hands, if $\mathbf{u}$ is distributed uniformly random, we can write $\mathbf{u}$ as $\mathbf{u} = \mathbf{y}+\mathbf{A}\mathbf{s}+\mathbf{e}$ for a uniform random $\mathbf{y} \leftarrow\$ \mathcal{R}^k_q$, $\mathbf{s} \leftarrow\$ \mathcal{D}^{\ell}_{\mathcal{R},\sigma^*}$, and $\mathbf{e} \leftarrow\$ \mathcal{D}^k_{\mathcal{R},\sigma^*}$. Consequently, in this case, it holds also by Lemma 2.6 that

$$\begin{aligned}(\mathbf{A}, \tilde{\mathbf{u}}, \mathbf{h}) &\equiv \left(\mathbf{A}, (\mathbf{A}\|\mathbf{I}_{\mathcal{R},k}) \left(\begin{pmatrix}\mathbf{s}\\ \mathbf{e}\end{pmatrix} + \mathbf{f}_1\right), f_2\right)\\ &\approx_s (\mathbf{A}, \mathbf{y} + (\mathbf{A}\|\mathbf{I}_{\mathcal{R},k})\mathbf{r}_1, \mathbf{z}^\top \mathbf{r}_1 + r_2)\\ &\equiv (\mathbf{A}, \mathbf{u}', \mathbf{z}^\top \mathbf{r}_1 + r_2),\end{aligned}$$

where $\mathbf{u}' \in \mathcal{R}^k_q$ is a uniformly random vector. In this case, the sample computed by $\mathcal{B}$ is statistically close to a sample of $\mathsf{ahMLWE}_{k,\ell,q,\sigma,\tau,\beta}$ for $b = 1$. Putting these two facts together, we have

$$\mathsf{Adv}^{\mathsf{ahMLWE}}_{k,\ell,q,\sigma,\tau,\beta}(\lambda, \mathcal{A}) = \mathsf{Adv}^{\mathsf{MLWE}}_{k,\ell,q,\sigma^*}(\lambda, \mathcal{B}) + \mathsf{negl}(\lambda).$$

□

3.2 Gaussian Regularity with Leakage

Here, we provide a new Gaussian regularity with leakage over $\mathcal{R}_Q$, where Q is not a prime but *almost prime*. Our result generalizes the previous result in [SS11, SS13, MKMS21, MKMS22].

Theorem 3.3 (Gaussian Regularity with leakage)**.** Let $n, k, \ell, p, q, Q = pq \in \mathbb{N}$ such that $n \geq 4$ is a power of 2 and $X^n + 1$ splits into n linear factors modulo prime p, $\epsilon > 0$ be negligible in λ, and $\sigma, \tau \in \mathbb{R}$ be a positive real such that $\sigma, \tau \geq q\sqrt{n \ln(2n(k+1+\ell)(1+1/\epsilon))/\pi} \cdot p^{\frac{k+1}{k+1+\ell} + \frac{\epsilon}{k+1}}$. Then, it holds that

$$\left\{ (\mathbf{A}, \mathbf{c}, \mathbf{y}, c) : \begin{array}{l} \mathbf{x} \leftarrow\$ \mathcal{D}^{\ell}_{\mathcal{R},\sigma}, \\ \mathbf{z} \leftarrow\$ \mathcal{D}^{k}_{\mathcal{R},\sigma}, \\ e \leftarrow\$ \mathcal{D}_{\mathcal{R},\tau}, \\ \mathbf{y} := \mathbf{A}\mathbf{x} + \mathbf{z} \bmod Q, \\ \boxed{c := \mathbf{c}^\top \mathbf{x} + e \bmod Q} \end{array} \right\} \approx_s \left\{ (\mathbf{A}, \mathbf{c}, \mathbf{y}, c) : \begin{array}{l} \mathbf{x} \leftarrow\$ \mathcal{D}^{\ell}_{\mathcal{R},\sigma}, \\ \mathbf{z} \leftarrow\$ \mathcal{D}^{k}_{\mathcal{R},\sigma}, \\ \mathbf{y} := \mathbf{A}\mathbf{x} + \mathbf{z} \bmod Q, \\ \boxed{c \leftarrow\$ \mathcal{R}_Q} \end{array} \right\},$$

where $\mathbf{A} \leftarrow\$ \mathcal{R}^{k\times\ell}_Q$ and $\mathbf{c} \leftarrow\$ \mathcal{R}^{\ell}_Q$.

Proof. By Lemma 3.4 and the parameter condition, we have

$$\begin{aligned}\sigma, \tau &\geq p\sqrt{n \ln(2n(k+1+\ell)(1+1/\epsilon))/\pi} \cdot q^{\frac{k+1}{k+1+\ell} + \frac{\epsilon}{k+1}}.\\ &\geq \max\left\{ \eta_\epsilon\left(\Lambda^\perp_Q\left(\mathbf{I}_{\mathcal{R},k+1} \quad \begin{matrix}\mathbf{A}\\ \mathbf{c}^\top\end{matrix}\right)\right), \eta_\epsilon(\Lambda^\perp_Q(\mathbf{I}_{\mathcal{R},k}\|\mathbf{A}))\right\}.\end{aligned}$$

This implies that the following matrices are positive semi-definite:

$$\begin{aligned}\begin{pmatrix}\sigma^2 \cdot \mathbf{I}_{\mathbb{Z},nk} & \mathbf{0}\\ \mathbf{0} & \tau^2\end{pmatrix} - \eta_\epsilon\left(\Lambda^\perp_Q\left(\mathbf{I}_{\mathcal{R},k+1} \quad \begin{matrix}\mathbf{A}\\ \mathbf{c}^\top\end{matrix}\right)\right)^2 \cdot \mathbf{I}_{\mathbb{Z},nk+1} &\in \mathbb{R}^{(nk+1)\times(nk+1)},\\ (\sigma^2 - \eta_\epsilon(\Lambda^\perp_Q(\mathbf{I}_{\mathcal{R},k+1}\|\mathbf{A}))^2) \cdot \mathbf{I}_{\mathbb{Z},nk} &\in \mathbb{R}^{nk\times nk}.\end{aligned}$$

Therefore, by using Lemma 2.5 twice, we have

$$\left\{ (\mathbf{A}, \mathbf{c}, \mathbf{y}, c) : \begin{array}{l} \mathbf{x} \leftarrow\$ \mathcal{D}^{\ell}_{\mathcal{R},\sigma}, \\ \mathbf{z} \leftarrow\$ \mathcal{D}^{k}_{\mathcal{R},\sigma}, \\ e \leftarrow\$ \mathcal{D}_{\mathcal{R},\tau}, \\ \mathbf{y} := \mathbf{A}\mathbf{x} + \mathbf{z} \bmod Q, \\ c := \mathbf{c}^\top \mathbf{x} + e \bmod Q \end{array} \right\} \approx_s \left\{ (\mathbf{A}, \mathbf{c}, \mathbf{y}, c) : \begin{array}{l} \boxed{\mathbf{y} \leftarrow\$ \mathcal{R}^k_Q}, \\ \boxed{c \leftarrow\$ \mathcal{R}_Q} \end{array} \right\}$$

$$\approx_s \left\{ (\mathbf{A}, \mathbf{c}, \mathbf{y}, c) : \begin{array}{l} \mathbf{x} \leftarrow\$\, \mathcal{D}^{\ell}_{\mathcal{R},\sigma}, \\ \mathbf{z} \leftarrow\$\, \mathcal{D}^{k}_{\mathcal{R},\sigma}, \\ \boxed{\mathbf{y} := \mathbf{A}\mathbf{x} + \mathbf{z} \bmod Q}, \\ c \leftarrow\$\, \mathcal{R}_Q \end{array} \right\}.$$

□

We show the following lemma to complete the proof of Theorem 3.3.

Lemma 3.4. Let $n, k, \ell, p, q \in \mathbb{N}$ such that $n \geq 4$ is a power of 2 and $X^n + 1$ splits into n linear factors modulo prime p, and $\epsilon \in (0, 1)$ be a positive real. Then, it holds that

$$\eta_\epsilon(\Lambda^{\perp}_{pq}(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A})) \leq q \cdot \sqrt{n \ln(2n(k+\ell)(1+1/\epsilon))/\pi} \cdot p^{\frac{k}{k+\ell} + \frac{\epsilon}{k}}.$$

with all but negligible probability, where $\mathbf{A} \leftarrow\$\, \mathcal{R}^{k \times \ell}_{pq}$.

Proof. By Lemma 2.3, we have

$$\begin{aligned} \eta_\epsilon\left(\Lambda^{\perp}_{pq}(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A})\right) &\leq \frac{\sqrt{\ln(2n(k+\ell)(1+1/\epsilon))/\pi}}{\lambda^{\infty}_1(\Lambda^{\perp}_{pq}(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A})^*)} \\ &= \frac{\sqrt{\ln(2n(k+\ell)(1+1/\epsilon))/\pi}}{\frac{1}{pq} \cdot \lambda^{\infty}_1(\Lambda_{pq}(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A}))}. \end{aligned}$$

Since $\Lambda_{pq}(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A}) \subseteq \Lambda_p(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A})$, we have $\lambda^{\infty}_1(\Lambda_{pq}(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A})) \geq \lambda^{\infty}_1(\Lambda_p(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A}))$. By Lemma 2.4, we have

$$\lambda^{\infty}_1(\Lambda_p(\mathbf{I}_{\mathcal{R},k} \| \mathbf{A})) \geq \frac{1}{\sqrt{n}} \cdot p^{1 - \frac{k}{k+\ell} - \frac{\epsilon}{k}}$$

for a uniformly random matrix $\mathbf{A}$ with all but negligible probability. Combining the above completes our proof of the lemma. □

3.3 Compact Approximate Trapdoor for Module Lattices

Chen et al. [YJW23] proposed a compact approximate trapdoor for *integer* or *ideal* lattices. We extend their results to the *module* lattice setting.

Theorem 3.5 (Compact Approximate Trapdoor for Module Lattices)**.** Let $n, p, q, Q \in \mathbb{N}$ such that $Q = pq$. There exists PPT algorithms $(\mathsf{AppTrapGen}, \mathsf{AppSampPre})$ satisfying the following:

- $\mathsf{AppTrapGen}(1^k, p, q, \sigma_0)$ takes as input positive integers $k, p, q \in \mathbb{N}$ and a positive real $\sigma_0 > 0$, and returns a matrix-approximate trapdoor pair $(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \in \mathcal{R}^{k \times 2k}_Q \times \mathcal{R}^{2k \times k}$, where $Q = pq$.
- Let $\mathbf{A}$ be generated be $\mathsf{AppTrapGen}$, $\mathsf{Approx}.\mathbf{A}^{-1}(\cdot)$ denote the approximate preimage sampling algorithm, $\mathsf{AppSampPre}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \cdot, \sigma_1)$. The following two distributions are statistically close:

$$\left\{ (\mathbf{A}, \mathbf{x}, \mathbf{y}, \mathbf{z}) : \begin{array}{l} \mathbf{y} \leftarrow\$\, \mathcal{R}^k_Q, \\ \mathbf{x} \leftarrow\$\, \mathsf{Approx}.\mathbf{A}^{-1}(\mathbf{y}), \\ \mathbf{z} := \mathbf{y} - \mathbf{A}\mathbf{x} \bmod Q \end{array} \right\} \approx_s \left\{ (\mathbf{A}, \mathbf{x}, \mathbf{y}, \mathbf{z}) : \begin{array}{l} \mathbf{x} \leftarrow\$\, \mathcal{D}^{2k}_{\mathcal{R},\sigma_1}, \\ \mathbf{z} \leftarrow\$\, (\mathcal{D}_{\mathcal{R},\sigma_1} * \mathcal{R}_p)^k, \\ \mathbf{y} := \mathbf{A}\mathbf{x} + \mathbf{z} \bmod Q \end{array} \right\}$$

  for any $\sigma_1^2 \geq (q^2 + 1) \cdot (3kn\lambda\sigma_0^2 + 1) \cdot \eta_\epsilon(\mathcal{R}^k)$. Furthermore, in the second distribution, $\mathbf{A}$ is computationally indistinguishable from uniform random assuming $\mathsf{MLWE}_{k,k,Q,\sigma_0}$ assumption.

Proof. We first describe $(\mathsf{AppTrapGen}, \mathsf{AppSampPre})$.

- $\mathsf{AppTrapGen}(1^k, p, q, \sigma_0) \to (\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \in \mathcal{R}^{k \times 2k}_Q \times \mathcal{R}^{2k \times k}_Q$:

1. Sample $\bar{\mathbf{A}} \leftarrow\$ \mathcal{R}_Q^{k\times k}$, $\mathbf{S} \leftarrow\$ \mathcal{D}_{\mathcal{R},\sigma_0}^{k\times k}$, and $\mathbf{E} \leftarrow\$ \mathcal{D}_{\mathcal{R},\sigma_0}^{k\times k}$.
2. Compute

$$\mathbf{A} \coloneqq \left(\bar{\mathbf{A}} \| p \cdot \mathbf{I}_{\mathcal{R},k} + \bar{\mathbf{A}}\mathbf{S} + \mathbf{E}\right) \bmod Q \in \mathcal{R}_Q^{k\times 2k}, \qquad \mathbf{T}_{\mathbf{A}} \coloneqq \begin{pmatrix} -\mathbf{E} \\ -\mathbf{S} \end{pmatrix} \in \mathcal{R}^{2k\times k}.$$

3. Output $(\mathbf{A}, \mathbf{T}_{\mathbf{A}})$.

- $\mathsf{AppSampPre}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \mathbf{y}, \sigma_1) \to \mathbf{x} \in \mathcal{R}^{2k}$:

1. Set

$$\mathbf{A}_{\mathbb{Z}} \coloneqq (\mathbf{I}_{\mathbb{Z},kn} \| \mathsf{Rot}(\mathbf{A})) \in \mathbb{Z}_Q^{nk\times 3nk}, \qquad \mathbf{T}_{\mathbb{Z}} \coloneqq \begin{pmatrix} \mathsf{Rot}(\mathbf{T}_{\mathbf{A}}) \\ \mathbf{I}_{\mathbb{Z},nk} \end{pmatrix} \in \mathbb{Z}^{3nk\times nk}.$$

2. Sample $\mathbf{x}_{\mathbb{Z}} \leftarrow\$ \mathsf{AppSampPre}\mathbb{Z}(\mathbf{A}_{\mathbb{Z}}, \mathbf{T}_{\mathbb{Z}}, \psi(\mathbf{y}), \sigma_1)$.
3. Parse $\mathbf{x}_{\mathbb{Z}} = \begin{pmatrix} \overline{\mathbf{x}}_{\mathbb{Z}} \\ \underline{\mathbf{x}}_{\mathbb{Z}} \end{pmatrix} \in \mathbb{Z}^{3nk}$, where $\overline{\mathbf{x}}_{\mathbb{Z}} \in \mathbb{Z}^{kn}$ and $\underline{\mathbf{x}}_{\mathbb{Z}} \in \mathbb{Z}^{2nk}$.
4. Output $\mathbf{x} \coloneqq \psi^{-1}(\underline{\mathbf{x}}_{\mathbb{Z}}) \in \mathcal{R}^{2k}$.

Then, we show that the algorithm $\mathsf{Approx}.\mathbf{A}^{-1}(\cdot) = \mathsf{AppSampPre}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \cdot, \sigma_1)$ correctly works. From the description, we have

$$\begin{aligned}
\mathbf{A}_{\mathbb{Z}}\mathbf{T}_{\mathbb{Z}} &= (\mathbf{I}_{\mathbb{Z},nk} \| \mathsf{Rot}(\mathbf{A})) \cdot \begin{pmatrix} \mathsf{Rot}(\mathbf{T}_{\mathbf{A}}) \\ \mathbf{I}_{\mathbb{Z},kn} \end{pmatrix} \\
&= \left(\mathbf{I}_{\mathbb{Z},nk} \| \mathsf{Rot}(\bar{\mathbf{A}}) \| p \cdot \mathbf{I}_{\mathbb{Z},nk} + \mathsf{Rot}(\bar{\mathbf{A}}\mathbf{S} + \mathbf{E})\right) \cdot \begin{pmatrix} -\mathsf{Rot}(\mathbf{E}) \\ -\mathsf{Rot}(\mathbf{S}) \\ \mathbf{I}_{\mathbb{Z},nk} \end{pmatrix} \\
&= -\mathsf{Rot}(\mathbf{E}) - \mathsf{Rot}(\bar{\mathbf{A}}\mathbf{S}) + p \cdot \mathbf{I}_{\mathbb{Z},nk} + \mathsf{Rot}(\bar{\mathbf{A}}\mathbf{S} + \mathbf{E}) \\
&= p \cdot \mathbf{I}_{\mathbb{Z},nk}.
\end{aligned}$$

Furthermore, by Lemmata 2.1 and 2.2, we have

$$\begin{aligned}
\sigma_1^2 &\geq (q^2+1) \cdot (3kn\lambda\sigma_0^2 + 1) \cdot \eta_\epsilon(\mathcal{R}^k) \\
&\geq (q^2+1) \cdot (\sigma_{\mathsf{max}}(\mathbf{T}_{\mathbb{Z}})^2 + 1) \cdot \eta_\epsilon(\mathcal{R}^k)
\end{aligned}$$

with overwhelming probability. Thus, $\mathsf{AppSampPre}\mathbb{Z}$ correctly works, and we have

$$\mathbf{A}'\mathbf{x}' = (\mathbf{I}_{\mathbb{Z},kn} \| \mathsf{Rot}(\mathbf{A})) \begin{pmatrix} \overline{\mathbf{x}}_{\mathbb{Z}} \\ \underline{\mathbf{x}}_{\mathbb{Z}} \end{pmatrix} = \overline{\mathbf{x}}_{\mathbb{Z}} + \tau(\mathbf{A}\mathbf{x}) = \tau(\mathbf{y}) + \mathbf{z}_{\mathbb{Z}}. \tag{1}$$

Therefore, by setting

$$\mathbf{z} \coloneqq \psi^{-1}(\mathbf{z}_{\mathbb{Z}} - \overline{\mathbf{x}}_{\mathbb{Z}}) \in \mathcal{R}^k, \tag{2}$$

we have $\mathbf{A}\mathbf{x} = \mathbf{y} + \mathbf{z} \bmod Q$. This means that $\mathsf{Approx}.\mathbf{A}^{-1}(\cdot)$ correctly works.

Then, we show that

$$\left\{ (\mathbf{A}, \mathbf{x}, \mathbf{y}, \mathbf{z}) : \begin{array}{l} \mathbf{y} \leftarrow\$ \mathcal{R}_Q^k, \\ \mathbf{x} \leftarrow\$ \mathsf{Approx}.\mathbf{A}^{-1}(\mathbf{y}) \\ \mathbf{z} \coloneqq \mathbf{y} - \mathbf{A}\mathbf{x} \bmod Q \end{array} \right\} \approx_s \left\{ (\mathbf{A}, \mathbf{x}, \mathbf{y}, \mathbf{z}) : \begin{array}{l} \mathbf{x} \leftarrow\$ \mathcal{D}_{\mathcal{R},\sigma_1}^{2k}, \\ \mathbf{z} \leftarrow\$ (\mathcal{D}_{\mathcal{R},\sigma_1} * \mathcal{R}_p)^k, \\ \mathbf{y} \coloneqq \mathbf{A}\mathbf{x} + \mathbf{z} \bmod Q \end{array} \right\}. \tag{3}$$

By Lemma 2.7, we have

$$\left\{ (\mathbf{A}_{\mathbb{Z}}, \mathbf{x}_{\mathbb{Z}}, \mathbf{y}_{\mathbb{Z}}, \mathbf{z}_{\mathbb{Z}}) : \begin{array}{l} \mathbf{y}_{\mathbb{Z}} \leftarrow\!\$\, \mathbb{Z}_Q^n, \\ \mathbf{x}_{\mathbb{Z}} \leftarrow\!\$\, \mathsf{Approx}\mathbb{Z}.\mathbf{A}_{\mathbb{Z}}^{-1}(\mathbf{y}_{\mathbb{Z}}), \\ \mathbf{z}_{\mathbb{Z}} := \mathbf{y}_{\mathbb{Z}} - \mathbf{A}_{\mathbb{Z}}\mathbf{x}_{\mathbb{Z}} \bmod Q \end{array} \right\} \approx_s \left\{ (\mathbf{A}_{\mathbb{Z}}, \mathbf{x}_{\mathbb{Z}}, \mathbf{y}_{\mathbb{Z}}, \mathbf{z}_{\mathbb{Z}}) : \begin{array}{l} \mathbf{x}_{\mathbb{Z}} \leftarrow\!\$\, \mathcal{D}_{\mathbb{Z},\sigma_1}^{3n}, \\ \mathbf{z}_{\mathbb{Z}} \leftarrow\!\$\, \mathbb{Z}_p^n, \\ \mathbf{y}_{\mathbb{Z}} := \mathbf{A}_{\mathbb{Z}}\mathbf{x}_{\mathbb{Z}} + \mathbf{z}_{\mathbb{Z}} \bmod Q \end{array} \right\}. \quad (4)$$

By Equations (1) and (2), The distribution in Equation (3) follows directly from the distribution in Equation (4). Combining the above facts with Lemma 2.7, it holds that the distributions in Equation (3) are statistically close.

Furthermore, $\mathbf{A} = (\bar{\mathbf{A}} \| p \cdot \mathbf{I}_{\mathbb{Z},nk} + \bar{\mathbf{A}}\mathbf{S} + \mathbf{E})$ is computationally indistinguishable from uniform random assuming the $\mathsf{MLWE}_{k,k,Q,\sigma_0}$ assumption, since $\bar{\mathbf{A}}\mathbf{S} + \mathbf{E}$ is pseudorandom under the $\mathsf{MLWE}_{k,k,Q,\sigma_0}$ assumption. □

4 Construction of Our IBE Scheme

In this section, we present our IBE scheme Π.

4.1 Construction

For reference, we provide the parameters of Π in Table 2.

Parameter	Explanation
(p, q, Q)	Modulus $Q = pq$
$\mathcal{R}$, $\mathcal{R}_Q$	Polynomial rings $\mathcal{R} = \mathbb{Z}[X]/(X^n + 1)$ and $\mathcal{R}_Q = \mathcal{R}/Q\mathcal{R}$
k	Dimension of public matrix $\mathbf{A} \in \mathcal{R}_Q^{k \times 2k}$
σ_{msk}	Gaussian parameter for the master secret key $\mathbf{T}_{\mathbf{A}}$
σ_{sk}	Gaussian parameter for secret keys $\mathbf{x}_{\mathsf{id}}$
(σ, τ)	Gaussian parameters for encryption
$\mathcal{M}$	Message space $\mathcal{M} = \{0,1\}^n \subset \mathcal{R}$
ℓ_{id}	Identity-length

Table 2: Overview of parameters and notations used in Π.

Our IBE scheme $\Pi = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ is given as follows. Our scheme uses a hash function H modeled as a (quantum) random oracle in the security proof. $\mathsf{H} : \{0,1\}^{\ell_{\mathsf{id}}} \to \mathcal{R}_Q^k$ maps an identity $\mathsf{id} \in \{0,1\}^{\mathsf{id}}$ to a random vector in $\mathcal{R}_Q^k$.

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{msk}, \mathsf{mpk})$:
  1. Sample $(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \leftarrow\!\$\, \mathsf{AppTrapGen}(1^k, p, q, \sigma_{\mathsf{msk}})$.
  2. Output $(\mathsf{msk} := \mathbf{T}_{\mathbf{A}} \in \mathcal{R}^{2k \times k}, \mathsf{mpk} := \mathbf{A} \in \mathcal{R}_Q^{k \times 2k})$
- $\mathsf{KGen}(\mathsf{msk} = \mathsf{td}_{\mathbf{A}}, \mathsf{mpk} = \mathbf{A}, \mathsf{id} \in \{0,1\}^{\ell_{\mathsf{id}}}) \to \mathsf{sk}_{\mathsf{id}}$:
  1. Compute $\mathbf{y}_{\mathsf{id}} := \mathsf{H}(\mathsf{id})$.
  2. Sample $\mathbf{x}_{\mathsf{id}} \leftarrow\!\$\, \mathsf{AppSampPre}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \mathbf{y}_{\mathsf{id}}, \sigma_{\mathsf{sk}})$.
  3. Output $\mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}} \in \mathcal{R}^{2k}$.
- $\mathsf{Enc}(\mathsf{mpk} = \mathbf{A}, \mathsf{id} \in \{0,1\}^{\ell_{\mathsf{id}}}, \mathsf{M} \in \mathcal{M}) \to \mathsf{ct}$:
  1. Compute $\mathbf{y}_{\mathsf{id}} := \mathsf{H}(\mathsf{id})$.
  2. Sample $\mathbf{r} \leftarrow\!\$\, \mathcal{D}_{\mathcal{R},\sigma}^k$, $\mathbf{e}_1 \leftarrow\!\$\, \mathcal{D}_{\mathcal{R},\sigma}^{2k}$, and $e_2 \leftarrow\!\$\, \mathcal{D}_{\mathcal{R},\tau}$.

3. Compute $\mathbf{c}_1^\top \coloneqq \mathbf{r}^\top \mathbf{A} + \mathbf{e}_1^\top \bmod Q$ and $c_2 \coloneqq \mathbf{r}^\top \mathbf{y}_{\mathsf{id}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \bmod Q$.
4. Output $\mathsf{ct} \coloneqq (\mathbf{c}_1, c_2) \in \mathcal{R}_Q^{2k} \times \mathcal{R}_Q$.

- $\mathsf{Dec}(\mathsf{mpk} = \mathbf{A}, \mathsf{sk}_{\mathsf{id}} = \mathbf{x}_{\mathsf{id}}, \mathsf{ct} = (\mathbf{c}_1, c_2)) \to \mathsf{M}'$:
  1. Output $\mathsf{M}' \coloneqq \lfloor \frac{2}{Q} \rceil \cdot (c_2 - \mathbf{c}_1^\top \mathbf{x}_{\mathsf{id}})$.

4.2 Correctness

Here, we show the correctness of the above IBE scheme Π. Suppose that the ciphertext $\mathsf{ct} = (\mathbf{c}_1, c_2)$ and the secret key $\mathsf{sk}_{\mathsf{id}} = \mathbf{x}_{\mathsf{id}}$ are correctly generated. When the Dec algorithm operates as specified, we have

$$\begin{aligned}
c_2 - \mathbf{c}_1^\top \mathbf{x}_{\mathsf{id}} &= \mathbf{r}^\top \mathbf{y}_{\mathsf{id}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} - (\mathbf{r}^\top \mathbf{A} + \mathbf{e}_1^\top)\mathbf{x}_{\mathsf{id}} \\
&= \mathbf{r}^\top \mathbf{y}_{\mathsf{id}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} - \mathbf{r}^\top \mathbf{A}\mathbf{x}_{\mathsf{id}} + \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}} \\
&= \mathbf{r}^\top \mathbf{y}_{\mathsf{id}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} - \mathbf{r}^\top \mathbf{y}_{\mathsf{id}} - \mathbf{r}^\top \mathbf{z} - \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}} \\
&= \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} + \underbrace{e_2 - \mathbf{r}^\top \mathbf{z} - \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}}}_{\mathsf{noise}}.
\end{aligned}$$

Here, we use the fact that $\mathbf{A}\mathbf{x}_{\mathsf{id}} = \mathbf{y}_{\mathsf{id}} + \mathbf{z} \mod Q$ holds, where $\mathbf{z} \in \mathcal{R}^k$. By Lemma 2.2, $\|\mathbf{r}\|_\infty \le \sqrt{\lambda}\sigma$, $\|\mathbf{e}_1\|_\infty \le \sqrt{\lambda}\sigma$, and $\|e_2\|_\infty \le \sqrt{\lambda}\tau$ hold. In addition, by Theorem 3.5, $\|\mathbf{x}_{\mathsf{id}}\|_\infty \le \sqrt{\lambda}\sigma_{\mathsf{sk}}$ and $\|\mathbf{z}\|_\infty \le p+\sqrt{\lambda}\sigma_{\mathsf{sk}}$. Thus, the infinity norm of noise is bounded by

$$\begin{aligned}
\|\mathsf{noise}\|_\infty &= \|e_2 - \mathbf{r}^\top \mathbf{z} - \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}}\|_\infty \\
&\le \|e_2\|_\infty + \|\mathbf{r}^\top \mathbf{z}\|_\infty + \|\mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}}\|_\infty \\
&\le \sqrt{\lambda}\tau + nk \cdot \|\mathbf{r}\|_\infty \cdot \|\mathbf{z}\|_\infty + 2nk \cdot \|\mathbf{e}_1\|_\infty \cdot \|\mathbf{x}_{\mathsf{id}}\|_\infty \\
&\le \sqrt{\lambda}\tau + nk\sqrt{\lambda}\sigma(p + 3\sqrt{\lambda}\sigma_{\mathsf{sk}}).
\end{aligned}$$

For the correctness, we need $\|\mathsf{noise}\|_\infty \le Q/4$. We will set the parameters below so that the upper bound is less than $Q/4$.

4.3 Asymptotic Parameters

We set the parameters of the scheme Π to satisfy the following conditions:

- $\epsilon = \epsilon(\lambda) > 0$ is negligible.
- $\mathsf{AppTrapGen}$ and $\mathsf{AppSampPre}$ operate properly (Theorem 3.5): That is, $Q = pq$

$$\begin{aligned}
\sigma_{\mathsf{sk}}^2 &\ge (q^2+1) \cdot (3kn\lambda\sigma_{\mathsf{msk}}^2 + 1) \cdot \ln(2nk(1+1/\epsilon))/\pi \\
&\ge (q^2+1) \cdot (3kn\lambda\sigma_{\mathsf{msk}}^2 + 1) \cdot \eta_\epsilon(\mathcal{R}^k)^2.
\end{aligned}$$

- Correctness holds: That is, $Q/4 \ge \sqrt{\lambda}\tau + nk\sqrt{\lambda}\sigma(p + 3\sqrt{\lambda}\sigma_{\mathsf{sk}})$.
- The $\mathsf{MLWE}_{k,k,Q,\sigma_{\mathsf{msk}}}$ assumption holds (Lemma 2.9): That is, $\sigma_{\mathsf{msk}} \ge \sqrt{k} \cdot \omega(\sqrt{\log n})$.
- The $\mathsf{MLWE}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}$ assumption holds (Theorem 3.2): That is, there exists $s, t \ge 2\sqrt{2}$ with
  - $\sigma_0 \ge \sqrt{\ln(2nk(1+1/\epsilon))/\pi} \ge \eta_\epsilon(\mathcal{R}^k)$ and $\tau_0 \ge \sqrt{\ln(2n(1+1/\epsilon))/\pi} \ge \eta_\epsilon(\mathcal{R})$,
  - $t\tau_0 \ge \frac{\sqrt{(s^2+1)(s^2+2)}}{s}\sigma_0(p + \sqrt{\lambda}\sigma_{\mathsf{sk}})$,

– $\sigma := \sqrt{s^2+1}\sigma_0$, $\tau := \sqrt{t^2+1}\tau_0$, and $\sigma^* := s/2 \cdot \sigma_0$,
– the $\mathsf{MLWE}_{k,2k,Q,\sigma^*}$ assumption holds, i.e., $\sigma^* \geq \sqrt{2k} \cdot \omega(\sqrt{\log n})$.

- Conditions for Theorem 3.3 holds: That is, n is a power of 2 and X^n+1 splits into n linear factor modulo prime p, and

$$\tau, \sigma_{\mathsf{sk}} \geq q\sqrt{n \ln\left(2n(3k+1)(1+1/\epsilon)\right)/\pi} \cdot p^{\frac{k+1}{3k+1}+\frac{\epsilon}{k+1}}.$$

Candidate Asymptotic Parameters. We give a set of asymptotic parameters which fit the above conditions.

- $n, k = O(\lambda)$ such that $n \geq \lambda$.
- $\sigma_{\mathsf{msk}} = O(\sqrt{\lambda}) \cdot \omega(\sqrt{\log n})$.
- $\sigma_{\mathsf{sk}} = O(\lambda^{11/2} \ln(\lambda)) \cdot \omega(\log n)$.
- $(\sigma, \tau) = (O(\lambda) \cdot \omega(\sqrt{\log n}), O(\lambda \sigma_{\mathsf{sk}}) \cdot \omega(\sqrt{\log n}))$.
- $(p, q) = (O(\sigma_{\mathsf{sk}}), O(\lambda 7/2) \cdot \omega(\sqrt{\log n}))$.

5 Security Proof in the Random Oracle Model

In this section, we prove the following theorem.

Theorem 5.1. If the $\mathsf{MLWE}_{k,k,Q,\sigma_{\mathsf{msk}}}$ and $\mathsf{ahMLWE}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}$ assumptions hold, our IBE scheme Π in Section 4.1 satisfies adaptive-identity anonymity in the random oracle model. In particular, for any classical PPT adversary $\mathcal{A}$ making at most Q_{H} random oracle queries to H and Q_{id} secret key queries, there exist two classical PPT reduction algorithms $\mathcal{B}_1$ and $\mathcal{B}_2$ such that

$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\Pi}(\lambda) \leq \mathsf{Adv}^{\mathsf{MLWE}}_{k,k,Q,\sigma_{\mathsf{msk}}}(\lambda, \mathcal{B}_1) + \mathsf{Adv}^{\mathsf{ahMLWE}}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}(\lambda, \mathcal{B}_2) + \mathsf{negl}(\lambda).$$

Proof. Let $\mathcal{A}$ be a classical PPT adversary attacking the adaptive-identity anonymity of Π. Without loss of generality, we make some simplifying assumptions about $\mathcal{A}$. First, we assume that whenever $\mathcal{A}$ queries a secret key or asks for a challenge ciphertext, the corresponding id has already been queried to the random oracle H. Second, we assume that $\mathcal{A}$ makes the same query to the same random oracle at most once. Third, we assume that $\mathcal{A}$ does not repeat secret key queries for the same identity more than once.

We show the security of Π via the following games. In each game, we define E_i as the event that $\mathcal{A}$ wins in Game_i.

Game_0 : This is the real security game. At the beginning of the game, the challenger $\mathcal{C}$ first runs $\mathsf{Setup}(1^\lambda)$ to obtain $(\mathsf{mpk}, \mathsf{msk})$ and then gives mpk to $\mathcal{A}$. $\mathcal{C}$ then samples $\mathsf{coin} \leftarrow_\$ \{0,1\}$ and keeps it secret. During the game, $\mathcal{A}$ can make many random oracle and key generation queries and one challenge query. For each query, $\mathcal{C}$ behaves as follows:

- When $\mathcal{A}$ makes a random oracle query to H on id, $\mathcal{C}$ samples a random polynomial $\mathbf{y}_{\mathsf{id}} \leftarrow_\$ \mathcal{R}_Q^k$ and locally stores the tuple $(\mathsf{id}, \mathbf{y}_{\mathsf{id}}, \perp)$, and returns $\mathbf{y}_{\mathsf{id}}$ to $\mathcal{A}$.
- When $\mathcal{A}$ makes a key generation query for id, $\mathcal{C}$ returns $\mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}} \leftarrow_\$ \mathsf{AppSampPre}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \mathbf{y}_{\mathsf{id}}, \sigma_{\mathsf{sk}})$.
- When $\mathcal{A}$ makes the challenge query for the challenge identity id^* and a message M^*, $\mathcal{C}$ returns $\mathsf{ct}^* = (\mathbf{c}_1^*, c_2^*) \leftarrow_\$ \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*, \mathsf{M}^*)$ if $\mathsf{coin} = 0$ and $\mathsf{ct}^* \leftarrow_\$ \mathcal{R}_Q^{2k+1}$ if $\mathsf{coin} = 1$.

At the end of the game, $\mathcal{A}$ outputs a guess $\widehat{\mathsf{coin}}$ for coin. Finally, $\mathcal{C}$ outputs $\widehat{\mathsf{coin}}$.

By definition, we have

$$\left|\Pr[\mathsf{E}_0] - \frac{1}{2}\right| = \left|\Pr[\widehat{\mathsf{coin}} = \mathsf{coin}] - \frac{1}{2}\right| = \mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\Pi}(\lambda).$$

Game_1 : This is the same as Game_0 except how $\mathcal{C}$ answers the random oracle queries. Upon $\mathcal{A}$'s random oracle query on id in Game_1, $\mathcal{C}$ first samples $\mathbf{x}_{\mathsf{id}} \leftarrow\$ \mathcal{D}^{2k}_{\mathcal{R},\sigma_{\mathsf{sk}}}$ and $\mathbf{z}_{\mathsf{id}} \leftarrow\$ (\mathcal{D}_{\mathcal{R},\sigma_{\mathsf{sk}}} * \mathcal{R}_p)^k$ and sets $\mathbf{y}_{\mathsf{id}} := \mathbf{A}\mathbf{x}_{\mathsf{id}} + \mathbf{z}_{\mathsf{id}} \bmod Q$. Then, $\mathcal{C}$ locally stores $(\mathsf{id}, \mathbf{y}_{\mathsf{id}}, (\mathbf{x}_{\mathsf{id}}, \mathbf{z}_{\mathsf{id}}))$ and returns $\mathbf{y}_{\mathsf{id}}$.

Based on our choice of parameters, we can apply Theorem 3.5, which ensures that all $\mathbf{y}_{\mathsf{id}}$ are statistically close to uniform as in Game_0. Thus, the statistical distance between the view of $\mathcal{A}$ in Game_0 and Game_1 is $Q_{\mathsf{H}} \cdot \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda)$. Therefore, we have

$$|\Pr[\mathsf{E}_0] - \Pr[\mathsf{E}_1]| = \mathsf{negl}(\lambda).$$

Game_2 : This is the same as Game_1 except how $\mathcal{C}$ generates secret keys $\mathbf{x}_{\mathsf{id}}$. In particular, $\mathcal{C}$ does not use the trapdoor $\mathbf{T}_{\mathbf{A}}$ to generate them. When $\mathcal{C}$ generates $\mathbf{x}_{\mathsf{id}}$ for id, $\mathcal{C}$ does not run the $\mathsf{AppSampPre}$ algorithm but retrieves the unique tuple $(\mathsf{id}, \mathbf{y}_{\mathsf{id}}, (\mathbf{x}_{\mathsf{id}}, \mathbf{z}_{\mathsf{id}}))$ from local storage and returns $\mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}$.

Based on our choice of parameters, we can apply Theorem 3.5, which ensures that $\mathbf{x}$ in Game_1 sampled by the $\mathsf{AppSampPre}$ algorithms distribute statistically close to $\mathcal{D}^{2k}_{\mathcal{R},\sigma_{\mathsf{sk}}}$ conditioned on $\mathbf{y}_{\mathsf{id}}$. Since $\mathcal{A}$ obtains at most Q_{id} secret keys, we have

$$|\Pr[\mathsf{E}_1] - \Pr[\mathsf{E}_2]| = Q_{\mathsf{id}} \cdot \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda).$$

Game_3 : This is the same as Game_2 except how $\mathcal{C}$ generates a master public key $\mathbf{A}$. In Game_3, $\mathcal{C}$ does not run the $\mathsf{AppTrapGen}$ algorithm but samples a uniformly random matrix $\mathbf{A} \leftarrow\$ \mathcal{R}_Q^{k\times 2k}$. Since $\mathcal{C}$ did not use a master secret key $\mathbf{T}_{\mathbf{A}}$ to answer $\mathcal{A}$'s queries in Game_2, it can answer all $\mathcal{A}$'s queries.

By Theorem 3.5, the $\mathsf{MLWE}_{k,k,Q,\sigma_{\mathsf{msk}}}$ assumption ensures that Game_2 and Game_3 are computationally indistinguishable. Then, there exists a PPT algorithm $\mathcal{B}_1$ such that

$$|\Pr[\mathsf{E}_2] - \Pr[\mathsf{E}_3]| = \mathsf{Adv}^{\mathsf{MLWE}}_{k,k,Q,\sigma_{\mathsf{msk}}}(\lambda, \mathcal{B}_1).$$

Game_4 : This game is the same as Game_3 except how $\mathcal{C}$ generates a challenge ciphertext ct^* when $\mathsf{coin} = 0$. In Game_3, $\mathcal{C}$ samples $\mathbf{r} \leftarrow\$ \mathcal{D}^k_{\mathcal{R},\sigma}$, $\mathbf{e}_1 \leftarrow\$ \mathcal{D}^{2k}_{\mathcal{R},\sigma}$, and $e_2 \leftarrow\$ \mathcal{D}_{\mathcal{R},\tau}$, the computes

$$\mathbf{c}_1^{*\top} := \mathbf{r}^\top \mathbf{A} + \mathbf{e}_1^\top \bmod Q, \qquad\qquad c_2^* := \mathbf{r}^\top \mathbf{y}_{\mathsf{id}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \bmod Q.$$

In Game_4, $\mathcal{C}$ first retrieves the unique tuple $(\mathsf{id}^*, \mathbf{y}_{\mathsf{id}^*}, (\mathbf{x}_{\mathsf{id}^*}, \mathbf{z}_{\mathsf{id}^*}))$ from local storage. Then, $\mathcal{C}$ samples $\mathbf{r} \leftarrow\$ \mathcal{D}^k_{\mathcal{R},\sigma}$, $\mathbf{e}_1 \leftarrow\$ \mathcal{D}^{2k}_{\mathcal{R},\sigma}$, and $e_2 \leftarrow\$ \mathcal{D}_{\mathcal{R},\tau}$, and computes

$$\begin{aligned} \mathbf{c}_1^{*\top} &:= \mathbf{r}^\top \mathbf{A} + \mathbf{e}_1^\top \bmod Q, \\ c_2^* &:= \boxed{\mathbf{c}_1^{*\top}\mathbf{x}_{\mathsf{id}^*} - \mathbf{r}^\top \mathbf{z}_{\mathsf{id}^*} - \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}^*}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \bmod Q. \end{aligned}$$

This change is conceptual because

$$\begin{aligned} c_2^* &= \mathbf{c}_1^{*\top}\mathbf{x}_{\mathsf{id}^*} - \mathbf{r}^\top \mathbf{z}_{\mathsf{id}^*} - \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}^*} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \\ &= \mathbf{r}^\top \mathbf{A}\mathbf{x}_{\mathsf{id}^*} + \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}^*} - \mathbf{r}^\top \mathbf{z}_{\mathsf{id}^*} - \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}^*} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \\ &= \mathbf{r}^\top (\mathbf{y}_{\mathsf{id}^*} + \mathbf{z}_{\mathsf{id}^*}) - \mathbf{r}^\top \mathbf{z}_{\mathsf{id}^*} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \\ &= \mathbf{r}^\top \mathbf{y}_{\mathsf{id}^*} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M}. \end{aligned}$$

Therefore, we have

$$\Pr[\mathsf{E}_3] = \Pr[\mathsf{E}_4].$$

Game_5 : This is the same as Game_4 except how $\mathcal{C}$ generates $\mathbf{c}_1^*$ when $\mathsf{coin} = 0$. In Game_5, $\mathcal{C}$ computes $\mathbf{c}_1^* \coloneqq \mathbf{c} + \mathbf{A}^\top \mathbf{r} + \mathbf{e}_1 \bmod Q$ instead of $\mathbf{c}_1^* \coloneqq \mathbf{A}^\top \mathbf{r} + \mathbf{e}_1 \bmod Q$, where $\mathbf{c} \leftarrow\$ \mathcal{R}_Q^{2k}$.

The $\mathsf{ahMLWE}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}$ assumption ensures that Game_4 and Game_5 are computationally indistinguishable. To show this, we use $\mathcal{A}$ to construct an ahMLWE adversary $\mathcal{B}_2$ as follows:

1. $\mathcal{B}_2$ gives $\mathbf{A} \in \mathcal{R}_Q^{k\times 2k}$ from the ahMLWE challenger $\mathcal{C}_{\mathsf{ahMLWE}}$ and sends $\mathsf{mpk} \coloneqq \mathbf{A}$ to $\mathcal{A}$.
2. $\mathcal{B}_2$ answers $\mathcal{A}$'s random oracle and key generation queries as in Game_4.
3. Upon $\mathcal{A}$'s challenge query on $(\mathsf{id}^*, \mathsf{M}^*)$, $\mathcal{B}_2$ retrieves the tuple $(\mathsf{id}^*, \mathbf{y}_{\mathsf{id}^*}, (\mathbf{x}_{\mathsf{id}^*}, \mathbf{z}_{\mathsf{id}^*}))$ from local storage, and sends $\mathbf{z} \coloneqq \begin{pmatrix} -\mathbf{x}_{\mathsf{id}^*} \\ -\mathbf{z}_{\mathsf{id}^*} \end{pmatrix}$ to $\mathcal{C}_{\mathsf{ahMLWE}}$. Note that, it holds that $\|\mathbf{z}\|_\infty \le \beta$.
4. $\mathcal{B}_2$ gives $(\mathbf{u} \coloneqq \mathbf{c} + \mathbf{A}^\top \mathbf{r} + \mathbf{e}_1 \bmod Q, h \coloneqq -\mathbf{r}^\top \mathbf{z}_{\mathsf{id}^*} - \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}^*} + e')$ from $\mathcal{C}_{\mathsf{ahMLWE}}$, where $\mathbf{c} = \mathbf{0}$ or $\mathbf{c} \leftarrow\$ \mathcal{R}_Q^{2k}$, and $e' \leftarrow\$ \mathcal{D}_{\mathcal{R},\tau}$. Then, $\mathcal{B}_2$ sets
$$\mathbf{c}_1^* \coloneqq \mathbf{u}, \qquad\qquad c_2^* \coloneqq \mathbf{u}^\top \mathbf{x}_{\mathsf{id}^*} + h + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M}^* \bmod Q,$$
and send $(\mathbf{c}_1^*, c_2^*)$ as the challenge ciphertext to $\mathcal{A}$.
5. $\mathcal{B}_2$ receives $\widehat{\mathsf{coin}}$ from $\mathcal{A}$, it outputs $\widehat{\mathsf{coin}}$.

If $\mathbf{c} = \mathbf{0}$, $\mathbf{c}_1^*$ follows the same distribution as in Game_4. Otherwise, $\mathbf{c}_1^*$ follows the same distribution as in Game_5. Thus, we complete the reduction, and we have
$$|\Pr[\mathsf{E}_4] - \Pr[\mathsf{E}_5]| = \mathsf{Adv}^{\mathsf{ahMLWE}}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}(\lambda, \mathcal{B}_2).$$

Game_6 : This game is the same as Game_5 except how $\mathcal{C}$ computes ct^* when $\mathsf{coin} = 0$. In Game_6, $\mathcal{C}$ computes
$$\mathbf{c}_1^{*\top} \coloneqq \mathbf{c}^\top + \mathbf{r}^\top \mathbf{A} + \mathbf{e}_1^\top \bmod Q, \qquad c_2^* \coloneqq \boxed{\mathbf{c}^\top \mathbf{x}_{\mathsf{id}^*} + \mathbf{r}^\top \mathbf{y}_{\mathsf{id}}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \bmod Q.$$

This change is conceptual. Therefore, we have
$$\Pr[\mathsf{E}_5] = \Pr[\mathsf{E}_6].$$

Game_7 : This is the same as Game_6 except how $\mathcal{C}$ generates c_2^*. Regardless of the value coin, $\mathcal{C}$ samples $c_2^* \leftarrow\$ \mathcal{R}_Q$.

We show that Game_6 and Game_7 are statistically indistinguishable. Based on our choice of parameters, we can apply Theorem 3.3, which ensures that $\mathbf{c}^{*\top} \mathbf{x}_{\mathsf{id}^*} + e_2 \bmod Q$ is statistically close to uniform even given $\mathbf{y}_{\mathsf{id}^*} = \mathbf{A}\mathbf{x}_{\mathsf{id}} + \mathbf{z}_{\mathsf{id}^*} \bmod Q$. Therefore, the statistical distance between the view of $\mathcal{A}$ in Game_6 and Game_7 is $\mathsf{negl}(\lambda)$ and we have
$$|\Pr[\mathsf{E}_6] - \Pr[\mathsf{E}_7]| = \mathsf{negl}(\lambda).$$

Game_8 : This is the same as Game_7 ho $\mathcal{C}$ generates $\mathbf{c}_1^*$. Regardless of the value coin, $\mathcal{C}$ samples $\mathbf{c}_1^* \leftarrow\$ \mathcal{R}_Q^{2k}$. Thus, we have
$$\Pr[\mathsf{E}_8] = \frac{1}{2}.$$

Since this change does not affect the view of $\mathcal{A}$ at all, then we have
$$\Pr[\mathsf{E}_7] = \Pr[\mathsf{E}_8].$$

By combining everything, we have
$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\Pi}(\lambda) \le \mathsf{Adv}^{\mathsf{MLWE}}_{k,k,Q,\sigma_{\mathsf{msk}}}(\lambda, \mathcal{B}_1) + \mathsf{Adv}^{\mathsf{ahMLWE}}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}(\lambda, \mathcal{B}_2) + \mathsf{negl}(\lambda).$$

$\square$

6 Security Proof in the Quantum Random Oracle Model

This section provides the security proof of our scheme in the quantum random oracle model (QROM). To do this, we recall the foundations of the QROM with reference to [KYY21, Tak21]. We refer to [NC10] for more details.

6.1 Preliminaries on the QROM

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

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

QROM. The notion of the QROM was introduced by Boneh et al. [BDF+11] as an extension of the (classical) random oracle model (ROM) in a quantum world. In the case of the ROM, the QROM is an idealized model, where a hash function is idealized to be an oracle that simulates a random function. On the other hand, as opposed to the ROM, the hash function in the QROM is a quantumly accessible oracle. In security proofs in the QROM, a random function $\mathsf{H} : \mathsf{X} \to \mathsf{Y}$ is uniformly chosen at the beginning, and an adversary can make queries on a quantum state $\sum_{x,y} \alpha_{x,y}|x\rangle|y\rangle$ to the oracle and receive $\sum_{x,y} \alpha_{x,y}|x\rangle|\mathsf{H}(x)\oplus y\rangle$.

Let $\mathcal{A}^{|\mathsf{H}\rangle}$ denote a quantum algorithm that can quantumly access the oracle $|\mathsf{H}\rangle$. As shown in [Zha12], quantum random oracles can be simulated by a family of $2Q_{\mathsf{H}}$-wise independent hash functions for an adversary that quantumly accesses the random oracle at most Q_{H} times.

Lemma 6.1 ([Zha12])**.** Any quantum algorithm $\mathcal{A}$ making quantum queries to random oracles can be efficiently simulated by a quantum algorithm $\mathcal{B}$, which has the same output distribution but makes no queries.

6.2 Security Proof in the QROM

Theorem 6.2. If the $\mathsf{MLWE}_{k,k,Q,\sigma_{\mathsf{msk}}}$ and $\mathsf{ahMLWE}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}$ assumptions hold, our IBE scheme Π in Section 4.1 achieves adaptively anonymous in the quantum random oracle model. In particular, for any quantum PPT adversary $\mathcal{A}$ making at most Q_{H} random oracle queries to H and Q_{id} secret key queries, there exist two quantum polynomial time reduction algorithms $\mathcal{B}_1$ and $\mathcal{B}_2$ such that

$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\Pi}(\lambda) \leq \mathsf{Adv}^{\mathsf{MLWE}}_{k,k,Q,\sigma_{\mathsf{msk}}}(\lambda,\mathcal{B}_1) + \mathsf{Adv}^{\mathsf{ahMLWE}}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}(\lambda,\mathcal{B}_2) + \mathsf{negl}(\lambda).$$

Proof. We show the security of Π via the following games. In each game, we define E_i as the event that $\mathcal{A}$ wins in Game_i. Let $\mathsf{Samp}(\sigma_{\mathsf{sk}}, p; r)$ be a PPT algorithm that, given a Gaussian parameter σ_{sk}, a positive integer p, and a random coin $r \in \{0,1\}^{\ell_r}$, outputs $(\mathbf{x},\mathbf{z})$, where $\mathbf{x}$ sampled from a distribution statistically close to $\mathcal{D}^{2k}_{\mathcal{R},\sigma_{\mathsf{sk}}}$ and $\mathbf{z}$ sampled from a distribution statistically close to $(\mathcal{D}_{\mathcal{R},\sigma_{\mathsf{sk}}} * \mathcal{R}_p)^k$.

Game_0 : This is the actual security game. At the beginning of the game, the challenge $\mathcal{C}$ chooses a random function $\mathsf{H} : \{0,1\}^{\ell_{\mathsf{id}}} \to \mathcal{R}_Q^k$. Then, it generates $(\mathsf{msk},\mathsf{mpk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$ and gives mpk to the adversary

$\mathcal{A}$. Then, it samples $\mathsf{coin} \leftarrow\$ \{0,1\}$ and keeps it secret. During the game, $\mathcal{A}$ can make many (quantum) random oracle and secret key queries and one challenge query. These queries are handled as follows:

- When $\mathcal{A}$ makes a (quantum) random oracle query on a quantum state $\sum_{\mathsf{id},y} \alpha_{\mathsf{id},y}|\mathsf{id}\rangle|y\rangle$, $\mathcal{C}$ returns $\sum_{\mathsf{id},y} \alpha_{\mathsf{id},y}|\mathsf{id}\rangle|\mathsf{H}(\mathsf{id}) \oplus y\rangle$.
- When $\mathcal{A}$ makes a key generation query for id, $\mathcal{C}$ returns $\mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}} \leftarrow\$ \mathsf{AppSampPre}(\mathbf{A}, \mathbf{T}_{\mathbf{A}}, \mathbf{y}_{\mathsf{id}}, \sigma_{\mathsf{sk}})$.
- When $\mathcal{A}$ makes a challenge query $(\mathsf{id}^*, \mathsf{M}^*)$, $\mathcal{C}$ returns $\mathsf{ct}^* \leftarrow\$ \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*, \mathsf{M}^*)$ if $\mathsf{coin} = 0$ and $\mathsf{ct}^* \leftarrow\$ \mathcal{R}_Q^{2k+1}$ if $\mathsf{coin} = 1$.

At the end of the game, $\mathcal{A}$ outputs a guess $\widehat{\mathsf{coin}}$ for coin. Finally, $\mathcal{C}$ outputs $\widehat{\mathsf{coin}}$.

By definition, we have

$$\left|\Pr[\mathsf{E}_0] - \frac{1}{2}\right| = \left|\Pr[\widehat{\mathsf{coin}} = \mathsf{coin}] - \frac{1}{2}\right| = \mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\Pi}(\lambda).$$

Game_1 : This is the same as Game_0 except how $\mathcal{C}$ answers the quantum random oracle queries. First, $\mathcal{C}$ picks a $2Q_{\mathsf{H}}$-wise independent hash function $\mathsf{h}_{2Q_{\mathsf{H}}} : \{0,1\}^{\ell_{\mathsf{id}}} \to \{0,1\}^{\ell_r}$. Then, we define $\mathsf{H}(\mathsf{id}) := \mathbf{A}\mathbf{x}_{\mathsf{id}} + \mathbf{z}_{\mathsf{id}} \bmod Q$, where $(\mathbf{x}_{\mathsf{id}}, \mathbf{z}_{\mathsf{id}}) := \mathsf{Samp}(\sigma_{\mathsf{sk}}, p; \mathsf{h}_{2Q_{\mathsf{H}}}(\mathsf{id}))$ and use this H throughout the game.

For any fixed id, the distribution of $\mathsf{H}(\mathsf{id})$ is identical, and its statistical distance from the uniform distribution is $\mathsf{negl}(\lambda)$ due to Theorem 3.5. Note that in this game, we only change the distribution of $\mathbf{y}_{\mathsf{id}}$ for each identity, and how we create secret keys is unchanged. Then, due to Lemma 6.1, we have

$$|\Pr[\mathsf{E}_0] - \Pr[\mathsf{E}_1]| = \mathsf{negl}(\lambda).$$

Game_2 : This is the same as Game_1 except how $\mathcal{C}$ generates secret keys $\mathbf{x}_{\mathsf{id}}$. By the end of this game, $\mathcal{C}$ will no longer require the trapdoor $\mathbf{T}_{\mathbf{A}}$ to generate the secret keys. When $\mathcal{A}$ queries a secret key for id, $\mathcal{C}$ returns $\mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}$, where $(\mathbf{x}_{\mathsf{id}}, \mathbf{z}_{\mathsf{id}}) := \mathsf{Samp}(\sigma_{\mathsf{sk}}, p; \mathsf{h}_{2Q_{\mathsf{H}}}(\mathsf{id}))$.

By following the same argument in Game_2 of the proof of Theorem 5.1, we have

$$|\Pr[\mathsf{E}_1] - \Pr[\mathsf{E}_2]| = Q_{\mathsf{id}} \cdot \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda).$$

Game_3 : This is the same as Game_2 except how $\mathcal{C}$ generates a master public key $\mathbf{A}$. In Game_3, $\mathcal{C}$ does not run the $\mathsf{AppTrapGen}$ algorithm but samples a uniformly random matrix $\mathbf{A} \leftarrow\$ \mathcal{R}_Q^{k\times 2k}$.

By following the same argument in Game_3 of the proof of Theorem 5.1, we have

$$|\Pr[\mathsf{E}_2] - \Pr[\mathsf{E}_3]| = \mathsf{Adv}^{\mathsf{MLWE}}_{k,k,Q,\sigma_{\mathsf{msk}}}(\lambda, \mathcal{B}_1).$$

Game_4 : This game is the same as Game_3 except how $\mathcal{C}$ generates a challenge ciphertext ct^* when $\mathsf{coin} = 0$. In Game_3, $\mathcal{C}$ samples $\mathbf{r} \leftarrow\$ \mathcal{D}^k_{\mathcal{R},\sigma}$, $\mathbf{e}_1 \leftarrow\$ \mathcal{D}^{2k}_{\mathcal{R},\sigma}$, and $e_2 \leftarrow\$ \mathcal{D}_{\mathcal{R},\tau}$, the computes

$$\mathbf{c}_1^{*\top} := \mathbf{r}^\top \mathbf{A} + \mathbf{e}_1^\top \bmod Q, \qquad c_2^* := \mathbf{r}^\top \mathbf{y}_{\mathsf{id}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \bmod Q.$$

In Game_4, $\mathcal{C}$ first retrieves the unique tuple $(\mathsf{id}^*, \mathbf{y}_{\mathsf{id}^*}, (\mathbf{x}_{\mathsf{id}^*}, \mathbf{z}_{\mathsf{id}^*}))$ from local storage. Then, $\mathcal{C}$ samples $\mathbf{r} \leftarrow\$ \mathcal{D}^k_{\mathcal{R},\sigma}$, $\mathbf{e}_1 \leftarrow\$ \mathcal{D}^{2k}_{\mathcal{R},\sigma}$, and $e_2 \leftarrow\$ \mathcal{D}_{\mathcal{R},\tau}$, and computes

$$\mathbf{c}_1^{*\top} := \mathbf{r}^\top \mathbf{A} + \mathbf{e}_1^\top \bmod Q,$$
$$c_2^* := \mathbf{c}_1^{*\top} \mathbf{x}_{\mathsf{id}^*} - \mathbf{r}^\top \mathbf{z}_{\mathsf{id}^*} - \mathbf{e}_1^\top \mathbf{x}_{\mathsf{id}^*} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \bmod Q.$$

By following the same argument in Game_4 of the proof of Theorem 5.1, we have

$$\Pr[\mathsf{E}_3] = \Pr[\mathsf{E}_4].$$

Game_5 : This is the same as Game_4 except how $\mathcal{C}$ generates $\mathbf{c}_1^*$ when $\mathsf{coin} = 0$. In Game_5, $\mathcal{C}$ computes $\mathbf{c}_1^* \coloneqq \mathbf{c} + \mathbf{A}^\top \mathbf{r} + \mathbf{e}_1 \bmod Q$ instead of $\mathbf{c}_1^* \coloneqq \mathbf{A}^\top \mathbf{r} + \mathbf{e}_1 \bmod Q$, where $\mathbf{c} \leftarrow\!\!\$\, \mathcal{R}_Q^{2k}$.

By following the same argument in Game_5 of the proof of Theorem 5.1, we have

$$|\Pr[\mathsf{E}_4] - \Pr[\mathsf{E}_5]| = \mathsf{Adv}^{\mathsf{ahMLWE}}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}(\lambda, \mathcal{B}_2).$$

Game_6 : This game is the same as Game_5 except how $\mathcal{C}$ computes ct^* when $\mathsf{coin} = 0$. In Game_6, $\mathcal{C}$ computes

$$\mathbf{c}_1^{*\top} \coloneqq \mathbf{c}^\top + \mathbf{r}^\top \mathbf{A} + \mathbf{e}_1^\top \bmod Q, \qquad c_2^* \coloneqq \mathbf{c}^\top \mathbf{x}_{\mathsf{id}^*} + \mathbf{r}^\top \mathbf{y}_{\mathsf{id}} + e_2 + \lfloor \frac{Q}{2} \rceil \cdot \mathsf{M} \bmod Q.$$

By following the same argument in Game_6 of the proof of Theorem 5.1, we have

$$\Pr[\mathsf{E}_5] = \Pr[\mathsf{E}_6].$$

Game_7 : This is the same as Game_6 except how $\mathcal{C}$ generates c_2^*. Regardless of the value coin, $\mathcal{C}$ samples $c_2^* \leftarrow\!\!\$\, \mathcal{R}_Q$.

By following the same argument in Game_7 of the proof of Theorem 5.1, we have

$$|\Pr[\mathsf{E}_6] - \Pr[\mathsf{E}_7]| = \mathsf{negl}(\lambda).$$

Game_8 : This is the same as Game_7 ho $\mathcal{C}$ generates $\mathbf{c}_1^*$. Regardless of the value coin, $\mathcal{C}$ samples $\mathbf{c}_1^* \leftarrow\!\!\$\, \mathcal{R}_Q^{2k}$. By following the same argument in Game_8 of the proof of Theorem 5.1, we have Thus, we have

$$\Pr[\mathsf{E}_7] = \Pr[\mathsf{E}_8], \qquad \Pr[\mathsf{E}_8] = \frac{1}{2}.$$

Therefore, by combining everything, we have

$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\Pi}(\lambda) \leq \mathsf{Adv}^{\mathsf{MLWE}}_{k,k,Q,\sigma_{\mathsf{msk}}}(\lambda, \mathcal{B}_1) + \mathsf{Adv}^{\mathsf{ahMLWE}}_{k,2k,Q,\sigma,\tau,p+\sqrt{\lambda}\sigma_{\mathsf{sk}}}(\lambda, \mathcal{B}_2) + \mathsf{negl}(\lambda).$$

□

Acknowledgements

This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among “Research and Development for Expansion of Radio Wave Resources (JPJ000254)”, which was supported by the Ministry of Internal Affairs and Communications, Japan. This work was in part supported by JSPS KAKENHI Grant Numbers JP22H03590 and JP21H03395.

References

[ABB10a] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 553–572. Springer, Berlin, Heidelberg, May / June 2010. 1

[ABB10b] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 98–115. Springer, Berlin, Heidelberg, August 2010. 1

[AGJ+24] Sven Argo, Tim Güneysu, Corentin Jeudy, Georg Land, Adeline Roux-Langlois, and Olivier Sanders. Practical post-quantum signatures for privacy. Cryptology ePrint Archive, Report 2024/131, 2024. 6

[AKG+07] N Asokan, Kari Kostiainen, Philip Ginzboorg, Jörg Ott, and Cheng Luo. Applicability of identity-based cryptography for disruption-tolerant networking. In *Proceedings of the 1st international MobiSys workshop on Mobile opportunistic networking*, pages 52–56, 2007. 1

[ALWW21] Parhat Abla, Feng-Hao Liu, Han Wang, and Zhedong Wang. Ring-based identity based encryption - asymptotically shorter MPK and tighter security. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part III*, volume 13044 of *LNCS*, pages 157–187. Springer, Cham, November 2021. 1

[AP12] Jacob Alperin-Sheriff and Chris Peikert. Circular and KDM security for identity-based encryption. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 334–352. Springer, Berlin, Heidelberg, May 2012. 1

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Berlin, Heidelberg, December 2011. 17

[BEP+21] Pauline Bert, Gautier Eberhart, Lucas Prabel, Adeline Roux-Langlois, and Mohamed Sabt. Implementation of lattice trapdoors on modules and applications. In Jung Hee Cheon and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021*, pages 195–214. Springer, Cham, 2021. 2

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Berlin, Heidelberg, August 2001. 1, 6

[BFRS18] Pauline Bert, Pierre-Alain Fouque, Adeline Roux-Langlois, and Mohamed Sabt. Practical implementation of ring-SIS/LWE based signature and IBE. In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018*, pages 271–291. Springer, Cham, 2018. 2

[BGK08] Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar. Identity-based encryption with efficient revocation. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM CCS 2008*, pages 417–426. ACM Press, October 2008. 1

[BKP14] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (Hierarchical) identity-based encryption from affine message authentication. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425. Springer, Berlin, Heidelberg, August 2014. 1

[BL16] Xavier Boyen and Qinyi Li. Towards tightly secure lattice short signature and id-based encryption. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 404–434. Springer, Berlin, Heidelberg, December 2016. 1, 2

[BL18] Xavier Boyen and Qinyi Li. Almost tight multi-instance multi-ciphertext identity-based encryption on lattices. In Bart Preneel and Frederik Vercauteren, editors, *ACNS 18International Conference on Applied Cryptography and Network Security*, volume 10892 of *LNCS*, pages 535–553. Springer, Cham, July 2018. 2

[BRTM08] Kevin RB Butler, Sunam Ryu, Patrick Traynor, and Patrick D McDaniel. Leveraging identity-based cryptography for node id assignment in structured p2p systems. *IEEE Transactions on Parallel and Distributed Systems*, 20(12):1803–1815, 2008. 1

[CGM19] Yilei Chen, Nicholas Genise, and Pratyay Mukherjee. Approximate trapdoors for lattices and smaller hash-and-sign signatures. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 3–32. Springer, Cham, December 2019. 3, 4

[CHKP10] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 523–552. Springer, Berlin, Heidelberg, May / June 2010. 1

[CKKS19] Jung Hee Cheon, Duhyeong Kim, Taechan Kim, and Yongha Son. A new trapdoor over module-NTRU lattice and its application to ID-based encryption. Cryptology ePrint Archive, Report 2019/1468, 2019. 1, 2

[Coc01] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *8th IMA International Conference on Cryptography and Coding*, volume 2260 of *LNCS*, pages 360–363. Springer, Berlin, Heidelberg, December 2001. 1

[DG17] Nico Döttling and Sanjam Garg. Identity-based encryption from the Diffie-Hellman assumption. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 537–569. Springer, Cham, August 2017. 1

[DKL+23] Nico Döttling, Dimitris Kolonelos, Russell W. F. Lai, Chuanwei Lin, Giulio Malavolta, and Ahmadreza Rahimi. Efficient laconic cryptography from learning with errors. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part III*, volume 14006 of *LNCS*, pages 417–446. Springer, Cham, April 2023. 4, 6, 8

[DLP14] Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. Efficient identity-based encryption over NTRU lattices. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 22–41. Springer, Berlin, Heidelberg, December 2014. 1, 2

[DSDSAL08] Eduardo Da Silva, Aldri L Dos Santos, Luiz Carlos P Albini, and Michele N Lima. Identity-based key management in mobile ad hoc networks: techniques and applications. *IEEE Wireless Communications*, 15(5):46–52, 2008. 1

[EKW19] Keita Emura, Shuichi Katsumata, and Yohei Watanabe. Identity-based encryption with security against the KGC: A formal model and its instantiation from lattices. In Kazue Sako, Steve Schneider, and Peter Y. A. Ryan, editors, *ESORICS 2019, Part II*, volume 11736 of *LNCS*, pages 113–133. Springer, Cham, September 2019. 1

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008. 1, 2

[HSM13] Jinguang Han, Willy Susilo, and Yi Mu. Identity-based data storage in cloud computing. *Future Generation Computer Systems*, 29(3):673–681, 2013. 1

[IPR23] Malika Izabachène, Lucas Prabel, and Adeline Roux-Langlois. Identity-based encryption from lattices using approximate trapdoors. In Leonie Simpson and Mir Ali Rezazadeh Baee, editors, *ACISP 23*, volume 13915 of *LNCS*, pages 270–290. Springer, Cham, July 2023. 3

[JHTW24] Huiwen Jia, Yupu Hu, Chunming Tang, and Lin Wang. Towards compact identity-based encryption on ideal lattices. In Elisabeth Oswald, editor, *CT-RSA 2024*, volume 14643 of *LNCS*, pages 354–378. Springer, Cham, May 2024. 2, 3, 4

[JRS24] Corentin Jeudy, Adeline Roux-Langlois, and Olivier Sanders. Phoenix: Hash-and-sign with aborts from lattice gadgets. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I*, pages 265–299. Springer, Cham, June 2024. 4

[KMT19] Shuichi Katsumata, Takahiro Matsuda, and Atsushi Takayasu. Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 441–471. Springer, Cham, April 2019. 1

[KTY23] Shuichi Katsumata, Toi Tomita, and Shota Yamada. Direct computation of branching programs and its applications to more efficient lattice-based cryptography. *DCC*, 91(2):391–431, 2023. 2

[KY16] Shuichi Katsumata and Shota Yamada. Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 682–712. Springer, Berlin, Heidelberg, December 2016. 1, 3

[KYY18] Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa. Tighter security proofs for GPV-IBE in the quantum random oracle model. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 253–282. Springer, Cham, December 2018. 1, 2, 3, 4

[KYY21] Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa. Tighter security proofs for GPV-IBE in the quantum random oracle model. *Journal of Cryptology*, 34(1):5, January 2021. 1, 2, 3, 4, 6, 17

[Lan23] Roman Langrehr. On the multi-user security of LWE-based NIKE. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023, Part IV*, volume 14372 of *LNCS*, pages 33–62. Springer, Cham, November / December 2023. 4, 6

[LDK+22] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. 1

[LLW20] Qiqi Lai, Feng-Hao Liu, and Zhedong Wang. Almost tight security in lattices with polynomial moduli - PRF, IBE, all-but-many LTF, and more. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 652–681. Springer, Cham, May 2020. 2

[LS15] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *DCC*, 75(3):565–599, 2015. 6

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 738–755. Springer, Berlin, Heidelberg, April 2012. 5

[MKMS21] Jose Maria Bermudo Mera, Angshuman Karmakar, Tilen Marc, and Azam Soleimanian. Efficient lattice-based inner-product functional encryption. Cryptology ePrint Archive, Report 2021/046, 2021. 5, 9

[MKMS22] Jose Maria Bermudo Mera, Angshuman Karmakar, Tilen Marc, and Azam Soleimanian. Efficient lattice-based inner-product functional encryption. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022, Part II*, volume 13178 of *LNCS*, pages 163–193. Springer, Cham, March 2022. 9

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007. 5

[MSO17] Sarah McCarthy, Neil Smyth, and Elizabeth O'Sullivan. A practical implementation of identity-based encryption over NTRU lattices. In Máire O'Neill, editor, *16th IMA International Conference on Cryptography and Coding*, volume 10655 of *LNCS*, pages 227–246. Springer, Cham, December 2017. 1, 2

[MSW15] Tobias Markmann, Thomas C Schmidt, and Matthias Wählisch. Federated end-to-end authentication for the constrained internet of things using ibc and ecc. *ACM SIGCOMM Computer Communication Review*, 45(4):603–604, 2015. 1

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010. 17

[NY19] Ryo Nishimaki and Takashi Yamakawa. Leakage-resilient identity-based encryption in bounded retrieval model with nearly optimal leakage-ratio. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part I*, volume 11442 of *LNCS*, pages 466–495. Springer, Cham, April 2019. 1

[Pei08] Chris Peikert. Limits on the hardness of lattice problems in l_p norms. *Comput. Complex.*, 17(2):300–351, 2008. 5

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005. 1

[SAB+22] Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. 1

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer, Berlin, Heidelberg, August 1984. 1

[Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999. 1

[SS11] Damien Stehlé and Ron Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 27–47. Springer, Berlin, Heidelberg, May 2011. 9

[SS13] Damien Stehlé and Ron Steinfeld. Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive, Report 2013/004, 2013. 9

[Tak21] Atsushi Takayasu. Adaptively secure lattice-based revocable IBE in the QROM: compact parameters, tight security, and anonymity. *DCC*, 89(8):1965–1992, 2021. 17

[TS24] Toi Tomita and Junji Shikata. Efficient identity-based encryption with tight adaptive anonymity from RLWE. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I*, pages 300–321. Springer, Cham, June 2024. 4

[TWZL08] Chiu C Tan, Haodong Wang, Sheng Zhong, and Qun Li. Body sensor network security: an identity-based cryptography approach. In *Proceedings of the first ACM conference on Wireless network security*, pages 148–153, 2008. 1

[Wat09] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, Berlin, Heidelberg, August 2009. 1

[Yam17] Shota Yamada. Asymptotically compact adaptively secure lattice IBEs and verifiable random functions via generalized partitioning techniques. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 161–193. Springer, Cham, August 2017. 1

[YJW23] Yang Yu, Huiwen Jia, and Xiaoyun Wang. Compact lattice gadget and its applications to hash-and-sign signatures. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 390–420. Springer, Cham, August 2023. 2, 3, 6, 10

[ZC11] Sheng Zhong and Tingting Chen. An efficient identity-based protocol for private matching. *International Journal of Communication Systems*, 24(4):543–552, 2011. 1

[Zha12] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Berlin, Heidelberg, August 2012. 1, 2, 17

[ZMS+24] Raymond K. Zhao, Sarah McCarthy, Ron Steinfeld, Amin Sakzad, and Máire O'Neill. Quantum-safe HIBE: does it cost a latte? *IEEE Trans. Inf. Forensics Secur.*, 19:2680–2695, 2024. 1, 2

Contents