Identity-Based Encryption from Lattices with More Compactness in the Standard Model

Weidan Ji[1][0009−0006−4240−1621], Zhedong Wang[1⋆][0009−0007−1741−8744], Haoxiang Jin[1][0009−0007−9111−8280], Qi Wang[2][0009−0007−9333−5051], Geng Wang[1][0000−0003−1000−7903], Dawu Gu[1⋆][0000−0002−0504−9538]

[1] Shanghai Jiao Tong University, Shanghai, China.
{jiweidan,wzdstill,iniesta8,wanggxx,dwgu}@sjtu.edu.cn
[2] Heilongjiang University, Harbin, China. wangamyqi@gmail.com

Abstract. Lattice-based identity-based encryption having both efficiency and provable security in the standard model is currently still a challenging task and has drawn much attention. In this work, we introduce a new IBE construction from NTRU lattices in the standard model, based on the framework proposed by Agrawal, Boneh, and Boyen (EUROCRYPT 2010). Particularly, by introducing the NTRU trapdoor and the Ring-LWE computational assumption, we remove a crux restriction of the column number and obtain a more compact IBE construction in the standard model. Besides, we provide a concrete implementation and detailed performance results with a comparison of previous works in terms of the security model and the assumption, which demonstrates the advantage of our construction.

Keywords: Lattice-based cryptography · Identity-based encryption · NTRU lattice · Standard model.

1 Introduction

Identity-based encryption (IBE) is a generalization of public key encryption, where the public key can be an arbitrary string such as a name, a telephone number or an email address. The user's secret key can only be generated by a trusted authority, called a key generation center (KGC), which applies its master secret key to the user's identity after the user authenticates itself. Shamir [34] proposed the notion of IBE as a way to simplify the public key and certificate management. Since its first realization proposed by Boneh and Franklin [10], there has been significant research in the past two decades [1,7,8,12,17,18,21,22,25,36,37], constructing various IBE schemes from different assumptions. Recently, to prevent attacks from quantum computers, post-quantum cryptography, especially lattice-based cryptography, emerges as a popular research direction. In this paper, we focus on lattice-based IBE.

⋆ Corresponding author.

In [22], Gentry, Peikert and Vaikuntanathan made one of the major breakthroughs in lattice-based cryptography: they showed how to use the short trapdoor basis (known as Ajtai trapdoor [2]) to generate short lattice vectors without revealing the trapdoor (known as GPV sampling). This sampler can be used to construct the first lattice-based IBE construction, which can be proven secure in the random oracle model (ROM). However, the constructions based on the Ajtai trapdoor are not sufficiently efficient. Specifically, in [22], the Ajtai trapdoor generation algorithm outputs a pair $(\mathbf{A}, \mathbf{T_A}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}^{m\times m}$ where $\mathbf{T_A}$ is a trapdoor for the SIS function $f_{\mathbf{A}} = \mathbf{Ax} \bmod q$. To guarantee the security of $\mathbf{T_A}$, the distribution of $\mathbf{A}$ is set to be statistically close to the uniform distribution over $\mathbb{Z}_q^{n\times m}$, which induces the parameter constraint $m = \Theta(n \log q)$, and thus leads to large parameters. Later, Micciancio and Peikert [30] proposed a more simple trapdoor (known as MP-trapdoor) than the Ajtai trapdoor, but the parameter constraint still exists.

To overcome this *efficiency* bottleneck, Ducas, Lyubashevsky and Prest [18] (DLP-IBE) instantiated the GPV sampling algorithm by using a particular distribution of NTRU lattices that have nearly optimal trapdoor lengths (known as NTRU trapdoor). Specifically, for a polynomial ring $R \coloneqq \mathbb{Z}[X]/(X^n + 1)$, the NTRU trapdoor generation algorithm outputs a pair $(h, \mathbf{T}_h) \in R_q \times R^{2\times 2}$ satisfying $[1|h] \cdot \mathbf{T}_h = \mathbf{0} \bmod q$. The security of the trapdoor $\mathbf{T}_h$ is now obtained from the computational hardness assumption of NTRU lattices. Compared with the parameter constraint of the Ajtai trapdoor ($m = \Theta(n \log q)$), the NTRU trapdoor only requires $m = 2n$, which results in better efficiency. Based on the NTRU trapdoor, they proposed the first practical lattice-based IBE scheme.

On the *security* side, the above IBE constructions are all proven secure in the ROM. However, the ROM is arguably "unnatural" and significantly differs from real-world constructions, according to several works [5,11,23,28]. What's worse, Boneh et al. [9] pointed out that the ROM as in the classical setting is not reasonable when considering security against quantum adversaries, and one needs to alternatively prove post-quantum security of a scheme in the quantum random oracle model (QROM) [26,38], which is challenging and may involve a significant loss of security.

To obtain more reasonable security against quantum attacks, Agrawal, Boneh, and Boyen [1] provided a lattice-based IBE (ABB-IBE) in the standard model whose performance is comparable to the performance of the random-oracle system from [22]. Same as [22], their construction is not efficient enough due to the limitations of the Ajtai trapdoor.

Lattice-based IBE construction having both efficiency and provable security in the standard model remains a challenging task. Constructing a standard model IBE based on the NTRU trapdoor seems like a straight and promising idea, but it is difficult to realize. The difficulty lies in the fact that the security proof in the standard model requires that the real system and the simulated system are indistinguishable. The existing approach using the Leftover Hash Lemma (LHL) implicitly requires $m = \Theta(n \log q)$, which is contrary to the original purpose of using the NTRU trapdoor to improve efficiency. Therefore, it raises a natural

question:

Can we construct a lattice-based IBE in the standard model, whose performance is comparable to that of the random-oracle system from [18] ?

1.1 Our Results

In this paper, we provide and implement the first lattice-based IBE construction based on the NTRU trapdoor in the standard model, whose performance is comparable to the IBE in the ROM [18]. More precisely, our main contributions are the following perspectives:

- **NTRU trapdoor embedding in the standard model.** We embed the NTRU trapdoor into IBE construction in the standard model by a redesign of the sampling lattices (Sect. 4.2). This modification leads to shorter public parameters considering reasonable security against quantum attacks. Refer to Tab. 1 for a detailed comparison.
- **New proof techniques for NTRU trapdoor.** We introduce the RLWE computational assumption to eliminate the parameter constraint associated with the two-side trapdoor's indistinguishability (Sect. 3) and adapt the security proof to the new sampling lattices (Sect. 5.2), resulting in a more compact IBE construction without leaking any secret information.
- **Security analysis and implementation.** We conduct a rigorous security analysis against lattice reduction attacks and provide a comprehensive open-source implementation[3], complete with performance benchmarking. Moreover, we provide several concrete parameter settings for our IBE construction, achieving NIST level I, III, and V respectively. Refer to Tab. 2.

Note that we focus on compact IBE schemes with selective security, which can be upgraded to the adaptively secure schemes via the well-known complexity leveraging approach [8].

Table 1. Sizes Comparison between this paper and [18,1]. Compared to the most efficient scheme to date [18], we achieve more reasonable security with comparable performance (i.e., $O(1)$). Compared to the ring version of [1], we significantly reduce the sizes of all components (i.e., $O(\log q)$) under the same security model.

Scheme	Standard model	Assumption	mpk	msk	$\mathsf{sk}_{\mathsf{id}}$	ct
DLP-IBE [18]	×	NTRU/RLWE	$n \log q$	$> 2n \log q$	$< n \log q$	$> 2n \log q$
ABB-IBE [1]	✓	RSIS/RLWE	$n \log^2 q$	$> 2n \log q$	$< \frac{1}{2} n \log^2 q$	$n \log^2 q$
Ours	✓	NTRU/RLWE	$7n \log q$	$> 2n \log q$	$\approx 3.5n \log q$	$7n \log q$

[3] https://anonymous.4open.science/r/mntru_ibe-DF11/

1.2 Techniques Overview

The ABB-IBE. We briefly review the general framework of IBE in the standard model proposed by [1]. The key idea is to construct a family of sampling lattices that associates each identity with two distinct trapdoors for finding short vectors. Now we generalize the original Ajtai trapdoor from $\mathbb{Z}_q$ to R_q as in [25]. More concretely, on input a pair $(\mathbf{a}, \mathbf{T_a}) \in R_q^k \times R^{k\times k}$ satisfying $\mathbf{a}\cdot\mathbf{T_a} = \mathbf{0} \bmod q$, a hash function $H : \{0,1\}^* \to R$ satisfying $H(\mathsf{id}_1) \neq H(\mathsf{id}_2)$ if and only if $\mathsf{id}_1 \neq \mathsf{id}_2$, the family of lattices for each identity id can be constructed as

$$\mathsf{pk}_{\mathsf{id}} = [\mathbf{a}|\mathbf{aR} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}] \in R_q^{k+d}, \tag{1}$$

where $\mathbf{g} = [1|b|\cdots|b^{d-1}] \in R_q^d$ is a special gadget vector whose trapdoor $\mathbf{T_g}$ is publicly known [30], $\mathbf{R} \in R^{k\times d}$ is a random matrix with small spectral norm and id^* is the challenge identity. The critical step of [1] is that we can set $\mathbf{T} = \begin{bmatrix}-\mathbf{R}\\ \mathbf{I}\end{bmatrix}$, which satisfies $\mathsf{pk}_{\mathsf{id}} \cdot \mathbf{T} = (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}$, and thus inversion of $f_{\mathsf{pk}_{\mathsf{id}}}$ can be converted into the inversion of $f_{\mathbf{g}}$ for Ajtai's function (i.e., $f_{\mathbf{a}} = \mathbf{a}\cdot\mathbf{x}^\top \bmod q$)[4]. Therefore, for a given target $u \in R_q$, we can sample a short vector $\mathbf{e}_{\mathsf{id}} \in R^{k+d}$ satisfying

$$[\mathbf{a}|\mathbf{aR} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}] \cdot \mathbf{e}_{\mathsf{id}}^\top = u.$$

We observe that there are two restrictions on k:

- Security of the Ajtai trapdoor $\mathbf{T_a}$ requires $k > \log q$.
- Indistinguishability of the real system and the simulated system requires "$\mathbf{aR}$" to be close to the uniformly random distribution over R_q^d, which implies $k > \log q$.

The parameter k has a direct impact on the dimensions of the master public key, user's secret key, and ciphertext. Eliminating constraints on the parameter k is essential for designing a compact IBE scheme.

Remove Two Restrictions on k. To remove the first restriction on k, we replace the Ajtai trapdoor with the NTRU trapdoor. In detail, the NTRU trapdoor generation algorithm [18] outputs $(h, \mathbf{T}_h) \in R_q \times R^{2\times 2}$ satisfying $[1|h]\cdot\mathbf{T}_h = \mathbf{0} \bmod q$. Now if we directly embed the NTRU trapdoor into Eq. (1), we obtain

$$\mathsf{pk}_{\mathsf{id}} = [1|h|[1|h]\mathbf{R} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}].$$

In this case, the term "$[1|h]\mathbf{R}$" is no longer close to the uniform distribution over R_q^d. To solve this problem, we change the NTRU instance h on the right side to a uniformly random element $z \xleftarrow{\$} R_q$, and then choose $\mathbf{R} \leftarrow \mathcal{D}_{R,\sigma_{\mathbf{R}}}^{2\times d}$ from a

[4] In detail, $f_{\mathbf{g}} = \mathbf{a}\cdot\mathbf{x}^\top$, $f_{\mathsf{pk}_{\mathsf{id}}} = \mathsf{pk}_{\mathsf{id}}\cdot\mathbf{x}^\top$. Inversion of $f_{\mathsf{pk}_{\mathsf{id}}}$ means that given u, find a small $\mathbf{x}$ satisfying $\mathsf{pk}_{\mathsf{id}}\cdot\mathbf{x}^\top = u$. By the inversion of $f_{\mathbf{g}}$: $\mathbf{g}\cdot\tilde{\mathbf{x}}^\top = (H(\mathsf{id}) - H(\mathsf{id}^*))^{-1}\cdot u$ and the fact $\mathsf{pk}_{\mathsf{id}}\cdot\mathbf{T} = (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}$, we can obtain $\mathbf{x}^\top = \mathbf{T}\tilde{\mathbf{x}}^\top$. Note that $H(\mathsf{id}) - H(\mathsf{id}^*)$ is invertible.

specific discrete Gaussian distribution as defined in Def. 2. Now we obtain $\mathsf{pk}_{\mathsf{id}}$ with such form

$$\mathsf{pk}_{\mathsf{id}} = [1|h|[1|z]\mathbf{R} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}],$$

and we can prove that the term $[1|z]\mathbf{R}$ is computationally close to the uniform distribution over R_q^d in Theorem 1 according to the RLWE assumption. However, this kind of vector cannot be used for sampling, since $h \neq z$ and the trapdoor $\mathbf{T} = \begin{bmatrix} -\mathbf{R} \\ \mathbf{I} \end{bmatrix}$ cannot be constructed. To address this issue, we design a new form of sampling vector as follows:

$$\mathsf{pk}_{\mathsf{id}} = [1|h|z|[1|z]\mathbf{R} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}]. \tag{2}$$

and redesign the sampling algorithm as in Sect. 4.2. Briefly, the modified sampling algorithm samples e_0 first, then samples a short vector $\mathbf{e} = [e_1|e_2|\mathbf{e}_3]$ satisfying

$$[1|z|[1|z]\mathbf{R} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}] \cdot \begin{bmatrix} e_1 \\ e_2 \\ \mathbf{e}_3^\top \end{bmatrix} = u - h \cdot e_0,$$

which can be rewritten as

$$[1|h|z|[1|z]\mathbf{R}_{\mathsf{id}} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{g}] \cdot \begin{bmatrix} e_1 \\ e_0 \\ e_2 \\ \mathbf{e}_3^\top \end{bmatrix} = u.$$

Therefore, this new kind of vector in Eq. (2) can still meet the sampling requirements and remove the two restrictions on the parameter k.

1.3 Related Works

In 2023, Izabachène et al. [24] combined the ABB-IBE in the module setting [1,6] with the gadget-based approximate trapdoor [14], proposed a slightly compact IBE construction, which can be proven selectively secure in the standard model. Their scheme involves a trade-off between the gadget's length d and the modulus q. Specifically, they reduce the length of the sampling lattice at the cost of generating more noise, and experiment to find the parameter sets that achieve the highest efficiency.

2 Preliminaries

Notations. We denote $\mathbb{Z}$ as the set of the integers and $\mathbb{R}$ as the set of the real numbers. We use bold uppercase letters to denote matrices (e.g., $\mathbf{A}$), and bold lowercase letters for row vectors (e.g., $\mathbf{a}$), and denote the horizontal concatenation of two vectors $\mathbf{a}, \mathbf{b}$ by $[\mathbf{a}|\mathbf{b}]$. For a (quotient) polynomial ring R over $\mathbb{Z}$, we denote $[-b, b]_R \subseteq R$ as the set of elements in R with all coefficients in the interval $[-b, b]$. For a positive integer k, let $[k]$ be the set of integers $\{0, 1, \cdots, k-1\}$.

2.1 Identity-Based Encryption

Syntax. We use the standard syntax of IBE [10,34]. Let $\mathcal{ID}$ be the ID space of the scheme. An identity-based encryption scheme Π consists of four PPT algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ defined as follows:

- $\mathsf{Setup}(1^\lambda)$: Given the security parameter λ, it outputs the master public key mpk and the master secret key msk.
- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$: Given $(\mathsf{mpk}, \mathsf{msk})$ and an identity $\mathsf{id} \in \mathcal{ID}$, it outputs the secret key $\mathsf{sk}_{\mathsf{id}}$.
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, m)$: Given the master public key mpk, an identity $\mathsf{id} \in \mathcal{ID}$, and a message m, it outputs a ciphertext ct.
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$: Given the master public key mpk, the secret key $\mathsf{sk}_{\mathsf{id}}$, and a ciphertext ct, it outputs a message m' or $\perp$.

Correctness. We say an IBE scheme is correct, if for all λ, all $\mathsf{id} \in \mathcal{ID}$ and all m in the specified message space, the following holds:

$$\Pr[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) \neq m] = \mathsf{negl}(\lambda),$$

where the probability is taken over the randomness used in $(\mathsf{mpk}, \mathsf{msk}) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$, $\mathsf{sk}_{\mathsf{id}} \xleftarrow{\$} \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$ and $\mathsf{ct} \xleftarrow{\$} \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, m)$.

IND-CPA Security. We use the following experiment to describe the security for an IBE scheme Π against selective adversaries. Formally, we consider the game between a PPT adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ defined below:

Init: At the outset of the game, $\mathcal{A}$ gives a target identity $\mathsf{id}^* \in \mathcal{ID}$ to $\mathcal{C}$.

Setup: $\mathcal{C}$ runs $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$. It gives mpk to $\mathcal{A}$ and keeps msk itself.

Phase 1: When $\mathcal{A}$ submits $\mathsf{id} \in \mathcal{ID}$ to the challenger, with the restriction that $\mathsf{id} \neq \mathsf{id}^*$, the challenger $\mathcal{C}$ responds $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$.

Challenge: At some point, $\mathcal{A}$ output a message m, on which it wishes to be challenged. Then, $\mathcal{C}$ picks a random coin $b \xleftarrow{\$} \{0, 1\}$ and a random ciphertext ct from the ciphertext space. If $b = 0$, it sets the challenge ciphertext as $\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*, m)$ and gives it to $\mathcal{A}$. If $b = 1$, it sets the challenge ciphertext as $\mathsf{ct}^* = \mathsf{ct}$ and gives it to $\mathcal{A}$.

Phase 2: After the challenge query, $\mathcal{A}$ continues to make key extraction queries.

Guess: Finally, $\mathcal{A}$ outputs a bit b' as the guess of b. The advantage of $\mathbf{A}$ is defined as

$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathcal{A},\Pi} = |\Pr[b' = b] - \frac{1}{2}|.$$

We say that Π is selectively secure, if the advantage of any PPT $\mathcal{A}$ is negligible.

2.2 Lattices and Gaussian Distributions

Lattices. An n-dimensional (full rank) lattice $\Lambda \subseteq \mathbb{R}^n$ is the set of all integer linear combinations of some set of n linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$, $\Lambda = \{\sum_{i\in[n]} x_i \mathbf{b}_i \mid \mathbf{x} \in \mathbb{Z}^n\}$. We denote $\tilde{\mathbf{B}}$ as the Gram-Schmidt orthogonalization of $\mathbf{B}$, and $\|\mathbf{B}\|_{\mathsf{GS}}$ as the length of the longest vector of $\tilde{\mathbf{B}}$. For positive integers q, n, m, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, the m-dimensional "shifted" integer lattice is defined as $\Lambda_{\mathbf{u}}^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m \mid \mathbf{A}\cdot\mathbf{e}^\top = \mathbf{u}^\top \bmod q\}$. We simply write $\Lambda^{\perp}(\mathbf{A})$ in case $\mathbf{u} = \mathbf{0}$.

Gaussian Distributions. For a n-dimensional lattice $\Lambda \subset \mathbb{R}^n$, the discrete Gaussian distribution with width $\sigma > 0$ and center $\mathbf{c} \in \mathbb{R}^n$ denoted by $\mathcal{D}_{\Lambda,\sigma,\mathbf{c}}$ is a distribution over Λ which samples $\mathbf{y} \in \Lambda$ with the probability

$$\mathcal{D}_{\Lambda,\sigma,\mathbf{c}}(\mathbf{y}) = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{y})}{\sum_{\mathbf{x}\in\Lambda}\rho_{\sigma,\mathbf{c}}(\mathbf{x})},$$

where $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp(-\pi\|\mathbf{x}-\mathbf{c}\|^2/\sigma^2)$. We abbreviate $\rho_{\sigma,\mathbf{0}}$ and $\mathcal{D}_{\Lambda,\sigma,\mathbf{0}}$ as ρ_σ and $\mathcal{D}_{\Lambda,\sigma}$. Let $\eta_\epsilon(\Lambda)$ be the smoothing parameter of Λ defined as follows.

Definition 1 ([31], Smooth parameter). *For any n-dimensional lattice Λ and positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is the smallest real $\sigma > 0$ such that $\rho_{1/\sigma}(\Lambda^*\backslash\{0\}) \le \epsilon$, where Λ^* is the dual lattice of Λ.*

For a Gaussian over lattices, we have the following tail bounds.

Lemma 1 ([22,30]). *If $x \leftarrow \mathcal{D}_{\mathbb{Z},\sigma}$ for some $\sigma > \eta_\epsilon(\mathbb{Z})$, then $\mathsf{Pr}[|x| \ge t] \le 2e^{-\pi t^2/\sigma^2}$ for all $t \ge 0$.*

Lemma 2 ([25]). *Let $\mathbf{e}$ be some vector in $\mathbb{Z}^n$ and let $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$ for some $\sigma > \eta_\epsilon(\mathbb{Z})$. Then $\mathsf{Pr}[|\mathbf{e}\mathbf{x}^\top| > t] \le 2e^{-\pi t^2/(\|\mathbf{e}\|\sigma)^2}$ for all $t \ge 0$.*

Lemma 3 ([31], Lemma 4.4). *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $\sigma > \eta_\epsilon(\Lambda)$, we have $\mathsf{Pr}_{\mathbf{x}\sim\mathcal{D}_{\Lambda,\sigma,\mathbf{c}}}[\|\mathbf{x}-\mathbf{c}\| > \sigma\sqrt{n}] \le \frac{1+\epsilon}{1-\epsilon}\cdot 2^{-n}$.*

The following re-randomization lemma helps us consider the noise distribution in the security proof of our IBE scheme.

Lemma 4 ([25], Noise re-randomization). *Let q, l, m be positive integers and σ_1 be a positive real satisfying $\sigma_1 > \max\{\eta_\epsilon(\mathbb{Z}^m), \eta_\epsilon(\mathbb{Z}^l)\}$. Let $\mathbf{b} \in \mathbb{Z}_q^m$ be arbitrary and $\mathbf{x}$ chosen from $\mathcal{D}_{\mathbb{Z}^m,\sigma_1}$. Then for any $\mathbf{V} \in \mathbb{Z}^{m\times l}$ and positive real $\sigma_2 > s_1(\mathbf{V})$, there exists a PPT algorithm $\mathsf{ReRand}(\mathbf{V}, \mathbf{b}+\mathbf{x}, \sigma_1, \sigma_2)$ that outputs $\mathbf{b}' = \mathbf{b}\mathbf{V} + \mathbf{x}' \in \mathbb{Z}_q^l$ where the statistical distance of the discrete Gaussian $\mathcal{D}_{\mathbb{Z}^l,2\sigma_1\sigma_2}$ and the distribution of $\mathbf{x}'$ is within 8ϵ.*

2.3 Rings and Ideal Lattices

Rings. Let degree n be a power of 2 and write $K = \mathbb{Q}[X]/(X^n + 1)$ the corresponding cyclotomic field. In this setup, the polynomial quotient ring $R = \mathbb{Z}[X]/(X^n + 1)$ is the ring of integers of K. Any element of the ring R can be denoted as $a = \sum_{i=0}^{n-1} a_i X^i$, where $a_i \in \mathbb{Z}$. For any prime integer q, we denote R_q as $R/qR = \mathbb{Z}_q[X]/(X^n + 1)$ and $R_q^\times$ as the set of invertible elements of R_q.

Coefficient Embedding. We define the map $\phi : R \to \mathbb{Z}^n$ that sends $a \in R$ to $\mathbf{a} = [a_0, \cdots, a_{n-1}] \in \mathbb{Z}^n$. Furthermore, we can define another map $\mathsf{rot} : R \to \mathbb{Z}^{n\times n}$ that sends $a \in R$ to a matrix in $\mathbb{Z}^{n\times n}$ such that the i-th row is $\phi(a \cdot X^{i-1} \bmod (X^n + 1)) \in \mathbb{Z}^n$. We can extend the map rot to ring vectors and matrices.

Norm and Singular Value. The norms of ring vectors (or matrices) are defined by their corresponding coefficient embedding vectors (or matrices). Similarly, the singular value of a ring matrix is defined by the singular value of its corresponding matrix through the map rot. Namely, $s_1(\mathbf{R}) = \max_{\|\mathbf{u}\|=1} \|\mathbf{u} \cdot \mathsf{rot}(\mathbf{R})\|$. We can bound the singular value of matrices over ring R.

Lemma 5 ([19], Fact 6). *For $\mathbf{R} \leftarrow \mathcal{D}_{R,\sigma}^{s\times t}$, we have $\mathsf{Pr}[s_1(\mathbf{R}) > \frac{1}{\sqrt{\pi}} \cdot \sigma \cdot \sqrt{n}(\sqrt{s} + \sqrt{t} + \omega))] \leq 4ne^{-2\pi\omega^2}$.*

The following lemma shows that R_q has exponentially many invertible elements if q satisfies some certain properties.

Lemma 6 ([25], Lemma 3). *Let q be a prime such that $q \equiv 3 \bmod 8$ and n be a power of 2. Let $R_q = \mathbb{Z}_q[X]/(X^n+1)$. Then, all $x \in R_q$ satisfying $\|\phi(x)\| < \sqrt{q}$ are invertible, i.e., $x \in R_q^\times$.*

The following lemma captures the distribution of the output of the preimage sampling algorithm.

Lemma 7 ([22], Preimage sampling). *Let $q \geq 2$ and let $\mathbf{a}$ be a vector in R_q^k. Let $\mathbf{T_a}$ be a basis for $\Lambda^\perp(\mathsf{rot}(\mathbf{a}^\top)^\top)$ and $\sigma \geq \|\mathsf{rot}(\mathbf{T_a})\|_{\mathsf{GS}} \cdot \eta_\epsilon(\mathbb{Z})$. For some $u \in R_q$, there exists a PPT algorithm $\mathsf{SamplePre}(\mathbf{a}, \mathbf{T_a}, u, \sigma)$ that returns $\mathbf{x} \in \Lambda^\perp(\mathsf{rot}(\mathbf{a}^\top)^\top)$ sampled from a distribution $(4nk)\epsilon$-close to $\mathcal{D}_{\Lambda^\perp(\mathsf{rot}(\mathbf{a}^\top)^\top),\sigma}$, whenever $\Lambda^\perp(\mathsf{rot}(\mathbf{a}^\top)^\top)$ is not empty.*

Ring Learning With Errors. The Learning With Errors (LWE) problem was introduced by Regev [32]. To improve the efficiency of LWE-based schemes, the ring version of LWE, namely RLWE, was introduced [27].

Definition 2 ([27], RLWE). *For positive integers $n = n(\lambda), k = k(n)$, a prime integer $q = q(n) > 2$, an error distribution $\chi = \chi(n)$ over R, and an*

PPT algorithm $\mathcal{A}$, the advantage for the Ring-LWE problem $\mathsf{RLWE}_{n,k,q,\chi}$ of $\mathcal{A}$ is defined as follows:

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{RLWE}_{n,k,q,\chi}} = |\Pr[\mathcal{A}(\{(u_i, v_i)\}_{i=1}^{k}) \to 1] - \Pr[\mathcal{A}(\{(u_i, u_i s + e_i)\}_{i=1}^{k}) \to 1]|,$$

where $u_1, \cdots, u_k, v_1, \cdots, v_k \xleftarrow{\$} R_q, s \xleftarrow{\$} R_q$ and $e_1, \cdots, e_k \xleftarrow{\$} \chi$. We say that $\mathsf{RLWE}_{n,k,q,\chi}$ assumption holds if $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{RLWE}_{n,k,q,\chi}}$ is negligible for all PPT adversary $\mathcal{A}$.

2.4 NTRU lattices

Definition 3 ([18], NTRU lattices). *Let q be a positive integer, and $f, g \in R$. Let $h = g \cdot f^{-1} \bmod q$. The NTRU lattice constrained by h and q is*

$$\Lambda_{\mathsf{NTRU}} = \{(u, v) \in R^2 \mid u + v \cdot h = 0 \bmod q\}.$$

Λ_{NTRU} is a full-rank lattice of $\mathbb{Z}^{2n}$.

Definition 4 (DSPR assumption). *For positive integers $n = n(\lambda), q = q(n) > 2$, let $R = \mathbb{Z}[X]/(X^n+1)$ and $R_q = R/qR$, and let ψ denote a distribution over R. The decisional small polynomial ratio (DSPR) assumption $\mathsf{DSPR}_{n,q,\psi}$ says that the following two distributions are hard to distinguish:*

- *a polynomial $h = g \cdot f^{-1} \in R_q$, where $g, f \leftarrow \psi$ and f is invertible in R_q.*
- *a polynomial $u \xleftarrow{\$} R_q$.*

Lemma 8 (NTRU trapdoors). *Let $\Lambda_{\mathsf{NTRU}}, f, g$ be defined as Def. 3. There exists an efficient algorithm $\mathsf{TrapGen}(f, g)$ to generate a pair $(h, \mathbf{T}_h) \in R_q \times R^{2\times 2}$ satisfying $h = g \cdot f^{-1} \bmod q$ and $\mathbf{T}_h$ is the short basis for Λ_{NTRU}, i.e., $[1|h] \cdot \mathbf{T}_h = \mathbf{0} \bmod q$. Further, the Gram-Schmidt norm of the basis is $\|\mathsf{rot}(\mathbf{T})\|_{\mathsf{GS}} \leq 1.17\sqrt{q}$.*

3 Computational Indistinguishability

Let $\mathbf{a}$ and $\mathbf{b}$ be vectors chosen uniformly in R_q^k and R_q^d respectively. Let $\mathbf{R}$ be a $k \times d$ matrix chosen from a specific distribution. To prove the two distributions $(\mathbf{a}, \mathbf{aR})$ and $(\mathbf{a}, \mathbf{b})$ are indistinguishable, a very common statistical approach is Leftover Hash Lemma, which requires $k > \log q$. To remove this restriction, we use computational indistinguishability instead the statistical closeness.

Theorem 1. *Let $n = n(\lambda)$, $k = k(n) \geq 2$ and $d = d(n)$ be positive integers, $\chi = \chi(n)$ be a specific distribution in Def. 2 and $R = \mathbb{Z}[X]/(X^n+1)$, $R_q = R/qR$. Let h be a uniformly random element in R_q, and b be vectors chosen uniformly in R_q^d, $\mathbf{a} = [1|h] \in R_q^2$. Let $\mathbf{R}$ be a $2 \times d$ matrix chosen from $\chi^{2\times d}$. Then the distribution $(\mathbf{a}, \mathbf{aR})$ is computationally close to the distribution $(\mathbf{a}, \mathbf{b})$.*

Proof. Now we prove that the two distributions are computationally indistinguishable by a sequence of games between a challenger $\mathcal{C}$ and adversary $\mathcal{A}$.

$$\left([1|h], [1|h] \cdot \underbrace{\begin{bmatrix} e_1, \cdots, e_d \\ s_1, \cdots, s_d \end{bmatrix}}_{\mathbf{R}}\right) \approx_c \left([1|h], \begin{bmatrix} b_1, \cdots, b_d \end{bmatrix}\right)$$

Game 0. The challenger flips a coin $r \xleftarrow{\$} \{0,1\}$. If $r = 0$, $\mathcal{C}$ sends the former distribution to $\mathcal{A}$. If $r = 1$, $\mathcal{C}$ sends the latter distribution to $\mathcal{A}$. $\mathcal{A}$ outputs a guess bit $r' \in \{0,1\}$. We say the adversary $\mathcal{A}$ wins if $r' = r$.

Game 1. In this game, we change the way b_1 is chosen. Recall in Game 0, b_1 is chosen uniformly in R_q. In Game 1, the challenger chooses

$$b_1 = h \cdot s_1 + e_1.$$

By $\mathsf{RLWE}_{n,1,q,\chi}$ assumption as in Def. 2, Game 1 is computationally indistinguishable from Game 0. That is,

$$|\mathsf{Pr}[\mathcal{A}_{\text{Game 0}} = 1] - \mathsf{Pr}[\mathcal{A}_{\text{Game 1}} = 1]| \leq \mathsf{Adv}^{\mathsf{RLWE}_{n,1,q,\chi}}. \tag{3}$$

Game d. So on and so forth, in Game d, we change the way b_d is chosen to

$$b_d = h \cdot s_d + e_d.$$

Similarly,

$$|\mathsf{Pr}[\mathcal{A}_{\text{Game d-1}} = 1] - \mathsf{Pr}[\mathcal{A}_{\text{Game d}} = 1]| \leq \mathsf{Adv}^{\mathsf{RLWE}_{n,1,q,\chi}}. \tag{4}$$

Moreover, in Game d, $\mathcal{C}$ samples the identical distribution whether $r = 0$ or $r = 1$, and thus the advantage of the adversary $\mathcal{A}$ is exactly 0, i.e.,

$$\mathsf{Pr}[\mathcal{A}_{\text{Game d}} = 1] = \frac{1}{2}. \tag{5}$$

Combining the equations Eq. (3), Eq. (4) and Eq. (5), we obtain

$$|\mathsf{Pr}[\mathcal{A}_{\text{Game 0}} = 1] - \frac{1}{2}| \leq d \cdot \mathsf{Adv}^{\mathsf{RLWE}_{n,1,q,\chi}}.$$

Therefore, the advantage of the adversary in Game 0 is negligible under the RLWE assumption. We complete the proof.

4 Sampling Algorithms over NTRU Lattices

In this section, We first recall the sampling algorithms from [1] and show how to embed the NTRU trapdoor into sampling algorithms.

4.1 Recall sampling algorithms from [1]

In [22], the Ajtai trapdoor generation algorithm outputs a pair $(\mathbf{a}, \mathbf{T_a}) \in R_q^k \times R^{k\times k}$ satisfying that $\mathbf{a}\cdot\mathbf{T_a} = \mathbf{0} \bmod q$. Later, to improve the efficiency of lattice-based IBE in the standard model, Agrawal, Boneh, and Boyen constructed a family of lattices for which there are two distinct trapdoors for sampling, one is the Ajtai trapdoor, another is a "low norm" randomization matrix $\mathbf{R}$, used in the real world and security proof, respectively. Recall the sampling technique from [1]: the sampling vector is

$$\mathbf{f} = [\mathbf{a}|\mathbf{aR} + y\mathbf{g}]$$

where $\mathbf{R} \in R^{k\times d}$ is a secret, trapdoor matrix with small, random entries, $y \in R_q^\times$ is an invertible element and $\mathbf{g} = [1|b|\cdots|b^{d-1}] \in R_q^d$ is the specific gadget vector [30], which trapdoor $\mathbf{T_g}$ is publicly known. For some $u \in R_q$, the goal is to sample a short vector $\mathbf{e}$ that satisfying

$$\mathbf{f}\cdot\mathbf{e}^\top = u \bmod q.$$

The sampling algorithms consist of two parts: $\mathsf{SampleLeft}$ and $\mathsf{SampleRight}$.

$\mathsf{SampleLeft}(\mathbf{a} \in R_q^k, \mathbf{b} \in R_q^d, \mathbf{T_a} \in R^{k\times k}, u \in R_q, \sigma \geq \|\mathsf{rot}(\mathbf{T_a})\|_{\mathsf{GS}} \cdot \eta_\epsilon(\mathbb{Z}))$

- sample a random vector $\mathbf{e}_2 \in R^d$ distributed $(4nd)\epsilon$-close to $\mathcal{D}_{R,\sigma}^d$.
- run $\mathbf{e}_1 \leftarrow \mathsf{SamplePre}(\mathbf{a}, \mathbf{T_a}, u', \sigma)$ where $u' = u - \mathbf{b}\cdot\mathbf{e}_2^\top$.
- output $\mathbf{e} = [\mathbf{e}_1|\mathbf{e}_2] \in R^{k+d}$.

$\mathsf{SampleRight}(\mathbf{a} \in R_q^k, \mathbf{R} \in R^{k\times d}, \mathbf{g} \in R_q^d, \mathbf{T_g} \in R^{d\times d}, y \in R_q^\times, u \in R_q, \sigma \geq s_1(\mathbf{R}) \cdot \|\mathsf{rot}(\mathbf{T_g})\|_{\mathsf{GS}} \cdot \eta_\epsilon(\mathbb{Z}))$

- Sample a perturbation $\mathbf{p} \leftarrow \mathcal{D}_{R,\sqrt{\sum_p}}^{k+d}$ where $\sum_p$ is a positive definite matrix defined as $\sum_p := \sigma^2\mathbf{I} - s^2 \begin{bmatrix} \mathbf{R}\mathbf{R}^\top & \mathbf{R}^\top \\ \mathbf{R} & \mathbf{I} \end{bmatrix}$.
- Form $v = u - [\mathbf{a}|\mathbf{aR} + y\mathbf{g}]\cdot\mathbf{p}^\top$.
- run $\mathbf{x} \leftarrow \mathsf{SamplePre}(\mathbf{g}, \mathbf{T_g}, v', s)$ where $v' = y^{-1}\cdot v$.
- output $\mathbf{e}^\top = \mathbf{p}^\top + \begin{bmatrix} -\mathbf{R} \\ \mathbf{I}_d \end{bmatrix} \cdot \mathbf{x}^\top \in R^{k+d}$.

Lemma 9. *The distributions of the outputs of* $\mathsf{SampleLeft}$ *and* $\mathsf{SampleRight}$ *are both* $4n(k+d)\epsilon$*-close to* $\mathcal{D}_{\Lambda_{\phi(u)}^\perp(\mathsf{rot}(\mathbf{f}^\top)^\top),\sigma}$ *for any* $\sigma \geq \max\{\|\mathsf{rot}(\mathbf{T_a})\|_{\mathsf{GS}}, s_1(\mathbf{R}) \cdot \|\mathsf{rot}(\mathbf{T_g})\|_{\mathsf{GS}}\} \cdot \eta_\epsilon(\mathbb{Z})$.

4.2 New sampling algorithms based on NTRU trapdoor

As mentioned in the introduction, the main idea of designing a new sampling algorithm is to adapt the algorithms from [1] with the NTRU trapdoor. In [18],

the NTRU trapdoor generation algorithm outputs a pair $(h, \mathbf{T}_h) \in R_q \times R^{2\times 2}$ satisfying that $[1|h] \cdot \mathbf{T}_h = \mathbf{0} \bmod q$. For the security, we construct the sampling vector as

$$\mathbf{f}_{\mathsf{NTRU}} = [1|h|z|[1|z]\mathbf{R} + y\mathbf{g}]$$

where z is an element chosen uniformly at random from R_q and the rest unchanged. We define the sampling algorithms over NTRU lattices.

$\mathsf{SampleLeft}_{\mathsf{NTRU}}(h \in R_q, \mathbf{b} \in R_q^{d+1}, \mathbf{T}_h \in R^{2\times 2}, u \in R_q, \sigma \geq \|\mathsf{rot}(\mathbf{T}_h)\|_{\mathsf{GS}} \cdot \eta_\epsilon(\mathbb{Z}))$

- sample a random vector $\mathbf{e}_2 \in R^{d+1}$ distributed $4n(d+1)\epsilon$-close to $\mathcal{D}_{R,\sigma}^{d+1}$.
- run $\mathbf{e}_1 \leftarrow \mathsf{SamplePre}([1|h], \mathbf{T}_h, v, \sigma)$ where $v = u - \mathbf{b} \cdot \mathbf{e}_2^\top$.
- output $\mathbf{e} = [\mathbf{e}_1|\mathbf{e}_2] \in R^{3+d}$.

$\mathsf{SampleRight}_{\mathsf{NTRU}}(h \in R_q, \mathbf{R} \in R^{2\times d}, \mathbf{g} \in R_q^d, \mathbf{T}_{\mathbf{g}} \in R^{d\times d}, y \in R_q^\times, u \in R_q, \sigma \geq s_1(\mathbf{R}) \cdot \|\mathsf{rot}(\mathbf{T}_{\mathbf{g}})\|_{\mathsf{GS}} \cdot \eta_\epsilon(\mathbb{Z}))$

- sample a random element $e' \in R$ distributed $(4n)\epsilon$-close to $\mathcal{D}_{R,\sigma}$.
- Form $u' = u - h \cdot e'$.
- Sample a perturbation $\mathbf{p} \leftarrow \mathcal{D}_{R,\sqrt{\sum_p}}^{2+d}$ where $\sum_p$ defined as above.
- Form $v = u' - [1|z|[1|z]\mathbf{R} + y\mathbf{g}] \cdot \mathbf{p}^\top$.
- run $\mathbf{x} \leftarrow \mathsf{SamplePre}(\mathbf{g}, \mathbf{T}_{\mathbf{g}}, v', s)$ where $v' = y^{-1} \cdot v$.
- write $\mathbf{R} = \begin{bmatrix}\mathbf{r}_1\\ \mathbf{r}_2\end{bmatrix}, \mathbf{p}^\top = \begin{bmatrix}p_1\\ p_2\\ \mathbf{p}_3^\top\end{bmatrix}$, compute $\tilde{\mathbf{e}}^\top = \mathbf{p}^\top + \begin{bmatrix}-\mathbf{R}\\ \mathbf{I}_d\end{bmatrix}\mathbf{x}^\top = \begin{bmatrix}p_1 - \mathbf{r}_1 \cdot \mathbf{x}^\top\\ p_2 - \mathbf{r}_2 \cdot \mathbf{x}^\top\\ \mathbf{p}_3^\top + \mathbf{x}^\top\end{bmatrix}$.
- Insert e' into $\tilde{e}$, output $\mathbf{e}^\top = \begin{bmatrix}p_1 - \mathbf{r}_1 \cdot \mathbf{x}^\top\\ e'\\ p_2 - \mathbf{r}_2 \cdot \mathbf{x}^\top\\ \mathbf{p}_3^\top + \mathbf{x}^\top\end{bmatrix} \in R^{3+d}$.

Theorem 2. *Let $(h, \mathbf{T}_h)$ be generated from the NTRU trapdoor generation algorithm. The two distributions from $\mathsf{SampleLeft}_{\mathsf{NTRU}}$ and $\mathsf{SampleRight}_{\mathsf{NTRU}}$ are both $4n(3+d)\epsilon$-close to $\mathcal{D}_{\Lambda_{\phi(u)}^\perp(\mathsf{rot}(\mathbf{f}_{\mathsf{NTRU}}^\top)^\top),\sigma}$ for any $\sigma \geq \max\{\|\mathsf{rot}(\mathbf{T}_h)\|, s_1(\mathbf{R}) \cdot \|\mathsf{rot}(\mathbf{T}_{\mathbf{g}})\|_{\mathsf{GS}}\} \cdot \eta_\epsilon(\mathbb{Z})$.*

Proof. For the $\mathsf{SampleLeft}_{\mathsf{NTRU}}$, the distribution of the short vector $\mathbf{e}$ is $4n(3+d)\epsilon$-close to $\mathcal{D}_{\Lambda_{\phi(u)}^\perp([\mathsf{rot}([1|h]^\top)^\top|\mathsf{rot}(\mathbf{b}^\top)^\top]),\sigma}$ from Lemma 9. For the $\mathsf{SampleRight}_{\mathsf{NTRU}}$, we know the short vector $\tilde{\mathbf{e}}^\top = \mathbf{p}^\top + \begin{bmatrix}-\mathbf{R}\\ \mathbf{I}_d\end{bmatrix} \cdot \mathbf{x}^\top \in R^{2+d}$ satisfies

$$[1|z|[1|z]\mathbf{R} + y\mathbf{g}] \cdot \left(\mathbf{p}^\top + \begin{bmatrix}-\mathbf{r}_1 \cdot \mathbf{x}^\top\\ -\mathbf{r}_2 \cdot \mathbf{x}^\top\\ \mathbf{x}^\top\end{bmatrix}\right) = u' = u - h \cdot e'$$

and the distribution of $\tilde{\mathbf{e}}$ is $4n(2+d)\epsilon$-close to $\mathcal{D}_{\Lambda^{\perp}_{\phi(u')}([\mathsf{rot}([1|z]^{\top})^{\top}|\mathsf{rot}([[1|z]\mathbf{R}+y\mathbf{g}]^{\top})^{\top}]),\sigma}$ from Lemma 9. Inserting e' into the vector $\tilde{\mathbf{e}}$, we obtain the vector $\mathbf{e}$ satisfies

$$[1|h|z|[1|z]\mathbf{R}+y\mathbf{g}]\cdot\begin{bmatrix}-\mathbf{r}_1\cdot\mathbf{x}^{\top}\\ e'\\ -\mathbf{r}_2\cdot\mathbf{x}^{\top}\\ \mathbf{x}^{\top}\end{bmatrix}=u.$$

Since the distribution of e' is $4n(3+d)\epsilon$-close to $\mathcal{D}_{R,\sigma}$, the distribution of the total vector $\mathbf{e}$ generated by $\mathsf{SampleRight}_{\mathsf{NTRU}}$ is statistically close to $\mathcal{D}_{\Lambda^{\perp}_{\phi(u)}([\mathsf{rot}([1|h]^{\top})^{\top}|\mathsf{rot}(\mathbf{b}^{\top})^{\top}]),\sigma}$ where $\mathbf{b}=[z|[1|z]\mathbf{R}+y\mathbf{g}]$. We complete the proof.

5 IBE Scheme

In this section, we show our IBE scheme based on the RLWE assumption and DSPR assumption, including the construction and the security proof.

5.1 Construction

Let the identity space of the scheme be $\mathcal{ID}=\{0,1\}^{\kappa}$ for some $\kappa<n$ and the message space be $\mathcal{M}=\{0,1\}^{n}\subset R$[5]. Let $n:=n(\lambda)$, $b:=b(n)$, $d:=d(n)$, $q:=q(n)$, $\sigma:=\sigma(n)$, $\sigma_1:=\sigma_1(n)$ and $\sigma_{\mathsf{R}}:=\sigma_{\mathsf{R}}(n)$ be parameters that are specified later. Let $\chi=\mathcal{D}_{R,\sigma_{\mathsf{R}}},\psi=\mathcal{D}_{R,1.17\sqrt{\frac{q}{2n}}}$. Let $R=\mathbb{Z}[X]/(X^n+1)$ and $R_q=\mathbb{Z}_q[X]/(X^n+1)$. Let $H:\{0,1\}^{\kappa}\to R_q$ be the identity function, i.e., given a bit string $\mathsf{id}=\mathsf{id}_0\mathsf{id}_1\cdots\mathsf{id}_{\kappa-1}$, output $\mathsf{id}=\mathsf{id}_0+\mathsf{id}_1X+\cdots+\mathsf{id}_{\kappa-1}X^{\kappa-1}\in R_q$.

$\mathsf{Setup}(1^{\lambda})$**.** On input a security parameter λ, set the parameters as specified in Sect. 6 below, do:

1. Generate $(h,\mathbf{T}_h)\in R_q\times R^{2\times 2}$ as defined in Lemma 8.
2. Pick a uniformly random d-vector $\mathbf{w}\xleftarrow{\$}R_q^d$.
3. Pick two uniformly random elements $u,z\xleftarrow{\$}R_q$.
4. Pick a uniformly random element $t\leftarrow R_q^{\times}$.
5. Output the master public key and the master secret key,

$$\mathsf{mpk}=(h,z,\mathbf{w},u,t),\quad \mathsf{msk}=\mathbf{T}_h.$$

$\mathsf{KeyGen}(\mathsf{mpk},\mathsf{msk},\mathsf{id})$**.** On input the master public key mpk, the master secret key msk, and an identity $\mathsf{id}\in\mathcal{ID}$, do:

1. Run $\mathsf{SampleLeft}_{\mathsf{NTRU}}(h,[z|\mathbf{w}+H(\mathsf{id})\mathbf{g}],\mathbf{T}_h,t^{-1}u,\sigma)$ to sample a short vector $\mathbf{e}_{\mathsf{id}}\in R^{3+d}$, such that

$$[1|h|z|\mathbf{w}+H(\mathsf{id})\mathbf{g}]\cdot\mathbf{e}_{\mathsf{id}}^{\top}=t^{-1}u.$$

[5] Note that we regard m as an element in R via $\phi^{-1}:\mathbb{Z}^n\to R$.

2. Output $\mathsf{sk}_{\mathsf{id}} := \mathbf{e}_{\mathsf{id}} \in R^{3+d}$.

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, m)$**.** On input the master public key mpk, an identity $\mathsf{id} \in \mathcal{ID}$, and a message $m \in \mathcal{M}$, do:

1. Set $\mathbf{f}_{\mathsf{id}} = [1|h|z|\mathbf{w} + H(\mathsf{id})\mathbf{g}] \in R_q^{3+d}$.
2. Choose a small $s \leftarrow \mathcal{D}_{R,\sigma_\mathsf{R}}$.
3. Choose noise vectors $e_0 \leftarrow \mathcal{D}_{R,\sigma_\mathsf{R}}$, $\mathbf{e}_1 \leftarrow \mathcal{D}_{R,\sigma_1}^{3+d}$.
4. Set $c_0 = u \cdot s + e_0 + \lfloor \frac{q}{2} \rceil m \in R_q$ and $\mathbf{c}_1 = t \cdot \mathbf{f}_{\mathsf{id}} \cdot s + \mathbf{e}_1 \in R_q^{3+d}$.
5. Output the ciphertext $\mathsf{ct} := (c_0, \mathbf{c}_1) \in R_q \times R_q^{3+d}$.

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$**.** On input the master public key mpk, the user secret key $\mathsf{sk}_{\mathsf{id}} := \mathbf{e}$, and the ciphertext $\mathsf{ct} := (c_0, \mathbf{c}_1)$, do:

1. Output $\lfloor 2/q \cdot \phi(c_0 - \mathbf{c}_1 \cdot \mathbf{e}^\top) \rceil \bmod 2$.

Lemma 10 (Correctness). *If parameters σ_R, σ, σ_1, n, d and q satisfy $\sqrt{\frac{70}{\pi}}\sigma_\mathsf{R} + \sqrt{\frac{70}{\pi}}\sigma\sigma_1\sqrt{n(3+d)} < q/5$, then the above IBE scheme has decryption error at most $4e^{-70} + 2^{-n(3+d)} + 2^{-100}$.*

Proof. For the Dec algorithm to output m, we need to find the condition that the error term does not exceed, say $q/5$. First, we have the following equality:

$$\begin{aligned} c_0 - \mathbf{c}_1 \cdot \mathbf{e}^\top &= u \cdot s + e_0 + \lfloor \frac{q}{2} \rceil m - (t \cdot \mathbf{f}_{\mathsf{id}} \cdot s + \mathbf{e}_1) \cdot \mathbf{e}^\top \\ &= \underbrace{(e_0 - \mathbf{e}_1 \cdot \mathbf{e}^\top)}_{\text{error term}} + \lfloor \frac{q}{2} \rceil m \end{aligned}$$

By Lemma 1 and $e_0 \leftarrow \mathcal{D}_{R,\sigma_\mathsf{R}}$, we have

$$\mathsf{Pr}[|\phi(e_0)_j| > t_1] \le 2e^{-\pi t_1^2/\sigma_\mathsf{R}^2}. \tag{6}$$

By Lemma 2 and $\mathbf{e}_1 \leftarrow \mathcal{D}_{R,\sigma_1}^{3+d}$, we have

$$\mathsf{Pr}[|\phi(\mathbf{e}_1)\mathsf{rot}(\mathbf{e}^\top)_j| > t_2] \le 2e^{-\pi t_2^2/(\|\mathbf{e}\|\sigma_1)^2}. \tag{7}$$

By Theorem 2, $\mathbf{e}$ is $4n(3+d)\epsilon$-close to $\mathcal{D}_{\Lambda^\perp_{\phi(u)}(\mathsf{rot}(\mathbf{f}_{\mathsf{NTRU}}^\top)^\top),\sigma}$ for some σ. Further, by Lemma 3 and take $\epsilon = \frac{1}{4n(3+d)\cdot 2^{100}}$, we have

$$\mathsf{Pr}[\|\mathbf{e}\| \ge \sigma\sqrt{n(3+d)}] \le 2^{-n(3+d)} + 2^{-100}.$$

Then, take $t_1 = \sqrt{\frac{70}{\pi}}\sigma_\mathsf{R}$ in Eq. (6) and $t_2 = \sqrt{\frac{70}{\pi}}\sigma\sigma_1\sqrt{n(3+d)}$ in Eq. (7), we have

$$\mathsf{Pr}[|(\phi(e_0) - \phi(\mathbf{e}_1)\mathsf{rot}(\mathbf{e}^\top))_j| > t_1 + t_2] \le 4e^{-70} + 2^{-n(3+d)} + 2^{-100}.$$

Therefore, if $t_1 + t_2 = \sqrt{\frac{70}{\pi}}\sigma_\mathsf{R} + \sqrt{\frac{70}{\pi}}\sigma\sigma_1\sqrt{n(3+d)} < q/5$, then the decryption error occurs with probability $4e^{-70} + 2^{-n(3+d)} + 2^{-100}$.

Parameter Constraints. To ensure correctness and security, we require:

- n, q: By Lemma 6, n is a power of 2 and q is a prime such that $q \equiv 3 \bmod 8$.
- d: By [30], the gadget vector $\mathbf{g} = [1|b|\cdots|b^{d-1}] \in R_q^d$ satisfies $d \geq \lceil \log_b q \rceil$.
- σ: By Theorem 2, σ should be sufficiently large so the sampling algorithms work. Concretely, $\sigma > \|\mathsf{rot}(\mathbf{T}_h)\|_{\mathsf{GS}} \cdot \eta_\epsilon(\mathbb{Z})$ and $\sigma > s_1(\mathbf{R}_{\mathsf{id}}) \cdot \sqrt{b^2+1} \cdot \eta_\epsilon(\mathbb{Z})$. By Lemma 8 and Lemma 5, we have

$$\|\mathsf{rot}(\mathbf{T}_h)\|_{\mathsf{GS}} \leq 1.17 \cdot \sqrt{q}, \quad \mathsf{Pr}[s_1(\mathbf{R}_{\mathsf{id}}) > \frac{1}{\sqrt{\pi}} \cdot \sigma_{\mathsf{R}} \cdot \sqrt{n} \cdot (\sqrt{2} + \sqrt{d} + \omega)] \leq 4ne^{-2\pi\omega^2}.$$

- σ_1: By Lemma 4, $\sigma_1 \geq 2\sigma_{\mathsf{R}} \cdot s_1 \left(\begin{bmatrix} 0\,1\,0\,\mathbf{0} \\ 1\,0\,0\,\mathbf{r}_1 \\ 0\,0\,1\,\mathbf{r}_2 \end{bmatrix} \right)$.
- *Error term*: Lemma 10 requires $\sqrt{\frac{70}{\pi}}\sigma_{\mathsf{R}} + \sqrt{\frac{70}{\pi}}\sigma\sigma_1\sqrt{n(3+d)} < q/5$ for the decryption error to be negligible.

5.2 Security Proof

Theorem 3. *The above IBE scheme is selectively secure in the standard model assuming the hardness of* $\mathsf{RLWE}_{n,4,q,\chi}$ *and* $\mathsf{DSPR}_{n,q,\psi}$*, where the ciphertext space is* $R_q \times R_q^{3+d}$.

Proof. The proof proceeds in a sequence of games where the first game is identical to the real security game. In the last game of the sequence, the adversary has an advantage of zero. We show that a PPT adversary cannot distinguish between the games which will prove that the adversary has a negligible advantage in winning the original game.

Game 0. This is the real security game.

Game 1. In this game, we change the way $\mathbf{w}$ is chosen. Recall in Game 0, the challenger chooses a uniformly random d-vector $\mathbf{w} \xleftarrow{\$} R_q^d$. In Game 1, let id^* be the identity that $\mathcal{A}$ intends to attack. During the setup phase, the challenger sets $\mathbf{a} = [1|z]$, samples a matrix $\mathbf{R}_{\mathsf{id}^*} \leftarrow \mathcal{D}_{R,\sigma_{\mathsf{R}}}^{2\times d}$, and constructs $\mathbf{w}$ as

$$\mathbf{w} = \mathbf{a}\mathbf{R}_{\mathsf{id}^*} - H(\mathsf{id}^*)\mathbf{g}. \tag{8}$$

By Theorem 1, the distribution $(\mathbf{a}, \mathbf{a}\mathbf{R}_{\mathsf{id}^*})$ is computationally close to the distribution $(\mathbf{a}, \mathbf{w}')$ where $\mathbf{w}'$ is a uniform R_q^d vector. It follows that in the adversary's view, the vector $\mathbf{a}\mathbf{R}_{\mathsf{id}^*}$ is computationally close to uniform, and therefore $\mathbf{w}$ as defined in Eq. (8) is close to uniform. Hence, Game 1 is indistinguishable from Game 0.

Game 2. In this game, we change the way of responding to the key extraction queries. To respond to a key extraction query for $\mathsf{id} \neq \mathsf{id}^*$, the challenger needs a short vector $\mathbf{e}$ that satisfies $\phi(\mathbf{e}) \in \Lambda^{\perp}_{\phi(t^{-1}u)}([\mathsf{rot}(\mathbf{f}_{\mathsf{id}}^{\top})^{\top}])$ where

$$\mathbf{f}_{\mathsf{id}} \coloneqq [1|h|z|\mathbf{w} + H(\mathsf{id})\mathbf{g}] = [1|h|z|[1|z]\mathbf{R}_{\mathsf{id}^*} + (H(\mathsf{id}) - H(\mathsf{id}^*))\,\mathbf{g}].$$

$H(\cdot)$ converts a bit string id to a ring element as defined in Sect. 5.1, then

$$\|\phi(H(\mathsf{id}) - H(\mathsf{id}^*))\| \leq \|\phi(H(\mathsf{id}))\| + \|\phi(H(\mathsf{id}^*))\| = 2\sqrt{\kappa} < 2\sqrt{n} < \sqrt{q}. \quad (9)$$

The first inequality comes from the triangle inequality, the second comes from the parameter setting $\kappa < n$ in Sect. 5.1 and the last can be derived from Lemma 10. Combining Lemma 6 and Eq. (9), $H(\mathsf{id}) - H(\mathsf{id}^*)$ is invertible. The challenger can now respond to the key extraction query by running

$$\mathbf{e} \leftarrow \mathsf{SampleRight}_{\mathsf{NTRU}}(h, \mathbf{R}_{\mathsf{id}^*}, \mathbf{g}, \mathbf{T}_{\mathbf{g}}, H(\mathsf{id}) - H(\mathsf{id}^*), t^{-1}u, \sigma).$$

Theorem 2 shows that, for our choice of σ, the generated $\mathbf{e}$ is distributed close to $\mathcal{D}_{\Lambda^{\perp}_{\phi(t^{-1}u)}([\mathsf{rot}(\mathbf{f}_{\mathsf{id}}^{\top})^{\top}]),\sigma}$ as in Game 1. Hence, the adversary's advantage in Game 2 is at most negligibly different from its advantage in Game 1.

Game 3. In this game, we change the way h is chosen. Recall in Game 2, the challenger generates an NTRU pair $(h, \mathbf{T}_h) \in R_q \times R^{2\times 2}$. In Game 3, the challenger chooses a uniform $h \xleftarrow{\$} R_q$. We show that the distributions of Game 3 and Game 2 are indistinguishable provided the $\mathsf{DSPR}_{n,q,\psi}$ assumption.

Reduction from DSPR. Suppose a PPT adversary $\mathcal{A}$ is non-negligible in distinguishing Game 2 and Game 3, then we can use $\mathcal{A}$ to construct another PPT adversary $\mathcal{B}$ to distinguish the DSPR instance.

Instance. $\mathcal{B}$ is given the DSPR instance $h \in R_q$.

Setup. To make up the master public key mpk, $\mathcal{B}$ first chooses $z \xleftarrow{\$} R_q$ and sets $\mathbf{w}$ as Game 1. Then $\mathcal{B}$ samples $u \xleftarrow{\$} R_q$. Finally, it outputs $\mathsf{mpk} = (h, z, \mathbf{w}, u)$, which simulates the setup phase.

Phase 1 & Phase 2. When $\mathcal{A}$ makes the key extraction queries, $\mathcal{B}$ responds as in Game 2.

Challenge. When $\mathcal{A}$ makes the challenge query for the challenge identity id^* and a message m, $\mathcal{B}$ responds as in Game 0.

Guess. When $\mathcal{A}$ receives the challenge ciphertext, it guesses if it is interacting with the Game 2 or Game 3 challenger. $\mathcal{B}$ outputs $\mathcal{A}$'s guess as the answer to the DSPR challenge it is trying to solve.

When the DSPR oracle is pseudorandom, i.e., $h = g \cdot f^{-1}$ for some $g, f \leftarrow \psi$ and f is invertible in R_q, the challenge ciphertext is distributed exactly as in Game 2. When the DSPR oracle is truly random, then the challenge ciphertext is distributed exactly as in Game 3. As a result, the advantage of $\mathcal{B}$ is the same as that of $\mathcal{A}$. By the $\mathsf{DSPR}_{n,q,\psi}$ assumption, the advantage of $\mathcal{B}$ is negligible, and then the advantage of $\mathcal{A}$ in distinguishing Game 2 and Game 3 is negligible. This completes the proof.

Game 4. In this game, we change the way that the challenge ciphertext $(c_0, \mathbf{c}_1)$ is generated in the Enc algorithm. Recall in the previous games, the challenger picks $e_0 \leftarrow \mathcal{D}_{R,\sigma_\mathsf{R}}, \mathbf{e}_1 \leftarrow \mathcal{D}^{3+d}_{R,\sigma_1}$. The corresponding ciphertext is

$$c_0 = u \cdot s + e_0 + \lfloor \frac{q}{2} \rceil m, \quad \mathbf{c}_1 = t \cdot \mathbf{f}_\mathsf{id} \cdot s + \mathbf{e}_1. \tag{10}$$

While in Game 4, the challenger picks $\mathbf{e}' \leftarrow \mathcal{D}^3_{R,\sigma_\mathsf{R}}$, $\mathbf{v} = t \cdot [h|1|z] \cdot s + \mathbf{e}'$ and sets the challenge ciphertext $\mathbf{c}_1$ as

$$c_0 = t \cdot u \cdot s + e_0 + \lfloor \frac{q}{2} \rceil m, \quad \mathbf{c}_1 = \mathsf{ReRand}\left(\begin{bmatrix} 0\ 1\ 0\ \mathbf{0} \\ 1\ 0\ 0\ \mathbf{r}_1 \\ 0\ 0\ 1\ \mathbf{r}_2 \end{bmatrix}, \mathbf{v}, \sigma_\mathsf{R}, \frac{\sigma_1}{2\sigma_\mathsf{R}} \right), \tag{11}$$

where $\mathbf{R}_{\mathsf{id}^*} = \begin{bmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{bmatrix}$. We claim that this change alters the view of $\mathcal{A}$ only negligibly. By the property of ReRand (Lemma 4), we can rewrite the changed ciphertext $\mathbf{c}_1$ as

$$\mathbf{c}_1 = t \cdot [h|1|z] \cdot \begin{bmatrix} 0\ 1\ 0\ \mathbf{0} \\ 1\ 0\ 0\ \mathbf{r}_1 \\ 0\ 0\ 1\ \mathbf{r}_2 \end{bmatrix} \cdot s + \mathbf{e}'_1 = t \cdot [1|h|z|[1|z]\mathbf{R}_{\mathsf{id}^*}]s + \mathbf{e}'_1 \tag{12}$$

where the distribution of $\mathbf{e}'_1$ is within negligible distance from the discrete Gaussian distribution $\mathcal{D}^{3+d}_{R,\sigma_1}$. Here, we use the fact that $\mathbf{f}_{\mathsf{id}^*} = [1|h|z|[1|z]\mathbf{R}_{\mathsf{id}^*}]$ holds since $\mathsf{id} = \mathsf{id}^*$. It can be readily seen that the distribution of the changed ciphertext in Eq. (12) is statistically close to that in Eq. (10).

Game 5. In this game, we further change the way the challenge ciphertext is created. Recall in the Game 4, the challenger picks $e_0 \leftarrow \mathcal{D}_{R,\sigma_\mathsf{R}}, \mathbf{e}' \leftarrow \mathcal{D}^3_{R,\sigma_\mathsf{R}}$, sets $\mathbf{v} = t \cdot [h|1|z]s + \mathbf{e}'$ and sets the challenger ciphertext as in Eq. (11). In Game 5, the challenger first picks $v_0 \xleftarrow{\$} R_q, v'_i \xleftarrow{\$} R_q, \mathbf{v}' = [v'_1|v'_2|v'_3] \in R^3_q, \mathbf{e}' \leftarrow \mathcal{D}^3_{R,\sigma_\mathsf{R}}$, sets $\mathbf{v} = \mathbf{v}' + \mathbf{e}'$. Then it sets the challenge ciphertext as

$$c_0 = v_0 + \lfloor \frac{q}{2} \rceil m, \quad \mathbf{c}_1 = \mathsf{ReRand}\left(\begin{bmatrix} 0\ 1\ 0\ \mathbf{0} \\ 1\ 0\ 0\ \mathbf{r}_1 \\ 0\ 0\ 1\ \mathbf{r}_2 \end{bmatrix}, \mathbf{v}, \sigma_\mathsf{R}, \frac{\sigma_1}{2\sigma_\mathsf{R}} \right). \tag{13}$$

v_0 is uniformly random and independent of $\mathbf{c}_1$, so it serves as a one-time pad that perfectly hides m. Thus the adversary's advantage in Game 5 is zero. We show that the distributions of Game 5 and Game 4 are indistinguishable provided the $\mathsf{RLWE}_{n,4,q,\chi}$ assumption.

Instance. $\mathcal{B}$ is given the RLWE instance $(u_i, v_i) \in R_q \times R_q$, for each $i \in [4]$. If u_2 is not invertible, then aborts. This is reasonable since the probability for a uniform element of R_q being invertible is non-negligible when $q = \Omega(n)$ [35]. We can assume without loss of generality that $v_i = v'_i + e_i$ for $e_i \leftarrow \mathcal{D}_{R,\sigma_\mathsf{R}}$. Then $\mathcal{B}$'s task is to distinguish whether $v'_i = u_i s$ for some $s \xleftarrow{\$} R_q$ or $v'_i \leftarrow R_q$.

Setup. To make up the master public key mpk, $\mathcal{B}$ first sets

$$u \coloneqq u_0, \quad t \coloneqq u_2, \quad h \coloneqq u_2^{-1} \cdot u_1, \quad z \coloneqq u_2^{-1} \cdot u_3, \quad v_0 \coloneqq v_0, \quad \mathbf{v} \coloneqq [v_1 | v_2 | v_3]$$

Then it picks $\mathbf{R}_{\mathsf{id}^*}$ and sets $\mathbf{w}$ as Game 1. Finally, it outputs $\mathsf{mpk} = (h, z, \mathbf{w}, u)$, which simulates the setup phase.

Phase 1 & Phase 2. When $\mathcal{A}$ makes the key extraction queries, $\mathcal{B}$ responds as in Game 2.

Challenge. When $\mathcal{A}$ makes the challenge query for the challenge identity id^* and a message m, $\mathcal{B}$ sets the challenge ciphertext as

$$c_0 = v_0 + \lfloor \frac{q}{2} \rceil m, \quad \mathbf{c}_1 = \mathsf{ReRand}\left(\begin{bmatrix} 0\ 1\ 0\ \mathbf{0} \\ 1\ 0\ 0\ \mathbf{r}_1 \\ 0\ 0\ 1\ \mathbf{r}_2 \end{bmatrix}, \mathbf{v}, \sigma_{\mathsf{R}}, \frac{\sigma_1}{2\sigma_{\mathsf{R}}} \right).$$

When the RLWE oracle is pseudorandom, i.e., $v_i = u_i s + e_i$ for some $s \in R_q$, the challenge ciphertext is distributed exactly as in Eq. (11). When the RLWE oracle is truly random, then the challenge ciphertext is distributed exactly as in Eq. (13).

Guess. When $\mathcal{A}$ receives the challenge ciphertext, it guesses if it is interacting with the Game 4 or Game 5 challenger. $\mathcal{B}$ outputs $\mathcal{A}$'s guess as the answer to the RLWE challenge it is trying to solve.

As a result, the advantage of $\mathcal{B}$ is the same as that of $\mathcal{A}$. By $\mathsf{RLWE}_{n,4,q,\chi}$ assumption, the advantage of $\mathcal{B}$ is negligible, and then the advantage of $\mathcal{A}$ in distinguishing Game 4 and Game 5 is negligible. This completes the proof.

6 Security Analysis and Implementation

In this section, we explain how to instantiate the various parameters for our IBE scheme, to optimize the efficiency, under the correctness and security constraints.

6.1 Security Analysis

In the absence of a thorough study on the asymptotic security of the DSPR assumption, which we leave for future work, we give a security analysis of our IBE scheme based on the existing cryptanalysis. At a high level, we follow the core SVP hardness methodology proposed by [3], which involves calling an SVP oracle in selected block-size β by BKZ algorithm [33]. To be more concrete, if an N-dimensional lattice Λ is known to have an unusually short vector $\mathbf{v}$ whose size is evidently smaller than Gaussian Heuristic $\sqrt{\frac{N}{2\pi e}} \cdot \det(\Lambda)^{1/N}$, it can be found by BKZ with block-size β satisfying

$$\sqrt{\beta/N} \cdot \|\mathbf{v}\| \leq \delta^{2\beta - N} \cdot \det(\Lambda)^{1/N},$$

where the root Hermite factor δ is given by $(\frac{\beta}{2\pi e}(\pi\beta)^{\frac{1}{\beta}})^{\frac{1}{2(\beta-1)}}$ [15]. In another case, for any N-dimensional lattice Λ, if one wants to find a vector $\mathbf{v}$ whose size is larger than the Gaussian Heuristic, the root Hermite factor δ is required by

$$\delta^N \leq \frac{\|\mathbf{v}\|}{\det(\Lambda)^{1/N}}.$$

Based on these facts, we hope to find the minimal β that allows breaking the underlying problem, thus inferring the classical bit-security $\lambda_C := 0.292\beta$ [4] and the quantum bit-security $\lambda_Q := 0.257\beta$ [13], respectively. The security levels implied by the following attacks are given in Tab. 2.

Master Key Recovery. One may try to recover msk from mpk, by finding an unusually short vector in the lattice Λ_{NTRU} with the short basis $\mathbf{T}$. For the lattice Λ_{NTRU}, a $2n$-dimensional lattice with determinant q^n, we choose the short vector to have a norm smaller than $1.17\sqrt{q}$, which is less than the expected norm $\sqrt{\frac{2n}{2\pi e}}\sqrt{q}$ of a shortest non-zero vector, thus it can be found by BKZ algorithm with block-size β satisfying

$$1.17\sqrt{\frac{\beta}{2n}} \leq \delta^{2\beta-2n}.$$

User Key Recovery. One may try to recover $\mathsf{sk}_{\mathsf{id}}$ from mpk, which involves finding any short vector $\mathbf{e}_{\mathsf{id}} \in R^{3+d}$ satisfying $[1|h|z|\mathbf{w} + H(\mathsf{id})\mathbf{g}] \cdot \mathbf{e}_{\mathsf{id}}^{\top} = t^{-1}u$. This can be done by finding a short vector in a $n(3+d)$-dimensional lattice with determinant q^n. For correct decryption, the target vector norm would be approximately $\sigma\sqrt{n(3+d)}$, which is larger than $\sqrt{\frac{n(3+d)}{2\pi e}}q^{1/(3+d)}$, then the root Hermite factor δ is required by

$$\delta^{n(3+d)} \leq \frac{\sigma\sqrt{n(3+d)}}{q^{1/(3+d)}}.$$

Remark 1. Recent works [20] have shown that when f, g are extremely small compared to q, it is easy to attack cryptographic schemes based on NTRU lattices. To the contrary, in our IBE scheme, we take f, g to be not too small while q is hardly large: a side-effect is that this makes our scheme impervious to the so-called "overstretched NTRU" attacks.

6.2 Implementation and Performance

Considering the parameter constraints in Sect. 5.1 and the above security analysis, we provide the concrete parameter sets in Tab. 2, achieving NIST level I, III, and V respectively.

Table 2. Different parameters sets for our IBE scheme.

Security level	δ	β	λ_C	λ_Q	n	d	$\lceil \log_2 q \rceil$	σ	σ_1
I	1.0035	482	141	124	512	3	39	2743284	279
III	1.0027	727	212	186	512-2*	3	40	5220211	277
V	1.0021	972	284	250	1024	3	42	11257610	403

$*$: stands for NTRU module lattices [16], where $\mathbf{h} = \mathbf{g} \cdot \mathbf{F}^{-1} \in R_q^2$ and $\mathbf{T_h} \in R^{3\times 3}$.

Comparison with Related Works. To the best of our knowledge, the first (proof-of-concept) implementation of IBE with practical parameters was instantiated on the NTRU lattice [18] (Random-Oracle Model), and its performance was later improved by several software optimizations in [29]. Compared to [29], our IBE scheme achieves a more reasonable level of security against quantum attacks without significant size growth. Moreover, the size increment is constrained within the range of $O(1)$, which would not continue to increase with higher security levels, as indicated in Tab. 3.

Table 3. Concrete sizes (KB) comparison between this paper and [29].

Scheme	Standard model	Level*	mpk	msk	$\mathsf{sk}_{\mathsf{id}}$	ct
[29]	×	I	3	6.25	2.125	6.125
Ours	✓	I	17.0625 (×7)†	5.5	8.25 (×4)	17.0625 (×3)
[29]	×	III	3.5	12.75	2.55	7.15
Ours	✓	III	20 (×7)‡	11.25	10.0625 (×4)	20 (×3)

$*$: stands for the NIST security level (level I: 128; level III: 192; level V: 256.)
†: approximately compare the size growth of the second and the first rows.
‡: approximately compare the size growth of the fourth and the third rows.

As for implementations on ideal lattices, in 2018, Bert et al. [6] mixed the IBE scheme [1] in the standard model on the Ring-SIS/LWE assumptions with the efficient trapdoor of Peikert and Micciancio [30] and provided an efficient implementation. It mainly aimed to demonstrate the time efficiency of the preimage sampling, ignoring the huge key size. Compared to [6], our IBE scheme achieves much better compactness without changing the security model. Further, our size reduction is on the order of $O(\log q)$, that is, the higher the security level and the larger the q, the more significant our size reduction will be, as shown in Tab. 4.

Table 4. Concrete sizes (KB) comparison between this paper and [6].

Scheme	Standard model	Level	mpk	msk	$\mathsf{sk}_{\mathsf{id}}$	ct
[6]	✓	I	600	67.5	320	600
Ours	✓	I	17.0625 ($\div$35)†	5.5	8.25 ($\div$19)	17.0625 ($\div$35)
[6]	✓	III	1007.5	93	256	1007.5
Ours	✓	III	20 ($\div$50)‡	11.25	10.0625 ($\div$25)	20 ($\div$50)

†: approximately compare the size reduction of the second and the first rows.
‡: approximately compare the size reduction of the fourth and the third rows.

Acknowledgments. This work was supported by National Natural Science Foundation of China (Grant No. 62202305), Young Elite Scientists Sponsorship Program by China Association for Science and Technology (YESS20220150), Shanghai Pujiang Program under Grant 22PJ1407700. We thank the anonymous reviewers of SAC 2024 for their careful examination of our work and their insightful comments and constructive suggestions.

References

1. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer (2010), https://doi.org/10.1007/978-3-642-13190-5_28
2. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: Miller, G.L. (ed.) STOC 1996. pp. 99–108. ACM (1996), https://doi.org/10.1145/237814.237838
3. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - A new hope. In: Holz, T., Savage, S. (eds.) USENIX 2016. pp. 327–343. USENIX Association (2016), https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim
4. Becker, A., Ducas, L., Gama, N., Laarhoven, T.: New directions in nearest neighbor searching with applications to lattice sieving. In: Krauthgamer, R. (ed.) SODA 2016. pp. 10–24. SIAM (2016), https://doi.org/10.1137/1.9781611974331.ch2
5. Bellare, M., Boldyreva, A., Palacio, A.: An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 171–188. Springer (2004), https://doi.org/10.1007/978-3-540-24676-3_11
6. Bert, P., Fouque, P., Roux-Langlois, A., Sabt, M.: Practical implementation of ring-sis/lwe based signature and IBE. In: Lange, T., Steinwandt, R. (eds.) PQCrypto 2018. LNCS, vol. 10786, pp. 271–291. Springer (2018), https://doi.org/10.1007/978-3-319-79063-3_13
7. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer (2004), https://doi.org/10.1007/978-3-540-24676-3_14
8. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer (2004), https://doi.org/10.1007/978-3-540-28628-8_27

9. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer (2011), https://doi.org/10.1007/978-3-642-25385-0_3
10. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer (2001), https://doi.org/10.1007/3-540-44647-8_13
11. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited (preliminary version). In: Vitter, J.S. (ed.) STOC 1998. pp. 209–218. ACM (1998), https://doi.org/10.1145/276698.276741
12. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer (2010), https://doi.org/10.1007/978-3-642-13190-5_27
13. Chailloux, A., Loyer, J.: Lattice sieving via quantum random walks. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021. LNCS, vol. 13093, pp. 63–91. Springer (2021), https://doi.org/10.1007/978-3-030-92068-5_3
14. Chen, Y., Genise, N., Mukherjee, P.: Approximate trapdoors for lattices and smaller hash-and-sign signatures. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11923, pp. 3–32. Springer (2019), https://doi.org/10.1007/978-3-030-34618-8_1
15. Chen, Y.: Réduction de réseau et sécurité concrete du chiffrement completement homomorphe. Ph.D. thesis, Paris 7 (2013)
16. Chuengsatiansup, C., Prest, T., Stehlé, D., Wallet, A., Xagawa, K.: Modfalcon: Compact signatures based on module-ntru lattices. In: Sun, H., Shieh, S., Gu, G., Ateniese, G. (eds.) ASIA CCS 2020. pp. 853–866. ACM (2020), https://doi.org/10.1145/3320269.3384758
17. Cocks, C.C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) IMA 2001. vol. 2260, pp. 360–363. Springer (2001), https://doi.org/10.1007/3-540-45325-3_32
18. Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 22–41. Springer (2014), https://doi.org/10.1007/978-3-662-45608-8_2
19. Ducas, L., Micciancio, D.: Improved short lattice signatures in the standard model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 335–352. Springer (2014), https://doi.org/10.1007/978-3-662-44371-2_19
20. Ducas, L., van Woerden, W.P.J.: NTRU fatigue: How stretched is overstretched? In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021. LNCS, vol. 13093, pp. 3–32. Springer (2021), https://doi.org/10.1007/978-3-030-92068-5_1
21. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer (2006), https://doi.org/10.1007/11761679_27
22. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Dwork, C. (ed.) STOC 2008. pp. 197–206. ACM (2008), https://doi.org/10.1145/1374376.1374407
23. Goldwasser, S., Kalai, Y.T.: On the (in)security of the fiat-shamir paradigm. In: FOCS 2003. pp. 102–113. IEEE Computer Society (2003), https://doi.org/10.1109/SFCS.2003.1238185
24. Izabachène, M., Prabel, L., Roux-Langlois, A.: Identity-based encryption from lattices using approximate trapdoors. In: Simpson, L., Baee, M.A.R. (eds.) ACISP 2023. LNCS, vol. 13915, pp. 270–290. Springer (2023), https://doi.org/10.1007/978-3-031-35486-1_13

25. Katsumata, S., Yamada, S.: Partitioning via non-linear polynomial functions: More compact ibes from ideal lattices and bilinear maps. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 682–712 (2016), https://doi.org/10.1007/978-3-662-53890-6_23
26. Katsumata, S., Yamada, S., Yamakawa, T.: Tighter security proofs for GPV-IBE in the quantum random oracle model. In: Peyrin, T., Galbraith, S.D. (eds.) ASIACRYPT 2018. LNCS, vol. 11273, pp. 253–282. Springer (2018), https://doi.org/10.1007/978-3-030-03329-3_9
27. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer (2010), https://doi.org/10.1007/978-3-642-13190-5_1
28. Maurer, U.M., Renner, R., Holenstein, C.: Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 21–39. Springer (2004), https://doi.org/10.1007/978-3-540-24638-1_2
29. McCarthy, S., Smyth, N., O'Sullivan, E.: A practical implementation of identity-based encryption over NTRU lattices. In: O'Neill, M. (ed.) IMACC 2017. LNCS, vol. 10655, pp. 227–246. Springer (2017), https://doi.org/10.1007/978-3-319-71045-7_12
30. Micciancio, D., Peikert, C.: Trapdoors for lattices: Simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer (2012), https://doi.org/10.1007/978-3-642-29011-4_41
31. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. In: FOCS 2004. pp. 372–381. IEEE Computer Society (2004), https://doi.org/10.1109/FOCS.2004.72
32. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) STOC 2005. pp. 84–93. ACM (2005), https://doi.org/10.1145/1060590.1060603
33. Schnorr, C., Euchner, M.: Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Math. Program. **66**, 181–199 (1994), https://doi.org/10.1007/BF01581144
34. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO '84. LNCS, vol. 196, pp. 47–53. Springer (1984), https://doi.org/10.1007/3-540-39568-7_5
35. Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 27–47. Springer (2011), https://doi.org/10.1007/978-3-642-20465-4_4
36. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer (2005), https://doi.org/10.1007/11426639_7
37. Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer (2009), https://doi.org/10.1007/978-3-642-03356-8_36
38. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 758–775. Springer (2012), https://doi.org/10.1007/978-3-642-32009-5_44