# Lattice-based IBE with equality test in standard model

Dung Hoang Duong[1], Huy Quoc Le[2], Partha Sarathi Roy[3], and Willy Susilo[1]

[1] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong
Northfields Avenue, Wollongong NSW 2522, Australia
{hduong,wsusilo}@uow.edu.au
[2] Graduate School of Mathematics, Kyushu University
744 Motooka, Nishi-ku, Fukuoka-shi, Fukuoka-ken 819-0395, Japan
q-le@math.kyushu-u.ac.jp
[3] Information Security Laboratory, KDDI Research, Inc.
2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan
pa-roy@kddi-research.jp

**Abstract.** Public key encryption with equality test (PKEET) allows the testing of equality of underlying messages of two ciphertexts. PKEET is a potential candidate for many practical applications like efficient data management on encrypted databases. Identity-based encryption scheme with equality test (IBEET), which was introduced by Ma (Information Science 2016), can simplify the certificate management of PKEET. Potential applicability of IBEET leads to intensive research from its first instantiation. Ma's IBEET and most of the constructions are proven secure in the random oracle model based on number-theoretic hardness assumptions which are vulnerable in the post-quantum era. Recently, Lee et al. (ePrint 2016) proposed a generic construction of IBEET schemes in the standard model and hence it is possible to yield the first instantiation of IBEET schemes based on lattices. Their method is to use a 3-level hierarchical identity-based encryption (HIBE) scheme together with a one-time signature scheme. In this paper, we propose, for the first time, a concrete construction of an IBEET scheme based on the hardness assumption of lattices in the standard model and compare the data sizes with the instantiation from Lee et al. (ePrint 2016). Further, we have modified our proposed IBEET to make it secure against *insider attack*.

## 1 Introduction

The concept of IBEET is the combination of PKEET and identity-based encryption (IBE). IBEET can simplify the certificate management of PKEET with all messages encrypted with the receiver's public identity. IBEET is a special kind of IBE featuring equality test between ciphertexts under different as well as the same identity. This property is very useful in various practical applications, such as keyword search on encrypted data, encrypted data partitioning for efficient encrypted data management, personal health record system and spam filtering in encrypted email systems. Due to its numerous practical applications, there have been elegant research outcomes in this direction with the appearance of improved schemes or ones with additional functionalities [10,8,15]. However, they are all proven secure in the random oracle model which does not exist in reality. Therefore it is necessary to construct such a scheme in the standard model. Moreover, all aforementioned existing schemes base their security on some number-theoretic hardness assumptions which will be efficiently solved in the quantum era [13]. Up to the present, there is only one IBEET scheme secure in the standard model, which was generically constructed by Lee et al. [7]. Their method is to use a 3-level hierarchical identity-based encryption (HIBE) scheme together with a one-time signature scheme. This is the first one with the possibility of yielding a post-quantum instantiation based on lattices, since lattice-based cryptography is the only one among other post-quantum areas up to present offers HIBE primitives, e.g., [1] . Hence it remains a question of either yielding an efficient instantiation or directly constructing an IBEET based on lattices.

On the other hand, supporting equality tests makes the security of IBEET schemes weaken. If the adversary can have a trapdoor for the equality test on the target ciphertext, he can generate a ciphertext of any message by himself and perform equality tests between the target ciphertext and the ciphertext generated by himself. We call this type of attacks as an *insider attack* [15]. IBEET secure against insider attack is proposed by Wu et al. [15]. There is a security flaw which is fixed by Lee et al. [9]. However, the construction is secure in the random oracle model based on number-theoretic hardness assumption. So, it is required to consider the secure construction in standard model based on the hardness assumptions which will remain secure in post-quantum era.

***Our contribution:*** In this paper, our contribution is twofold:

- According to the best of our knowledge, we propose the first concrete construction of an addaptive secure IBEET scheme secure in the standard model based on the hardness assumption of lattices. From Table 1, it is evident that the proposed construction outperformed the instantiation from [7].

**Table 1.** Comparison of Proposed IBEET with instantiation from [7].

| Scheme | Ciphertext | Public Key | Master Secret Key | Secret Key |
|---|---|---|---|---|
| Proposed | $2t + 4m$ | $(l + 3)mn + nt$ | $2m^2$ | $4mt$ |
| Instantiation* from [7] | $8m + 2t + 2mt$ | $(l + 3)mn + nt$ | $2m^2$ | $2mt$ |

* see Appendix A; ** Data sizes are in number of field elements. In case of [7], we do not count the part of ciphertex which is possible to obtain from the public key.

- We have modified the proposed IBEET to make it secure against insider attack. This is also secure in the standard model based on the hardness assumption of lattices, whereas the previous constructions are secure in the random oracle model based on the number-theoretic hardness assumptions.

Our ideas come from the use of the full lattice-based IBE in the standard model by Agrawal et al. [1] and a recent technique by Duong et al. [6] in directly constructing a PKEET based on lattices in the standard model.

**Remark 1.** *Our proposed schemes achieve only IND-CPA security (defined in Section 2), which can be modified to achieve IND-CCA2 security by using the HIBE scheme in [1] through the BCHK's transformation [4]. Hence in definition of security model in Section 2, we provide only the definition of CPA-security models, in which the adversary cannot query the decryption oracle.*

## 2 Preliminaries

### 2.1 Identity-based encryption with equality test (IBEET)

**Definition 2** (IBEET)**.** *An identity-based encryption with equality test (IBEET) consists of the following polynomial-time algorithms:*

- $\mathsf{Setup}(\lambda)$*: On input a security parameter* $\lambda$ *and set of parameters, it outputs a public parameter* $\mathsf{PP}$ *and a master secret key* $\mathsf{MSK}$*. Note that* $\mathsf{PP}$ *consists of the information of the message space* $\mathcal{M}$ *and we assume that all other algorithms take* $\mathsf{PP}$ *as an input implicitly without stated.*
- $\mathsf{Extract}(\mathsf{PP}, \mathsf{MSK}, \mathsf{ID})$*: On input* $\mathsf{PP}, \mathsf{MSK}$ *and an identity* $\mathsf{ID}$*, it outputs a user* $\mathsf{ID}$*'s secret key* $\mathsf{SK}_{\mathsf{ID}}$*.*
- $\mathsf{Enc}(\mathsf{PP}, \mathsf{ID}, \mathbf{m})$*: On input* $\mathsf{PP}$*, an identity* $\mathsf{ID}$ *and a message* $\mathbf{m}$*, it outputs a ciphertext* $\mathsf{CT}$*.*
- $\mathsf{Dec}(\mathsf{PP}, \mathsf{SK}_{\mathsf{ID}}, \mathsf{CT})$*: On input* $\mathsf{PP}$*, a user* $\mathsf{ID}$*'s secret key* $\mathsf{SK}$ *and a ciphertext* $\mathsf{CT}$*, it outputs a message* $\mathbf{m}'$ *or* $\perp$*.*
- $\mathsf{Td}(\mathsf{SK}_{\mathsf{ID}})$*: On input the secret key* $\mathsf{SK}_{\mathsf{ID}}$ *for the user* $\mathsf{ID}$*, it outputs a trapdoor* $\mathsf{td}_{\mathsf{ID}}$*.*
- $\mathsf{Test}(\mathsf{td}_{\mathsf{ID}_i}, \mathsf{td}_{\mathsf{ID}_j}, \mathsf{CT}_{\mathsf{ID}_i}, \mathsf{CT}_{\mathsf{ID}_j})$*: On input two trapdoors* $\mathsf{td}_{\mathsf{ID}_i}, \mathsf{td}_{\mathsf{ID}_j}$ *and two ciphertexts* $\mathsf{CT}_{\mathsf{ID}_i}, \mathsf{CT}_{\mathsf{ID}_j}$ *for users* $\mathsf{ID}_i$ *and* $\mathsf{ID}_j$ *respectively, it outputs* $1$ *or* $0$*.*

**Correctness.** We say that an IBEET scheme is *correct* if the following conditions hold:

**(1)** For any security parameter $\lambda$, any user $\mathsf{ID}_i$ and any message $\mathbf{m}$, it holds that

$$\Pr\left[\mathsf{Dec}(\mathsf{PP}, \mathsf{SK}_{\mathsf{ID}}, \mathsf{CT}_{\mathsf{ID}}) = \mathbf{m} \,\middle|\, \begin{array}{c} \mathsf{SK}_{\mathsf{ID}} \leftarrow \mathsf{Extract}(\mathsf{PP}, \mathsf{MSK}, \mathsf{ID}) \\ \mathsf{CT}_{\mathsf{ID}} \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{ID}, \mathbf{m}) \end{array}\right] = 1.$$

**(2)** For any security parameter $\lambda$, any users $\mathsf{ID}_i$, $\mathsf{ID}_j$ and any messages $\mathbf{m}_i, \mathbf{m}_j$, it holds that:

$$\Pr\left[\mathsf{Test}\begin{pmatrix}\mathsf{td}_{\mathsf{ID}_i}\\ \mathsf{td}_{\mathsf{ID}_j}\\ \mathsf{CT}_{\mathsf{ID}_i}\\ \mathsf{CT}_{\mathsf{ID}_j}\end{pmatrix}=1\ \middle|\ \begin{array}{l}\mathsf{SK}_{\mathsf{ID}_i}\leftarrow\mathsf{Extract}(\mathsf{PP},\mathsf{MSK},\mathsf{ID}_i)\\ \mathsf{CT}_{\mathsf{ID}_i}\leftarrow\mathsf{Enc}(\mathsf{PP},\mathsf{ID}_i,\mathbf{m}_i)\\ \mathsf{td}_{\mathsf{ID}_i}\leftarrow\mathsf{Td}(\mathsf{SK}_{\mathsf{ID}_i})\\ \mathsf{SK}_{\mathsf{ID}_j}\leftarrow\mathsf{Extract}(\mathsf{PP},\mathsf{MSK},\mathsf{ID}_j)\\ \mathsf{CT}_{\mathsf{ID}_j}\leftarrow\mathsf{Enc}(\mathsf{PP},\mathsf{ID}_j,\mathbf{m}_j)\\ \mathsf{td}_{\mathsf{ID}_j}\leftarrow\mathsf{Td}(\mathsf{SK}_{\mathsf{ID}_j})\end{array}\right]$$

is 1 if $\mathbf{m}_i = \mathbf{m}_j$ and is negligible in $\lambda$ for any ciphertexts $\mathsf{CT}_i$, $\mathsf{CT}_j$ such that $\mathsf{Dec}(\mathsf{SK}_i, \mathsf{CT}_i) \neq \mathsf{Dec}(\mathsf{SK}_j, \mathsf{CT}_j)$, regardless of whether $i = j$.

**Security model of IBEET.** For the security model of IBEET, we consider two types of adversaries:

- Type-I adversary: for this type, the adversary can request to issue a trapdoor for the target identity and thus can perform equality tests on the challenge ciphertext. The aim of this type of adversaries is to reveal the message in the challenge ciphertext.
- Type-II adversary: for this type, the adversary cannot request to issue a trapdoor for the target identity and thus cannot perform equality tests on the challenge ciphertext. The aim of this type of adversaries is to distinguish which message is in the challenge ciphertext between two candidates.

The security model of a IBEET scheme against two types of adversaries above is described in the following.

**OW-ID-CPA security against Type-I adversaries.** We illustrate the game between a challenger $\mathcal{C}$ and a Type-I adversary $\mathcal{A}$ who can have a trapdoor for all ciphertexts of the target identity, say $\mathsf{ID}^*$, that he wants to attack, as follows:

1. **Setup:** The challenger $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate the pair $(\mathsf{PP}, \mathsf{MSK})$, and sends the public parameter $\mathsf{PP}$ to $\mathcal{A}$.
2. **Phase 1:** The adversary $\mathcal{A}$ may make queries polynomially many times adaptively and in any order to the following oracles:
   – $\mathcal{O}^{\mathsf{Ext}}$: an oracle that on input an identity $\mathsf{ID}$ (different from $\mathsf{ID}^*$), returns the $\mathsf{ID}$'s secret key $\mathsf{SK}_{\mathsf{ID}}$.
   – $\mathcal{O}^{\mathsf{Td}}$: an oracle that on input an identity $\mathsf{ID}$, return $\mathsf{td}_{\mathsf{ID}}$ by running $\mathsf{td}_{\mathsf{ID}} \leftarrow \mathsf{Td}(\mathsf{SK}_{\mathsf{ID}})$ using the secret key $\mathsf{SK}_{\mathsf{ID}}$ of the identity $\mathsf{ID}$.
3. **Challenge:** $\mathcal{C}$ chooses a random message $\mathbf{m}$ in the message space and run $\mathsf{CT}^*_{\mathsf{ID}^*} \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{ID}^*, \mathbf{m})$, and sends $\mathsf{CT}^*_{\mathsf{ID}^*}$ to $\mathcal{A}$.
4. **Phase 2:** $\mathcal{A}$ can query as in Phase 1 with the constraint that the identity $\mathsf{ID}^*$ cannot be queried to the key generation oracle $\mathcal{O}^{\mathsf{Ext}}$.
5. **Guess:** $\mathcal{A}$ output $\mathbf{m}'$.

The adversary $\mathcal{A}$ wins the above game if $\mathbf{m} = \mathbf{m}'$ and the success probability of $\mathcal{A}$ is defined as

$$\mathsf{Adv}^{\mathsf{OW\text{-}ID\text{-}CPA}}_{\mathcal{A},\mathrm{IBEET}}(\lambda) := \Pr[\mathbf{m} = \mathbf{m}'].$$

**Remark 3.** *If the message space is polynomial in the security parameter or the min-entropy of the message distribution is much lower than the security parameter then a Type-I adversary $\mathcal{A}$ with a trapdoor for the challenge ciphertext can reveal the message in polynomial-time or small exponential time in the security parameter, by performing the equality tests with the challenge ciphertext and all other ciphertexts of all messages generated by himself. Hence to prevent this attack, we assume that the size of the message space $\mathcal{M}$ is exponential in the security parameter and the min-entropy of the message distribution is sufficiently higher than the security parameter.*

**IND-ID-CPA security against Type-II adversaries.** We present the game between a challenger $\mathcal{C}$ and a Type-II adversary $\mathcal{A}$ who cannot have a trapdoor for all ciphertexts of the target identity $\mathsf{ID}^*$ as follows:

1. **Setup:** The challenger $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate $(\mathsf{PP}, \mathsf{MSK})$ and gives the public parameter $\mathsf{PP}$ to $\mathcal{A}$.
2. **Phase 1:** The adversary $\mathcal{A}$ may make queries polynomially many times adaptively and in any order to the following oracles:
   - $\mathcal{O}^{\mathsf{Ext}}$: an oracle that on input an identity $\mathsf{ID}$ (different from $\mathsf{ID}^*$), returns the $\mathsf{ID}$'s secret key $\mathsf{SK}_{\mathsf{ID}}$.
   - $\mathcal{O}^{\mathsf{Td}}$: an oracle that on input an identity $\mathsf{ID}$, return $\mathsf{td}_{\mathsf{ID}}$ by running $\mathsf{td}_{\mathsf{ID}} \leftarrow \mathsf{Td}(\mathsf{SK}_{\mathsf{ID}})$ using the secret key $\mathsf{SK}_{\mathsf{ID}}$ of the identity $\mathsf{ID}$.
3. **Challenge:** $\mathcal{A}$ selects a target user $\mathsf{ID}^*$, which was never queried to the $\mathcal{O}^{\mathsf{Ext}}$ and $\mathcal{O}^{\mathsf{Td}}$ oracles in Phase 1, and two messages $\mathbf{m}_0$ $\mathbf{m}_1$ of same length and pass to $\mathcal{C}$, who then selects a random bit $b \in \{0,1\}$, runs $\mathsf{CT}^*_{\mathsf{ID}^*,b} \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathsf{ID}^*, \mathbf{m}_b)$ and sends $\mathsf{CT}^*_{\mathsf{ID}^*,b}$ to $\mathcal{A}$.
4. **Phase 2:** $\mathcal{A}$ can query as in Phase 1 with the constraint that the target identity $\mathsf{ID}^*$ cannot be queried to the secret key extraction oracle $\mathcal{O}^{\mathsf{Ext}}$ and the trapdoor generation oracle $\mathcal{O}^{\mathsf{Td}}$.
5. **Guess:** $\mathcal{A}$ output $b'$.

The adversary $\mathcal{A}$ wins the above game if $b = b'$ and the advantage of $\mathcal{A}$ is defined as

$$\mathsf{Adv}^{\mathsf{IND\text{-}ID\text{-}CPA}}_{\mathcal{A},\mathrm{IBEET}} := \left| \Pr[b = b'] - \frac{1}{2} \right| .$$

### 2.2 IBEET against insider attack

**Definition 4.** *An IBEET against insider attack consists of the following polynomial-time algorithms:*

- $\mathsf{Setup}(\lambda)$*: On input a security parameter $\lambda$, it outputs a public parameter* $\mathsf{PP}$*, a master secret key* $\mathsf{MSK}$ *and a master token key* $\mathsf{MTK}$*.*
- $\mathsf{Extract}(\mathsf{ID}, \mathsf{MSK}, \mathsf{MTK})$*: On input an identity* $\mathsf{ID}$*, the master secret key* $\mathsf{MSK}$ *and a master token key* $\mathsf{MTK}$*, it outputs the secret key* $\mathsf{SK}_{\mathsf{ID}}$ *and token* $\mathsf{tok}_{\mathsf{ID}}$ *for the identity* $\mathsf{ID}$*.*

  *It is assumed that* $\mathsf{SK}_{\mathsf{ID}}$ *and* $\mathsf{tok}_{\mathsf{ID}}$ *are delivered to the user of identity* $\mathsf{ID}$ *and the token* $\mathsf{tok}_{\mathsf{ID}}$ *is delivered to all group users via secure channel.*

- $\mathsf{Enc}(\mathsf{PP}, \mathbf{m}, \mathsf{ID}, \mathsf{tok}_{\mathsf{ID}})$: *On input* $\mathsf{PP}$, *an identity* $\mathsf{ID}$ *with its token* $\mathsf{tok}_{\mathsf{ID}}$ *and a message* $\mathbf{m}$, *it outputs a ciphertext* $\mathsf{CT}$.
- $\mathsf{Dec}(\mathsf{CT}, \mathsf{SK}_{\mathsf{ID}}, \mathsf{tok}_{\mathsf{ID}})$: *On input a ciphertext* $\mathsf{CT}$, *the secret key* $\mathsf{SK}_{\mathsf{ID}}$ *and token* $\mathsf{tok}_{\mathsf{ID}}$ *of the identity* $\mathsf{ID}$, *it outputs a message* $\mathbf{m}'$ *or* $\perp$.
- $\mathsf{Test}(\mathsf{CT}_i, \mathsf{CT}_j)$: *On input two ciphertexts* $\mathsf{CT}_i$ *and* $\mathsf{CT}_j$, *it outputs* $1$ *or* $0$.

**Correctness.** We say that the above IBEET is correct if the following holds:

**(1)** For any security parameter $\lambda$, identity $\mathsf{ID}$ and message $\mathbf{m}$, it holds that

$$\Pr[\mathbf{m} \leftarrow \mathsf{Dec}(\mathsf{CT}, \mathsf{SK}_{\mathsf{ID}}, \mathsf{tok}_{\mathsf{ID}})] = 1$$

where $(\mathsf{PP}, \mathsf{MSK}, \mathsf{MTK}) \leftarrow \mathsf{Setup}(\lambda)$, $(\mathsf{SK}_{\mathsf{ID}}, \mathsf{tok}_{\mathsf{ID}}) \leftarrow \mathsf{Extract}(\mathsf{ID}, \mathsf{MSK}, \mathsf{MTK})$ and $\mathsf{CT} \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathbf{m}, \mathsf{ID}, \mathsf{tok}_{\mathsf{ID}})$.

**(2)** For any security parameter $\lambda$, identities $\mathsf{ID}_i, \mathsf{ID}_j$ and messages $\mathbf{m}_i, \mathbf{m}_j$, it holds that

$$\Pr\left[\mathsf{Test}\left(\mathsf{CT}_i, \mathsf{CT}_j\right) = 1 \;\middle|\; \begin{array}{l} (\mathsf{PP}, \mathsf{MSK}, \mathsf{MTK}) \leftarrow \mathsf{Setup}(\lambda) \\ (\mathsf{SK}_{\mathsf{ID}_i}, \mathsf{tok}_{\mathsf{ID}_i}) \leftarrow \mathsf{Extract}(\mathsf{ID}_i, \mathsf{MSK}, \mathsf{MTK}) \\ (\mathsf{SK}_{\mathsf{ID}_j}, \mathsf{tok}_{\mathsf{ID}_j}) \leftarrow \mathsf{Extract}(\mathsf{ID}_j, \mathsf{MSK}, \mathsf{MTK}) \\ \mathsf{CT}_i \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathbf{m}_i, \mathsf{ID}_i, \mathsf{tok}_{\mathsf{ID}_i}) \\ \mathsf{CT}_j \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathbf{m}_j, \mathsf{ID}_j, \mathsf{tok}_{\mathsf{ID}_j}) \end{array}\right]$$

is 1 if $\mathbf{m}_i = \mathbf{m}_j$ and negligible in the security parameter $\lambda$ otherwise.

**Security model.** The security model of IBEET against insider attack [15] is slightly weaker than the formal security model of traditional IBE. In such a scheme, two messages $\mathbf{m}_0$ and $\mathbf{m}_1$ submitted by the adversary to the challenger should not be queried to the encryption oracle before and after the challenge phase. We call this security model the weak indistinguishability under adaptive identity and chosen message attacks ($\mathsf{wIND\text{-}ID\text{-}CPA}$). In particular, we present the game between the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ as the following.

1. **Setup:** The challenger $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate $(\mathsf{PP}, \mathsf{MSK}, \mathsf{MTK})$ and gives the public parameter $\mathsf{PP}$ to $\mathcal{A}$.
2. **Phase 1:** The adversary $\mathcal{A}$ may make queries polynomially many times adaptively and in any order to the following oracles:
   - $\mathcal{O}^{\mathsf{Ext}}$: an oracle that on input an identity $\mathsf{ID}$, returns the $\mathsf{ID}$'s secret key $\mathsf{SK}_{\mathsf{ID}}$, where $(\mathsf{SK}_{\mathsf{ID}}, \mathsf{tok}_{\mathsf{ID}}) \leftarrow \mathsf{Extract}(\mathsf{ID}, \mathsf{MSK}, \mathsf{MTK})$.
   - $\mathcal{O}^{\mathsf{Enc}}$: an oracle that on input a pair of an identity $\mathsf{ID}$ and a message $\mathbf{m}$, returns the output of $\mathsf{Enc}(\mathsf{PP}, \mathbf{m}, \mathsf{ID}, \mathsf{tok}_{\mathsf{ID}})$.
3. **Challenge:** $\mathcal{A}$ submits a target identity $\mathsf{ID}^*$ and two messages $\mathbf{m}_0$, $\mathbf{m}_1$ of same length to $\mathcal{C}$, where $\mathsf{ID}^*$ was never queried to $\mathcal{O}^{\mathsf{Ext}}$ and $\mathbf{m}_0$, $\mathbf{m}_1$ were never queried to $\mathcal{O}^{\mathsf{Enc}}$ in Phase 1. Then $\mathcal{C}$ picks a random bit $b \in \{0, 1\}$, runs $\mathsf{CT}^*_{\mathsf{ID}^*,b} \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathbf{m}_b, \mathsf{ID}^*, \mathsf{tok}_{\mathsf{ID}^*})$, and sends $\mathsf{CT}^*_{\mathsf{ID}^*,b}$ to $\mathcal{A}$.
4. **Phase 2:** $\mathcal{A}$ can query as in Phase 1 with the following constraints:
   - The target identity $\mathsf{ID}^*$ cannot be queried to $\mathcal{O}^{\mathsf{Ext}}$;
   - The submitted messages $\mathbf{m}_0$, $\mathbf{m}_1$ cannot be queried to $\mathcal{O}^{\mathsf{Enc}}$;

5. **Guess:** $\mathcal{A}$ outputs a bit $b'$.

The adversary $\mathcal{A}$ wins the above game if $b = b'$ and the advantage of $\mathcal{A}$ is defined as

$$\mathsf{Adv}^{\mathsf{wIND\text{-}ID\text{-}CPA}}_{\mathcal{A},\mathrm{IBEET}} := \left|\Pr[b = b'] - \frac{1}{2}\right|.$$

### 2.3 Lattices

Throughout the paper, we will mainly focus on integer lattices, which are discrete subgroups of $\mathbb{Z}^m$. Specially, a lattice $\Lambda$ in $\mathbb{Z}^m$ with basis $B = [\mathbf{b}_1, \cdots, \mathbf{b}_n] \in \mathbb{Z}^{m\times n}$, where each $\mathbf{b}_i$ is written in column form, is defined as

$$\Lambda := \left\{ \sum_{i=1}^{n} \mathbf{b}_i x_i | x_i \in \mathbb{Z}\ \forall i = 1, \cdots, n \right\} \subseteq \mathbb{Z}^m.$$

We call $n$ the rank of $\Lambda$ and if $n = m$ we say that $\Lambda$ is a full rank lattice. In this paper, we mainly consider full rank lattices containing $q\mathbb{Z}^m$, called $q$-ary lattices, defined as the following, for a given matrix $A \in \mathbb{Z}^{n\times m}$ and $\mathbf{u} \in \mathbb{Z}_q^n$

$$\begin{aligned}
\Lambda_q(A) &:= \left\{\mathbf{e} \in \mathbb{Z}^m \text{ s.t. } \exists \mathbf{s} \in \mathrm{\mathbb{Z}_q^n} \text{ where } \mathrm{A^T}\mathbf{s} = \mathbf{e} \mod \mathrm{q}\right\} \\
\Lambda_q^{\perp}(A) &:= \{\mathbf{e} \in \mathbb{Z}^m \text{ s.t. } \mathrm{A}\mathbf{e} = 0 \mod \mathrm{q}\} \\
\Lambda_q^{\mathbf{u}}(A) &:= \{\mathbf{e} \in \mathbb{Z}^m \text{ s.t. } \mathrm{A}\mathbf{e} = \mathbf{u} \mod \mathrm{q}\}
\end{aligned}$$

Note that if $\mathbf{t} \in \Lambda_q^{\mathbf{u}}(A)$ then $\Lambda_q^{\mathbf{u}}(A) = \Lambda_q^{\perp}(A) + \mathbf{t}$.

Let $S = \{\mathbf{s}_1, \cdots, \mathbf{s}_k\}$ be a set of vectors in $\mathbb{R}^m$. We denote by $\|S\| := \max_i \|\mathbf{s}_i\|$ for $i = 1, \cdots, k$, the maximum $l_2$ length of the vectors in $S$. We also denote $\tilde{S} := \{\tilde{\mathbf{s}}_1, \cdots, \tilde{\mathbf{s}}_k\}$ the Gram-Schmidt orthogonalization of the vectors $\mathbf{s}_1, \cdots, \mathbf{s}_k$ in that order. We refer to $\|\tilde{S}\|$ the Gram-Schmidt norm of $S$.

Ajtai [2] first proposed how to sample a uniform matrix $A \in \mathbb{Z}_q^{n\times m}$ with an associated basis $S_A$ of $\Lambda_q^{\perp}(A)$ with low Gram-Schmidt norm. It is improved later by Alwen and Peikert [3] in the following Theorem.

**Theorem 1.** *Let $q \geq 3$ be odd and $m := \lceil 6n \log q \rceil$. There is a probabilistic polynomial-time algorithm $\mathsf{TrapGen}(q, n)$ that outputs a pair $(A \in \mathbb{Z}_q^{n\times m}, S \in \mathbb{Z}^{m\times m})$ such that $A$ is statistically close to a uniform matrix in $\mathbb{Z}_q^{n\times m}$ and $S$ is a basis for $\Lambda_q^{\perp}(A)$ satisfying*

$$\|\tilde{S}\| \leq O(\sqrt{n \log q}) \quad \text{and} \quad \|S\| \leq O(n \log q)$$

*with all but negligible probability in $n$.*

**Definition 1 (Gaussian distribution).** *Let $\Lambda \subseteq \mathbb{Z}^m$ be a lattice. For a vector $\mathbf{c} \in \mathbb{R}^m$ and a positive parameter $\sigma \in \mathbb{R}$, define:*

$$\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp\left(\pi \frac{\|\mathbf{x} - \mathbf{c}\|^2}{\sigma^2}\right) \quad \text{and} \quad \rho_{\sigma,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in\Lambda} \rho_{\sigma,\mathbf{c}}(\mathbf{x}).$$

*The discrete Gaussian distribution over $\Lambda$ with center $\mathbf{c}$ and parameter $\sigma$ is*

$$\forall \mathbf{y} \in \Lambda \quad , \quad \mathcal{D}_{\Lambda,\sigma,\mathbf{c}}(\mathbf{y}) = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{y})}{\rho_{\sigma,\mathbf{c}}(\Lambda)}.$$

For convenience, we will denote by $\rho_\sigma$ and $\mathcal{D}_{\Lambda.\sigma}$ for $\rho_{\mathbf{0},\sigma}$ and $\mathcal{D}_{\Lambda,\sigma,\mathbf{0}}$ respectively. When $\sigma = 1$ we will write $\rho$ instead of $\rho_1$. We recall below in Theorem 2 some useful results. The first one comes from [11, Lemma 4.4] . The second one is from [5] and formulated in [1, Theorem 17] and the last one is from [1, Theorem 19].

**Theorem 2.** *Let $q > 2$ and let $A, B$ be a matrix in $\mathbb{Z}_q^{n\times m}$ with $m > n$ and $B$ is rank $n$. Let $T_A, T_B$ be a basis for $\Lambda_q^\perp(A)$ and $\Lambda_q^\perp(B)$ respectively. Then for $c \in \mathbb{R}^m$ and $U \in \mathbb{Z}_q^{n\times t}$:*

1. *Let $M$ be a matrix in $\mathbb{Z}_q^{n\times m_1}$ and $\sigma \geq \|\widetilde{T_A}\|\omega(\sqrt{\log(m+m_1)})$. Then there exists a PPT algorithm $\mathsf{SampleLeft}(A, M, T_A, U, \sigma)$ that outputs a vector $\mathbf{e} \in \mathbb{Z}^{m+m_1}$ distributed statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(F_1),\sigma}$ where $F_1 := (A \mid M)$. In particular $\mathbf{e} \in \Lambda_q^U(F_1)$, i.e., $F_1 \cdot \mathbf{e} = U \mod q$.*
2. *Let $R$ be a matrix in $\mathbb{Z}^{k\times m}$ and let $s_R := \sup_{\|\mathbf{x}\|=1} \|R\mathbf{x}\|$. Let $F_2 := (A \mid AR+B)$. Then for $\sigma \geq \|\widetilde{T_B}\| s_R \omega(\sqrt{\log m})$, there exists a PPT algorithm $\mathsf{SampleRight}(A, B, R, T_B, U, \sigma)$ that outputs a vector $\mathbf{e} \in \mathbb{Z}^{m+k}$ distributed statistically close to $\mathcal{D}_{\Lambda_q^U(F_2),\sigma}$. In particular $\mathbf{e} \in \Lambda_q^{\mathbf{u}}(F_2)$, i.e., $F_2 \cdot \mathbf{e} = U$ mod $q$.*
   *Note that when $R$ is a random matrix in $\{-1,1\}^{m\times m}$ then $s_R < O(\sqrt{m})$ with overwhelming probability (cf. [1, Lemma 15]).*

The security of our construction reduces to the LWE (Learning With Errors) problem introduced by Regev [12].

**Definition 2 (LWE problem).** *Consider publicly a prime $q$, a positive integer $n$, and a distribution $\chi$ over $\mathbb{Z}_q$. An $(\mathbb{Z}_q, n, \chi)$-LWE problem instance consists of access to an unspecified challenge oracle $\mathcal{O}$, being either a noisy pseudorandom sampler $\mathcal{O}_{\mathbf{s}}$ associated with a secret $\mathbf{s} \in \mathbb{Z}_q^n$, or a truly random sampler $\mathcal{O}_\$$ who behaviors are as follows:*

**$\mathcal{O}_{\mathbf{s}}$:** *samples of the form $(\mathbf{u}_i, v_i) = (\mathbf{u}_i, \mathbf{u}_i^T\mathbf{s} + x_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ where $\mathbf{s} \in \mathbb{Z}_q^n$ is a uniform secret key, $\mathbf{u}_i \in \mathbb{Z}_q^n$ is uniform and $x_i \in \mathbb{Z}_q$ is a noise withdrawn from $\chi$.*

**$\mathcal{O}_\$$:** *samples are uniform pairs in $\mathbb{Z}_q^n \times \mathbb{Z}_q$.*

*The $(\mathbb{Z}_q, n, \chi)$-LWE problem allows responds queries to the challenge oracle $\mathcal{O}$. We say that an algorithm $\mathcal{A}$ decides the $(\mathbb{Z}_q, n, \chi)$-LWE problem if*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LWE}} := \left|\Pr[\mathcal{A}^{\mathcal{O}_{\mathbf{s}}} = 1] - \Pr[\mathcal{A}^{\mathcal{O}_\$} = 1]\right|$$

*is non-negligible for a random $\mathbf{s} \in \mathbb{Z}_q^n$.*

Regev [12] showed that (see Theorem 3 below) when $\chi$ is the distribution $\overline{\Psi}_\alpha$ of the random variable $\lfloor qX \rceil \mod q$ where $\alpha \in (0,1)$ and $X$ is a normal random variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$ then the LWE problem is hard.

**Theorem 3.** *If there exists an efficient, possibly quantum, algorithm for deciding the $(\mathbb{Z}_q, n, \overline{\Psi}_\alpha)$-LWE problem for $q > 2\sqrt{n}/\alpha$ then there is an efficient quantum algorithm for approximating the SIVP and GapSVP problems, to within $\tilde{\mathcal{O}}(n/\alpha)$ factors in the $l_2$ norm, in the worst case.*

Hence if we assume the hardness of approximating the SIVP and GapSVP problems in lattices of dimension $n$ to within polynomial (in $n$) factors, then it follows from Theorem 3 that deciding the LWE problem is hard when $n/\alpha$ is a polynomial in $n$.

## 3 Proposed Construction: IBEET

### 3.1 Construction

**Setup($\lambda$)** : On input a security parameter $\lambda$, set the parameters $q, n, m, \sigma, \alpha$ as in section 3.2

1. Use $\mathsf{TrapGen}(q, n)$ to generate uniformly random $n \times m$-matrices $A, A' \in \mathbb{Z}_q^{n\times m}$ together with trapdoors $T_A$ and $T_{A'}$ respectively.
2. Select $l+1$ uniformly random $n \times m$ matrices $A_1, \cdots, A_l, B \in \mathbb{Z}_q^{n\times m}$.
3. Select a uniformly random matrix $U \in \mathbb{Z}_q^{n\times t}$.
4. $H : \{0,1\}^* \to \{0,1\}^t$ is a hash function.
5. $H' : \{0,1\}^* \to \{0,1\}^l$ is a hash function.
6. Output the public key and the secret key

$$\mathsf{PK} = (A, A', A_1, \cdots, A_l, B, U) \quad , \quad \mathsf{MSK} = (T_A, T_{A'}).$$

**Extract($\mathsf{PP}, \mathsf{MSK}, \mathsf{ID}$)** : On input the public parameter $\mathsf{PP}$, a master secret key $\mathsf{MSK}$ and an identity $\mathsf{ID} = (b_1, \cdots, b_l) \in \{-1,1\}^l$:

1. Let $A_{\mathsf{ID}} = B + \sum_{i+1}^{l} b_i A_i \in \mathbb{Z}_q^{n\times m}$.
2. Sample $E_{\mathsf{ID}}, E'_{\mathsf{ID}} \in \mathbb{Z}_q^{2m\times t}$ as

$$E_{\mathsf{ID}} \leftarrow \mathsf{SampleLeft}(A, A_{\mathsf{ID}}, T_A, U, \sigma) \quad , \quad E'_{\mathsf{ID}} \leftarrow \mathsf{SampleLeft}(A', A_{\mathsf{ID}}, T_{A'}, U, \sigma).$$

3. Output $\mathsf{SK}_{\mathsf{ID}} := (E_{\mathsf{ID}}, E'_{\mathsf{ID}})$.

Let $F_{\mathsf{ID}} = (A|A_{\mathsf{ID}}), F'_{\mathsf{ID}} = (A'|A_{\mathsf{ID}}) \in \mathbb{Z}_q$ then $F_{\mathsf{ID}} \cdot E_{\mathsf{ID}} = U, F'_{\mathsf{ID}} \cdot E'_{\mathsf{ID}} = U$ in $\mathbb{Z}_q$ and $E_{\mathsf{ID}}, E'_{\mathsf{ID}}$ are distributed as $D_{\Lambda_q^U(F_{\mathsf{ID}}),\sigma}$, $D_{\Lambda_q^U(F'_{\mathsf{ID}}),\sigma}$ respectively.

**Encrypt($\mathsf{PP}, \mathsf{ID}, \mathbf{m}$)** : On input the public parameter $\mathsf{PP}$, an identity $\mathsf{ID}$ and a message $\mathbf{m} \in \{0,1\}^t$, do:

1. Let $A_{\mathsf{ID}} = B + \sum_{i+1}^{l} b_i A_i \in \mathbb{Z}_q^{n\times m}$.
2. Set $F_{\mathsf{ID}} := (A|A_{\mathsf{ID}}), F'_{\mathsf{ID}} := (A'|A_{\mathsf{ID}}) \in \mathbb{Z}_q^{n\times 2m}$
3. Choose uniformly random $\mathbf{s}_1, \mathbf{s}_2 \in \mathbb{Z}_q^n$

4. Choose $\mathbf{x}_1, \mathbf{x}_2 \in \overline{\Psi}_\alpha^t$ and compute

$$\mathsf{CT}_1 = U^T\mathbf{s}_1 + \mathbf{x}_1 + \mathbf{m}\lfloor\frac{q}{2}\rfloor \quad , \quad \mathsf{CT}_2 = U^T\mathbf{s}_2 + \mathbf{x}_2 + H(\mathbf{m})\lfloor\frac{q}{2}\rfloor \in \mathbb{Z}_q^t.$$

5. Choose $l$ uniformly random matrices $R_i \in \{-1, 1\}^{m\times m}$ for $i = 1, \cdots, l$ and define $R_{\mathsf{ID}} = \sum_{i=1}^{l} b_i R_i \in \{-l, \cdots, l\}^{m\times m}$.
6. Choose $\mathbf{y}_1, \mathbf{y}_2 \in \overline{\Psi}_\alpha^m$ and set $\mathbf{z}_1 = R_{\mathsf{ID}}^T\mathbf{y}_1, \mathbf{z}_2 = R_{\mathsf{ID}}^T\mathbf{y}_2 \in \mathbb{Z}_q^m$.
7. Compute

$$\mathsf{CT}_3 = F_{\mathsf{ID}}^T\mathbf{s}_1 + \begin{bmatrix}\mathbf{y}_1\\ \mathbf{z}_1\end{bmatrix}, \mathsf{CT}_4 = (F'_{\mathsf{ID}})^T\mathbf{s}_2 + \begin{bmatrix}\mathbf{y}_2\\ \mathbf{z}_2\end{bmatrix} \in \mathbb{Z}_q^{2m}.$$

8. The ciphertext is

$$\mathsf{CT}_{\mathsf{ID}} = (\mathsf{CT}_1, \mathsf{CT}_2, \mathsf{CT}_3, \mathsf{CT}_4) \in \mathbb{Z}_q^{2t+4m}.$$

**Decrypt**$(\mathsf{PP}, \mathsf{SK}_{\mathsf{ID}}, \mathsf{CT})$ : On input public parameter $\mathsf{PP}$, private key $\mathsf{SK}_{\mathsf{ID}} = (E_{\mathsf{ID}}, E'_{\mathsf{ID}})$ and a ciphertext $\mathsf{CT} = (\mathsf{CT}_1, \mathsf{CT}_2, \mathsf{CT}_3, \mathsf{CT}_4)$, do:

1. Compute $\mathbf{w} \leftarrow \mathsf{CT}_1 - E_{\mathsf{ID}}^T\mathsf{CT}_3 \in \mathbb{Z}_q^t$.
2. For each $i = 1, \cdots, t$, compare $w_i$ and $\lfloor\frac{q}{2}\rfloor$. If they are close, output $m_i = 1$ and otherwise output $m_i = 0$. We then obtain the message $\mathbf{m}$.
3. Compute $\mathbf{w}' \leftarrow \mathsf{CT}_2 - (E'_{\mathsf{ID}})^T\mathsf{CT}_4 \in \mathbb{Z}_q^t$.
4. For each $i = 1, \cdots, t$, compare $w'_i$ and $\lfloor\frac{q}{2}\rfloor$. If they are close, output $h_i = 1$ and otherwise output $h_i = 0$. We then obtain the vector $\mathbf{h}$.
5. If $\mathbf{h} = H(\mathbf{m})$ then output $\mathbf{m}$, otherwise output $\perp$.

**Trapdoor**$(\mathsf{SK}_{\mathsf{ID}})$ : On input an identity's secret key $\mathsf{SK}_{\mathsf{ID}} = (E_{\mathsf{ID}}, E'_{\mathsf{ID}})$, it outputs a trapdoor $\mathsf{td}_i = E'_{\mathsf{ID}}$.

**Test**$(\mathsf{td}_{\mathsf{ID}_i}, \mathsf{td}_{\mathsf{ID}_j}, \mathsf{CT}_{\mathsf{ID}_i}, \mathsf{CT}_{\mathsf{ID}_j})$ : On input trapdoors $\mathsf{td}_{\mathsf{ID}_i}, \mathsf{td}_{\mathsf{ID}_j}$ and ciphertexts $\mathsf{CT}_{\mathsf{ID}_i}, \mathsf{CT}_{\mathsf{ID}_j}$ for identities $\mathsf{ID}_i, \mathsf{ID}_j$ respectively, computes

1. For each $i$ (resp. $j$), compute $\mathbf{w}_i \leftarrow \mathsf{CT}_{i2} - (E'_{\mathsf{ID}_i})^T\mathsf{CT}_{i4} \in \mathbb{Z}_q^t$. For each $k = 1, \cdots, t$, compare each coordinate $w_{ik}$ with $\lfloor\frac{q}{2}\rfloor$ and output $\mathbf{h}_{ik} = 1$ if they are close, and 0 otherwise. At the end, we obtain the vector $\mathbf{h}_i$ (resp. $\mathbf{h}_j$).
2. Output 1 if $\mathbf{h}_i = \mathbf{h}_j$ and 0 otherwise.

**Theorem 4.** *Proposed IBEET construction above is correct if $H$ is a collision-resistant hash function.*

*Proof.* It is easy to see that if $\mathsf{CT}$ is a valid ciphertext of $\mathbf{m}$ then the decryption will always output $\mathbf{m}$. Moreover, if $\mathsf{CT}_{\mathsf{ID}_i}$ and $\mathsf{CT}_{\mathsf{ID}_j}$ are valid ciphertext of $\mathbf{m}$ and $\mathbf{m}'$ of identities $\mathsf{ID}_i$ and $ID_j$ respectively. Then the Test process checks whether $H(\mathbf{m}) = H(\mathbf{m}')$. If so then it outputs 1, meaning that $\mathbf{m} = \mathbf{m}'$, which is always correct with overwhelming probability since $H$ is collision resistant. Hence, proposed IBEET described above is correct. □

### 3.2 Parameters

We follow [1, Section 7.3] for choosing parameters for our scheme. Now for the system to work correctly we need to ensure

- the error term in decryption is less than $q/5$ with high probability, i.e., $q = \Omega(\sigma m^{3/2})$ and $\alpha < [\sigma l m \omega(\sqrt{\log m})]^{-1}$,
- that the $\mathsf{TrapGen}$ can operate, i.e., $m > 6n \log q$,
- that $\sigma$ is large enough for $\mathsf{SampleLeft}$ and $\mathsf{SampleRight}$, i.e., $\sigma > lm\omega(\sqrt{\log m})$,
- that Regev's reduction applies, i.e., $q > 2\sqrt{n}/\alpha$,
- that our security reduction applies (i.e., $q > 2Q$ where $Q$ is the number of identity queries from the adversary).

Hence the following choice of parameters $(q, m, \sigma, \alpha)$ from [1] satisfies all of the above conditions, taking $n$ to be the security parameter:

$$\begin{aligned} m &= 6n^{1+\delta} \quad , \quad q = \max(2Q, m^{2.5}\omega(\sqrt{\log n})) \\ \sigma &= ml\omega(\sqrt{\log n}) \quad , \quad \alpha = [l^2 m^2 \omega(\sqrt{\log n})]^{-1} \end{aligned} \tag{1}$$

and round up $m$ to the nearest larger integer and $q$ to the nearest larger prime. Here we assume that $\delta$ is such that $n^\delta > \lceil \log q \rceil = O(\log n)$. In [1, Section 7.5], it is shown that one can remove the restriction $q > 2Q$ and that $q = m^{2.5}\omega(\sqrt{\log n})$ is sufficient.

### 3.3 Security analysis

In this section, we claim that our proposed scheme is $\mathsf{OW\text{-}ID\text{-}CPA}$ secure against Type-I adversaries (cf. Theorem 5) and $\mathsf{IND\text{-}ID\text{-}CPA}$ secure against Type-II adversaries (cf. Theorem 6). The proofs will follow a similar argument of Theorem 8. We omit them in the current version and refer to the full version.

**Theorem 5.** *The IBEET with parameters $(q, n, m, \sigma, \alpha)$ as in (1) is $\mathsf{OW\text{-}ID\text{-}CPA}$ secure provided that $H$ is a one-way hash function and the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE assumption holds. In particular, suppose there exists a probabilistic algorithm $\mathcal{A}$ that wins the $\mathsf{OW\text{-}ID\text{-}CPA}$ game with advantage $\epsilon$, then there is a probabilistic algorithm $\mathcal{B}$ that solves the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem with advantage $\epsilon'$ such that*

$$\epsilon' \geq \frac{1}{2q}\left(\epsilon - \epsilon_{H,\mathsf{OW}}\right)$$

*where $\epsilon_{H,\mathsf{OW}}$ is the advantage of breaking the one-wayness of $H$.*

**Theorem 6.** *The IBEET with parameters $(q, n, m, \sigma, \alpha)$ as in (1) is $\mathsf{IND\text{-}ID\text{-}CPA}$ secure provided that $H$ is a one-way hash function and the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE assumption holds. In particular, suppose there exists a probabilistic algorithm $\mathcal{A}$ that wins the $\mathsf{IND\text{-}ID\text{-}CPA}$ game with advantage $\epsilon$, then there is a probabilistic algorithm $\mathcal{B}$ that solves the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem with advantage $\epsilon'$ such that*

$$\epsilon' \geq \frac{1}{4q}\left(\epsilon - -\epsilon_{H,\mathsf{OW}}\right)$$

*where $\epsilon_{H,\mathsf{OW}}$ is the advantage of breaking the one-wayness of $H$.*

# 4 Proposed Construction: IBEET against Insider Attack

## 4.1 Construction

**Setup**$(\lambda)$ : On input a security parameter $\lambda$, set the parameters $q, n, m, \sigma, \alpha$ as in section 3.2

1. Use $\mathsf{TrapGen}(q, n)$ to generate uniformly random $n \times m$-matrices $A, A' \in \mathbb{Z}_q^{n \times m}$ together with trapdoors $T_A$ and $T_{A'}$ respectively.
2. Select $l + 1$ uniformly random $n \times m$ matrices $A_1, \cdots, A_l, B \in \mathbb{Z}_q^{n \times m}$.
3. Select a uniformly random matrix $U \in \mathbb{Z}_q^{n \times t}$.
4. $H : \{0, 1\}^* \to \mathbb{Z}_q^m$ is a hash function.
5. Output the public parameter, the master secret key $\mathsf{MSK}$ and the master token $\mathsf{MTK}$:

$$\mathsf{PP} = (A, A', A_1, \cdots, A_l, B, U) \quad , \quad \mathsf{MSK} = T_A \quad , \quad \mathsf{MTK} = T_{A'}.$$

**Extract**$(\mathsf{ID}, \mathsf{MSK}, \mathsf{MTK})$ : On input a master secret key $\mathsf{MSK}$, a master token $\mathsf{MTK}$ and an identity $\mathsf{ID} = (b_1, \cdots, b_l) \in \{-1, 1\}^l$:

1. Let $A_{\mathsf{ID}} = B + \sum_{i+1}^{l} b_i A_i \in \mathbb{Z}_q^{n \times m}$.
2. Sample $E_{\mathsf{ID}} \in \mathbb{Z}_q^{2m \times t}$ as $E_{\mathsf{ID}} \leftarrow \mathsf{SampleLeft}(A, A_{\mathsf{ID}}, T_A, U, \sigma)$.
3. Output $\mathsf{SK}_{\mathsf{ID}} := E_{\mathsf{ID}}$ and $\mathsf{tok}_{\mathsf{ID}} = T_{A'}$.

Let $F_{\mathsf{ID}} = (A|A_{\mathsf{ID}})$ then $F_{\mathsf{ID}} \cdot E_{\mathsf{ID}} = U$ in $\mathbb{Z}_q$ and $E_{\mathsf{ID}}$ is distributed as $D_{\varLambda_q^U(F_{\mathsf{ID}}),\sigma}$.

**Encrypt**$(\mathsf{PP}, \mathsf{ID}, \mathsf{tok}_{\mathsf{ID}}, \mathbf{m})$ : On input the public parameter $\mathsf{PP}$, an identity $\mathsf{ID}$ with its token $\mathsf{tok}_{\mathsf{ID}}$ and a message $\mathbf{m} \in \{0, 1\}^t$, do:

1. Let $A_{\mathsf{ID}} = B + \sum_{i+1}^{l} b_i A_i \in \mathbb{Z}_q^{n \times m}$ and set $F_{\mathsf{ID}} := (A|A_{\mathsf{ID}}) \in \mathbb{Z}_q^{n \times 2m}$.
2. Choose uniformly random $\mathbf{s}', \mathbf{s} \in \mathbb{Z}_q^m$.
3. Choose $\mathbf{x} \in \overline{\Psi}_\alpha^t$ and compute

$$\mathsf{CT}_1 = T_{A'} \mathbf{s}'^T + H(\mathbf{m} \| T_{A'}) \in \mathbb{Z}_q^m \quad , \quad \mathsf{CT}_2 = U^T \mathbf{s} + \mathbf{x} + \mathbf{m} \lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q^t.$$

4. Choose $l$ uniformly random matrices $R_i \in \{-1, 1\}^{m \times m}$ for $i = 1, \cdots, l$ and define $R_{\mathsf{ID}} = \sum_{i=1}^{l} b_i R_i \in \{-l, \cdots, l\}^{m \times m}$.
5. Choose $\mathbf{y} \in \overline{\Psi}_\alpha^m$ and set $\mathbf{z} = R_{\mathsf{ID}}^T \mathbf{y} \in \mathbb{Z}_q^m$.
6. Compute

$$\mathsf{CT}_3 = F_{\mathsf{ID}}^T \mathbf{s} + \begin{bmatrix} \mathbf{y} \\ \mathbf{z} \end{bmatrix} \in \mathbb{Z}_q^{2m}.$$

7. The ciphertext is

$$\mathsf{CT}_{\mathsf{ID}} = (\mathsf{CT}_1, \mathsf{CT}_2, \mathsf{CT}_3) \in \mathbb{Z}_q^{t+3m}.$$

**Decrypt**$(\mathsf{SK}_{\mathsf{ID}}, \mathsf{tok}_{\mathsf{ID}}, \mathsf{CT})$ : On input the private key $\mathsf{SK}_{\mathsf{ID}} = E_{\mathsf{ID}}$, token $\mathsf{tok}_{\mathsf{ID}} = T_{A'}$ and a ciphertext $\mathsf{CT} = (\mathsf{CT}_1, \mathsf{CT}_2, \mathsf{CT}_3)$, do:

1. Compute $\mathbf{w} \leftarrow \mathsf{CT}_2 - E_{\mathsf{ID}}^T \mathsf{CT}_3 \in \mathbb{Z}_q^t$.
2. For each $i = 1, \cdots, t$, compare $w_i$ and $\lfloor \frac{q}{2} \rfloor$. If they are close, output $m_i = 1$ and otherwise output $m_i = 0$. We then obtain the message $\mathbf{m}$.

3. Compute $\mathbf{h} := A'\mathsf{CT}_1 \mod q$.
4. If $\mathbf{h} = A'H(\mathbf{m}\|T_{A'}) \mod q$, then output $\mathbf{m}$, otherwise output $\perp$.

**Test**$(\mathsf{CT}_{\mathsf{ID}_i}, \mathsf{CT}_{\mathsf{ID}_j})$ : On input ciphertexts $\mathsf{CT}_{\mathsf{ID}_i}, \mathsf{CT}_{\mathsf{ID}_j}$ for identities $\mathsf{ID}_i, \mathsf{ID}_j$ respectively, if $A'\mathsf{CT}_{i,1} = A'\mathsf{CT}_{j,1}$ then output 1, and 0 otherwise.

**Theorem 7.** *The above construction is correct if $H$ is a collision-resistant hash function.*

*Proof.* It is easy to see that if $\mathsf{CT}$ is a valid ciphertext of $\mathbf{m}$ then the decryption will always output $\mathbf{m}$. Moreover, if $\mathsf{CT}_{\mathsf{ID}_i}$ and $\mathsf{CT}_{\mathsf{ID}_j}$ are valid ciphertext of $\mathbf{m}$ and $\mathbf{m}'$ of identities $\mathsf{ID}_i$ and $ID_j$ respectively. Then the Test process checks whether $H(\mathbf{m}\|T_{A'}) = H(\mathbf{m}'\|T_{A'})$. If so then it outputs 1, meaning that $\mathbf{m} = \mathbf{m}'$, which is always correct with overwhelming probability since $H$ is collision resistant. Hence, proposed construction described above is correct. □

### 4.2 Security analysis

In this section, we prove that our IBEET scheme is wIND-ID-CPA secure.

**Theorem 8.** *The IBEET construction with parameters $(q, n, m, \sigma, \alpha)$ as in (1) is wIND-ID-CPA secure provided that $H$ is a one-way hash function and the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE assumption holds. In particular, suppose there exists a probabilistic algorithm $\mathcal{A}$ that wins the wIND-ID-CPA game with advantage $\epsilon$, then there is a probabilistic algorithm $\mathcal{B}$ that solves the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem with advantage $\epsilon'$ such that*

$$\epsilon' \geq \frac{1}{4q}\left(\epsilon - \epsilon_{H,\mathsf{OW}}\right)$$

*where $\epsilon_{H,\mathsf{OW}}$ is the advantage of breaking the one-wayness of $H$.*

*Proof.* Assume that there is an adversary $\mathcal{A}$ who breaks the wIND-ID-CPA security of the IBEET scheme with non-negligible probability $\epsilon$. We construct an algorithm $\mathcal{B}$ who solves the LWE problem using $\mathcal{A}$. We now describe the behavior of $\mathcal{B}$. Assume that $\mathsf{ID}^*$ is the target identity of the adversary $\mathcal{A}$ and the challenge ciphertext is $\mathsf{CT}^*_{\mathsf{ID}^*} = (\mathsf{CT}^*_{\mathsf{ID}^*,1}, \mathsf{CT}^*_{\mathsf{ID}^*,2}, \mathsf{CT}^*_{\mathsf{ID}^*,3})$.

We will proceed the proof in a sequence of games. In game $i$, let $\mathcal{W}_i$ denote the event that the adversary $\mathcal{A}$ correctly guesses the challenge bit. The adversary's advantage in Game $i$ is $\left|\Pr[\mathcal{W}_i] - \frac{1}{2}\right|$.

**Game 0.** This is the original wIND-ID-CPA game between the attacker $\mathcal{A}$ against the scheme and the wIND-ID-CPA challenger.

**Game 1.** This is similar to Game 0 except the way the challenger $\mathcal{B}$ generates the public key for the identity $\mathsf{ID}^*$, as the following. Let $R_i^* \in \{-1, 1\}^{m\times m}$ for $i = 1, \cdots, l$ be the ephemeral random matrices generated for the creation of the ciphertext $\mathsf{CT}^*_{\mathsf{ID}^*}$. In this game, the challenger chooses $l$ matrices $R_i^*$ uniformly random in $\{-1, 1\}^{m\times m}$ and chooses $l$ random scalars $h_i \in \mathbb{Z}_q$ for

$i = 1, \cdots, l$. Then it generates $A, T_{A'}$ and $B$ as in Game 0 and constructs the matrices $A_i$ for $i = 1, \cdots, l$ as

$$A_i \leftarrow A \cdot R_i^* - h_i \cdot B \in \mathbb{Z}_q^{n \times m}.$$

The remainder of the game is unchanged with $R_i^*$, $i = 1, \cdots, l$, used to generate the challenge ciphertext. Similar to the proof of [1, Theorem 25] we have that the $A_i$ are close to uniform and hence they are random independent matrices in the view of the adversary as in Game 0. Therefore

$$\Pr[\mathcal{W}_1] = \Pr[\mathcal{W}_0].$$

**Game 2.** This is similar to Game 1 except that at the challenge phase, $\mathcal{B}$ chooses arbitrary message $\mathbf{m}'$ from the message space and encrypts $\mathbf{m}'$ in $\mathsf{CT}_{\mathsf{ID},1}$. Other steps are similar to Game 1. Here we can not expect the behavior of $\mathcal{A}$. Since $A'$ is public, $\mathcal{A}$ can obtain $A'H(\mathbf{m}'\|T'_A)$. At the end if $\mathcal{A}$ outputs $\mathbf{m}'$, call this event $E_2$, then $\mathcal{A}$ has broken the one-wayness of the hash function $H$. Therefore we have

$$\Pr[W_1] - \Pr[W_2] \leq \epsilon_{H,\mathsf{OW}}$$

where $\epsilon_{H,\mathsf{OW}}$ is the advantage of $\mathcal{A}$ in breaking the one-wayness of $H$.

**Game 3.** This game is similar to Game 2 except that we add an abort that is independent of adversary's view. The challenger behaves as follows:

- The setup phase is identical to Game 2 except that the challenger also chooses random $h_i \in \mathbb{Z}_q$, $i = 1, \cdots, l$ and keeps it to itself.
- In the final guess phase, the adversary outputs a random guess $b' \in \{0, 1\}$ for $b$. The challenger now does the following:
  1. **Abort check:** for all queries $\mathsf{CT}_{\mathsf{ID}}$ to the decryption oracle $\mathcal{O}^{\mathsf{Dec}}$, the challenger checks whether the identity $\mathsf{ID} = (b_1, \cdots, b_l)$ satisfies $1 + \sum_{i=1}^{h} b_i h_i \neq 0$ and $1 + \sum_{i=1}^{h} b_i^* h_i = 0$. If not then the challenger overwrites $b'$ with a fresh random bit in $\{0, 1\}$ and aborts the game.
  2. **Artificial abort:** the challenger samples a message $\Gamma$ such that $\Pr[\Gamma = 1]$ is calculated through a function $\mathcal{G}$ (defined as in [1]) evaluated through all the queries of $\mathcal{A}$. If $\Gamma = 1$ the challenger overwrites $b'$ with a fresh random bit and aborts the game (due to artificial abort); see [1] for more details.

It follows from the proof of [1, Theorem 25] that

$$\left|\Pr[\mathcal{W}_3] - \frac{1}{2}\right| \geq \frac{1}{4q}\left|\Pr[\mathcal{W}_2] - \frac{1}{2}\right|.$$

**Game 4.** We now change the way how $A$ and $B$ are generated in Game 3. In Game 4, $A$ is a random matrix in $\mathbb{Z}_q^{n \times m}$ and $B$ is generated through $\mathsf{TrapGen}(q, n)$ together with an associated trapdoor $T_B$ for $\Lambda_q^{\perp}(B)$. The construction of $A_i$ for $i = 1, \cdots, l$ remains the same as in Game 3, i.e., $A_i = AR_i^* - h_i B$. When $\mathcal{A}$ queries $\mathcal{O}^{\mathsf{Ext}}(\mathsf{ID})$ for the secret key of $\mathsf{ID} = (b_1, \cdots, b_l)$, $\mathcal{B}$ performs as follows:

- $\mathcal{B}$ sets
$$F_{\mathsf{ID}} := (A|B + \sum_{i=1}^{l} A_i) = (A|AR + h_{\mathsf{ID}} B)$$
where
$$R \leftarrow \sum_{i=1}^{l} b_i R_i^* \in \mathbb{Z}_q^{n\times m} \quad \text{and} \quad h_{\mathsf{ID}} \leftarrow 1 + \sum_{i=1}^{l} b_i h_i \in \mathbb{Z}_q. \tag{2}$$
- If $h_{\mathsf{ID}} = 0$ then abort the game and pretend that the adversary outputs a random bit $b'$ as in Game 3.
- Set $E_{\mathsf{ID}} \leftarrow \mathsf{SampleRight}(A, h_{\mathsf{ID}} B, R, T_B, U, \sigma) \in \mathbb{Z}_q^{2m\times t}$. Note that since $h_{\mathsf{ID}}$ is non-zero, and so $T_B$ is also a trapdoor for $h_\theta B$. And hence the output $E_{\mathsf{ID}}$ satisfies $F_{\mathsf{ID}} \cdot E_{\mathsf{ID}} = U$ in $\mathbb{Z}_q^t$. Moreover, Theorem 2 shows that when $\sigma > \|\widetilde{T_B}\| s_R \omega(\sqrt{m})$ with $s_R := \|R\|$, the generated $E_{\mathsf{ID}}$ is distributed close to $\mathcal{D}_{\Lambda_q^U}(F_{\mathsf{ID}})$ as in Game 2.
- Return $\mathsf{SK}_{\mathsf{ID}} := E_{\mathsf{ID}}$.

Game 4 is otherwise the same as Game 3. In particular, in the challenge phase, the challenger checks if $\mathsf{ID}^* = (b_1^*, \cdots, b_l^*)$ satisfies $1 + \sum_{i=1}^{l} b_i^* h_i = 0$. If not, the challenger aborts the game as in Game 3. Similarly, in Game 4, the challenger also implements an artificial abort in the guess phase. Since Game 3 and Game 2 are identical in the adversary's view, we have that
$$\Pr[\mathcal{W}_4] = \Pr[\mathcal{W}_3].$$

**Game 5.** Game 5 is identical to Game 4, except that the challenge ciphertext is always chosen randomly. And thus the advantage of $\mathcal{A}$ is always 0.

We now show that Game 4 and Game 5 are computationally indistinguishable. If the abort event happens then the games are clearly indistinguishable. We, therefore, consider only the queries that do not cause an abort.

Suppose now $\mathcal{A}$ has a non-negligible advantage in distinguishing Game 4 and Game 5. We use $\mathcal{A}$ to construct $\mathcal{B}$ to solve the LWE problem as follows.

**Setup.** First of all, $\mathcal{B}$ requests from $\mathcal{O}$ and receives, for each $j = 1, \cdots, t$ a fresh pair $(\mathbf{a}_i, d_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ and for each $i = 1, \cdots, m$, a fresh pair $(\mathbf{u}_i, v_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$. $\mathcal{A}$ announces an identity $\mathsf{ID}$ for the target identity. $\mathcal{B}$ constructs the public parameter $\mathsf{PP}$ as follows:

1. Assemble the random matrix $A \in \mathbb{Z}_q^{n\times m}$ from $m$ of previously given LWE samples by letting the $i$-th column of $A$ to be the $n$-vector $\mathbf{u}_i$ for all $i = 1, \cdots, m$.
2. Assemble the first $t$ unused LWE samples $\mathbf{a}_1, \cdots, \mathbf{a}_t$ to become a public random matrix $U \in \mathbb{Z}_q^{n\times t}$.
3. Run $\mathsf{TrapGen}(q, \sigma)$ to generate uniformly random matrices $A', B \in \mathbb{Z}_q^{n\times m}$ together with their trapdoor $T_{A'}$ and $T_B$ respectively.

4. Choose $l$ random matrices $R_i^* \in \{-1,1\}^{m\times m}$ for $i = 1, \cdots, l$ and $l$ random scalars $h_i \in \mathbb{Z}_q$ for $i = 1, \cdots, l$. Next it constructs the matrices $A_i$ for $i = 1, \cdots, l$ as
$$A_i \leftarrow AR_i^* - h_i B \in \mathbb{Z}_q^{n\times m}.$$
Note that it follows from the leftover hash lemma [14, Theorem 8.38] that $A_1, \cdots, A_l$ are statistically close to uniform.
5. Set $\mathsf{PP} := (A, A', A_1, \cdots, A_l, B, U)$ and send to $\mathcal{A}$.

**Queries.** $\mathcal{B}$ answers the queries as in Game 4, including aborting the game if needed.

**Challenge.** Now when $\mathcal{A}$ sends $\mathcal{B}$ two messages $\mathbf{m}_0$ and $\mathbf{m}_1$ and a target identity $\mathsf{ID}^*$. $\mathcal{B}$ choose a random bit $b \in \{0,1\}$ and computes the challenge ciphertext $\mathsf{CT}^*_{\mathsf{ID}^*} = (\mathsf{CT}^*_{\mathsf{ID}^*,1}, \mathsf{CT}^*_{\mathsf{ID}^*,2}, \mathsf{CT}^*_{\mathsf{ID}^*,3})$ for $\mathbf{m}_b$ as follows:

1. Choose a random $\mathbf{s}' \in \mathbb{Z}_q^m$ and compute
$$\mathsf{CT}^*_{\mathsf{ID}^*,1} = T_{A'}\mathbf{s}'^T + H(\mathbf{m}_b \| T_{A'}) \in \mathbb{Z}_q^m.$$
2. Assemble $d_1, \cdots, d_t, v_1, \cdots, v_m$ from the entries of the samples to form $\mathbf{d}^* = [d_1, \cdots, d_t]^T \in \mathbb{Z}_q^t$ and $\mathbf{v}^* = [v_1, \cdots, v_m]^T \in \mathbb{Z}_q^m$.
3. Set $\mathsf{CT}^*_{\mathsf{ID}^*,2} \leftarrow \mathbf{d}^* + \mathbf{m}_b\lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q^t$.
4. Compute $R^*_{\mathsf{ID}^*} := \sum_{i=1}^l b_i^* R_i^* \in \{-l, \cdots, l\}^{m\times m}$.
5. Set
$$\mathsf{CT}^*_{\mathsf{ID}^*,3} := \begin{bmatrix} \mathbf{v}^* \\ (R^*_{\mathsf{ID}^*})^T \mathbf{v}^* \end{bmatrix} \in \mathbb{Z}_q^{2m}.$$

Then $\mathcal{B}$ sends $\mathsf{CT}^*_{\mathsf{ID}^*} = (\mathsf{CT}^*_{\mathsf{ID}^*,1}, \mathsf{CT}^*_{\mathsf{ID}^*,2}, \mathsf{CT}^*_{\mathsf{ID}^*,3})$ to $\mathcal{A}$.

Note that in case of no abort, one has $h_{\mathsf{ID}^*} = 0$ and so $F_{\mathsf{ID}^*} = (A|AR^*_{\mathsf{ID}^*})$. When the oracle is pseudorandom, i.e., $\mathcal{O} = \mathcal{O}_{\mathbf{s}}$ then $\mathbf{v}^* = A^T\mathbf{s} + \mathbf{y}$ for some random noise vector $\mathbf{y} \leftarrow \overline{\Psi}_\alpha^m$. Therefore $\mathsf{CT}^*_{\mathsf{ID}^*,3}$ in Step 5 satisfies:
$$\mathsf{CT}^*_{\mathsf{ID}^*,3} := \begin{bmatrix} A^T\mathbf{s} + \mathbf{y} \\ (AR^*_{\mathsf{ID}^*})^T\mathbf{s} + (R^*_{\mathsf{ID}^*})^T\mathbf{y} \end{bmatrix} = (F^*_{\mathsf{ID}})^T\mathbf{s} + \begin{bmatrix} \mathbf{y} \\ (R^*_{\mathsf{ID}^*})^T\mathbf{y} \end{bmatrix}.$$
Moreover, $\mathbf{d}^* = U^T\mathbf{s} + \mathbf{x}$ for some $\mathbf{x} \leftarrow \overline{\Psi}_\alpha^t$ and therefore
$$\mathsf{CT}^*_{\mathsf{ID}^*,2} = U^T\mathbf{s} + \mathbf{x} + \mathbf{m}_b\lfloor \frac{q}{2} \rfloor.$$
Therefore $\mathsf{CT}^*_{\mathsf{ID}^*}$ is a valid ciphertext.

When $\mathcal{O} = \mathcal{O}_\$$ we have that $\mathbf{d}^*$ is uniform in $\mathbb{Z}_q^t$ and $\mathbf{v}^*$ is uniform in $\mathbb{Z}_q^m$. Then obviously $\mathsf{CT}^*_{\mathsf{ID}^*,2}$ is uniform. It follows also from the leftover hash lemma (cf. [14, Theorem 8.38]) that $\mathsf{CT}^*_{\mathsf{ID}^*,3}$ is also uniform.

**Guess.** After Phase 2, $\mathcal{A}$ guesses if it is interacting with a Game 4 or Game 5. The simulator also implements the artificial abort from Game 4 and Game 5 and output the final guess as to the answer to the LWE problem.

We have seen above that when $\mathcal{O} = \mathcal{O}_{\mathbf{s}}$ then the adversary's view is as in Game 4. When $\mathcal{O} = \mathcal{O}_{\$}$ then the view of the adversary is as in Game 5. Hence the advantage $\epsilon'$ of $\mathcal{B}$ in solving the LWE problem is the same as the advantage of $\mathcal{A}$ in distinguishing Game 4 and Game 5. Since $\Pr[\mathcal{W}_5] = 0$, we have

$$\Pr[\mathcal{W}_4] = \Pr[\mathcal{W}_4] - \Pr[\mathcal{W}_5] \leq \epsilon'.$$

Hence combining the above results yields the desired result. we obtain that

$$\epsilon = \Pr[W_0] \leq \epsilon_{H,\mathsf{ow}} + 4q\epsilon'$$

which implies

$$\epsilon' \geq \frac{1}{4q}\left(\epsilon - \epsilon_{H,\mathsf{ow}}\right)$$

as desired. □

## 5 Conclusion

In this paper, we propose a direct construction of IBEET based on the hardness of Learning With Errors problem. Efficiency is the reason to avoid the instantiation of lattice-based IBEET from the generic construction by Lee et al. [7]. In addition, we also modify our scheme to obtain an IBEET against insider attack. We will leave as a future work for improving our schemes to achieve CCA2-security as well as to support flexible authorisation.

## Acknowledgement

This work is supported by the Australian Research Council Discovery Project DP180100665. We would like to thank Tsz Hon Yuen and anonymous reviewers for many helpful comments and fruitful discussions.

## References

1. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, pages 553–572, 2010.
2. Miklós Ajtai. Generating hard instances of the short basis problem. In *Automata, Languages and Programming, 26th International Colloquium, ICALP'99, Prague, Czech Republic, July 11-15, 1999, Proceedings*, pages 1–9, 1999.
3. Joël Alwen and Chris Peikert. Generating shorter bases for hard random lattices. In *26th International Symposium on Theoretical Aspects of Computer Science, STACS 2009, February 26-28, 2009, Freiburg, Germany, Proceedings*, pages 75–86, 2009.
4. Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *SIAM J. Comput.*, 36(5):1301–1328, 2007.

5. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, pages 523–552, 2010.
6. Dung Hoang Duong, Kazuhide Fukushima, Shinsaku Kiyomoto, Partha Sarathi Roy, and Willy Susilo. A lattice based public key encryption with equality test in standard model. In *Information Security and Privacy - 24nd Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3-5, 2019, Proceedings*, pages 168–183, 2019.
7. Hyung Tae Lee, San Ling, Jae Hong Seo, Huaxiong Wang, and Taek-Young Youn. Public key encryption with equality test in the standard model. *Cryptology ePrint Archive*, Report 2016/1182, 2016.
8. Hyung Tae Lee, San Ling, Jae Hong Seo, and Huaxiong Wang. Semi-generic construction of public key encryption and identity-based encryption with equality test. *Inf. Sci.*, 373:419–440, 2016.
9. Hyung Tae Lee, Huaxiong Wang, and Kai Zhang. Security analysis and modification of id-based encryption with equality test from ACISP 2017. In *Information Security and Privacy - 23rd Australasian Conference, ACISP 2018, Wollongong, NSW, Australia, July 11-13, 2018, Proceedings*, pages 780–786, 2018.
10. Sha Ma. Identity-based encryption with outsourced equality test in cloud computing. *Information Sciences*, 328:389–402, 2016.
11. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 372–381, 2004.
12. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93, 2005.
13. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
14. Victor Shoup. *A computational introduction to number theory and algebra*. Cambridge University Press, second edition, 2008.
15. Tong Wu, Sha Ma, Yi Mu, and Shengke Zeng. Id-based encryption with equality test against insider attack. In *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part I*, pages 168–183, 2017.

## Appendix A: An instantiation of Lee et al.'s construction

In this section, we will present a lattice-based IBEET which is an instantiation of the Lee et al.'s construction [7]. In their generic construction, they need (i) a multi-bit HIBE scheme and (ii) an one-time signature scheme. To instantiate their construction, we modify the lattice based single-bit HIBE of [1] to multi-bit one and use it, along with the signature scheme, to have following construction of lattice based IBEET. Even though one needs only a one-time signature scheme, we choose the full secure signature scheme from [1] to unify the system, since in such case, both signature and HIBE schemes use the same public key. It is required to use multi-bit HIBE and signature scheme to have IBEET from Lee et al.'s [7].

In what follows, we will denote by $[id_1.id_2.id_3]$ the identity of a 3-level HIBE scheme where $id_1$ is the first level identity, $id_2$ is the second level identity and $id_3$ is third level identity. Below, we follow [7] to denote by $[\mathsf{ID}.0]$ (resp. $[\mathsf{ID}.1]$) an identity in the second level in which we indicate that $\mathsf{ID}$ is the identity of the first level.

### 5.1 Construction

$\mathsf{Setup}(\lambda)$

On input security parameter $\lambda$, and a maximum hierarchy depth 3, set the parameters $q, n, m, \bar{\sigma}, \bar{\alpha}$. The vector $\bar{\sigma}$ & $\bar{\alpha} \in \mathbb{R}^2$ and we use $\sigma_l$ and $\alpha_l$ to refer to their $l$- th coordinate.

1. Use algorithm $\mathsf{TrapGen}(q, n)$ to select a uniformly random $n \times m$- matrix $A, A' \in \mathbb{Z}_q^{n\times m}$ with a basis $T_A, T_{A'}$ for $\Lambda_q^{\perp}(A)$ and $\Lambda_q^{\perp}(A')$, respectively. Repeat this Step until $A$ and $A'$ have rank $n$.
2. Select $l + 1$ uniformly random $m \times m$ matrices $A_1, A_2, A_3, \cdots, A_l, B \in \mathbb{Z}_q^{n\times m}$.
3. Select a uniformly random matrix $U \in \mathbb{Z}_q^{n\times t}$.
4. We need some hash functions $H : \{0,1\}^* \to \{0,1\}^t$, $H_1 : \{0,1\}^* \to \{-1,1\}^t$, $H_2 : \{0,1\}^* \to \mathbb{Z}_q^n$ and a full domain difference map $H' : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$ as in [1, Section 5].
5. Output the public key and the secret key

$$\mathsf{PK} = (A, A', A_1, A_2, A_3, \cdots, A_l, B, U) \quad , \quad \mathsf{MSK} = T_A, \quad \mathsf{sk_s} = T_{A'}$$

**Extract**$(\mathsf{PP}, \mathsf{MSK}, \mathsf{ID})$ : On input the public parameter $\mathsf{PP}$, a master secret key $\mathsf{MSK}$ and an identity $\mathsf{ID}(\in \mathbb{Z}_q^n) = (b_1, \cdots, b_l) \in \{-1,1\}^l$:

1. Let $A_{\mathsf{ID}} = A_1 + H'(\mathsf{ID})B \in \mathbb{Z}_q^{n\times m}$.
2. Sample $E \in \mathbb{Z}_q^{2m\times t}$ as

$$E \leftarrow \mathsf{SampleBasisLeft}(A, A_{\mathsf{ID}}, T_A, U, \sigma).$$

3. Output $\mathsf{SK}_{\mathsf{ID}} := E$.

Let $F_{\mathsf{ID}} = (A|A_{\mathsf{ID}}) \in \mathbb{Z}_q^{n\times 2m}$ then $F_{\mathsf{ID}} \cdot E = U$ in $\mathbb{Z}_q$ and $E$ is distributed as $D_{\Lambda_q^U(F_{\mathsf{ID}}),\sigma}$.

$\mathsf{Enc}(\mathsf{PP}, \mathsf{ID}, \mathbf{m})$

On input the public key $\mathsf{PK}$ and a message $\mathbf{m} \in \{0,1\}^t$ do

1. Choose uniformly random $\mathbf{s}_1, \mathbf{s}_2 \in \mathbb{Z}_q^n$.
2. Choose $\mathbf{x}_1, \mathbf{x}_2 \in \overline{\Psi}_{\alpha}^{t}$ and compute

$$\mathbf{c}_1 = U^T\mathbf{s}_1 + \mathbf{x}_1 + \mathbf{m}\lfloor\frac{q}{2}\rfloor \in \mathbb{Z}_q^t,$$
$$\mathbf{c}_2 = U^T\mathbf{s}_2 + \mathbf{x}_2 + H(\mathbf{m})\lfloor\frac{q}{2}\rfloor \in \mathbb{Z}_q^t.$$

3. Set $vk_s = A_1\| \cdots \|A_l$.
4. Set $id := H_2(vk_s) \in \mathbb{Z}_q^n$.

5. Build the following matrices in $\mathbb{Z}_q^{n\times 4m}$:

$$F_{\mathsf{ID}.0.vk_s} = (F_{\mathsf{ID}}|A_2 + H'(0)\cdot B|A_3 + H'(id)\cdot B),$$
$$F_{\mathsf{ID}.1.vk_s} = (F_{\mathsf{ID}}|A_2 + H'(1)\cdot B|A_3 + H'(id)\cdot B).$$

6. Choose a uniformly random $n \times 2m$ matrix $R$ in $\{-1,1\}^{n\times 3m}$.
7. Choose $\mathbf{y}_1, \mathbf{y}_2 \in \overline{\Psi}_\alpha^m$ and set $\mathbf{z}_1 = R^T\mathbf{y}_1, \mathbf{z}_2 = R^T\mathbf{y}_2 \in \mathbb{Z}_q^{3m}$.
8. Compute

$$\mathbf{c}_3 = F_{\mathsf{ID}.0.vk_s}^T\mathbf{s}_1 + [\mathbf{y}_1^T|\mathbf{z}_1^T]^T \in \mathbb{Z}_q^{4m},$$
$$\mathbf{c}_4 = F_{\mathsf{ID}.1.vk_s}^T\mathbf{s}_2 + [\mathbf{y}_2^T|\mathbf{z}_2^T]^T \in \mathbb{Z}_q^{4m}.$$

9. Let $\mathbf{b} := H_1(\mathbf{c}_1\|\mathbf{c}_2\|\mathbf{c}_3\|\mathbf{c}_4) \in \{-1,1\}^l$ and define a matrix

$$F = (A'|B + \sum_{i=1}^{l} b_i A_i) \in \mathbb{Z}_q^{n\times 2m}.$$

10. Extract a signature $\mathbf{e} \in \mathbb{Z}^{2m\times t}$ by

$$\mathbf{e} \leftarrow \mathsf{SampleBasisLeft}(A', B + \sum_{i=1}^{l} b_i A_i, T_{A'}, 0, \sigma).$$

Note that $F\cdot\mathbf{e} = 0 \mod q$.

11. Output the ciphertext

$$\mathsf{CT} = (vk, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{e}).$$

$\mathsf{Dec}(\mathsf{PP}, \mathsf{SK}_{\mathsf{ID}}, \mathsf{CT})$

On input a secret key $\mathsf{SK}_{\mathsf{ID}}$ and a ciphertext $\mathsf{CT}$, do

1. Parse the ciphertext $\mathsf{CT}$ into

$$(vk, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{e}).$$

2. Let $\mathbf{b} := H_1(\mathbf{c}_1\|\mathbf{c}_2\|\mathbf{c}_3\|\mathbf{c}_4) \in \{-1,1\}^l$ and define a matrix

$$F = (A'|B + \sum_{i=1}^{l} b_i A_i) \in \mathbb{Z}_q^{n\times 2m}.$$

3. If $F\cdot\mathbf{e} = 0$ in $\mathbb{Z}_q$ and $\|\mathbf{e}\| \leq \sigma\sqrt{2m}$ then continue to Step 4; otherwise output $\perp$.
4. Set $id := H_2(vk) \in \mathbb{Z}_q^n$ and build the following matrices:

$$F_{\mathsf{ID}.0} = (F_{\mathsf{ID}}|A_2 + H'(0)\cdot B) \in \mathbb{Z}_q^{n\times 3m},$$
$$F_{\mathsf{ID}.1} = (F_{\mathsf{ID}}|A_2 + H'(1)\cdot B) \in \mathbb{Z}_q^{n\times 3m}.$$

$$F_{\mathsf{ID}.0.vk_s} = (F_{\mathsf{ID}}|A_2 + H'(0)\cdot B|A_3 + H'(id)\cdot B) \in \mathbb{Z}_q^{n\times 4m},$$
$$F_{\mathsf{ID}.1.vk_s} = (F_{\mathsf{ID}}|A_2 + H'(1)\cdot B|A_3 + H'(id)\cdot B) \in \mathbb{Z}_q^{n\times 4m}.$$

5. Generate

$$\begin{aligned}
E_{\mathsf{ID}.0} &\leftarrow \mathsf{SampleBasisLeft}(F_{\mathsf{ID}}, A_2 + H'(0)\cdot B, E, U, \sigma)\\
&\qquad s.t.\ F_{\mathsf{ID}.0}\cdot E_{\mathsf{ID}.0} = U\\
E_{\mathsf{ID}.1} &\leftarrow \mathsf{SampleBasisLeft}(F_{\mathsf{ID}}, A_2 + H'(1)\cdot B, E, U, \sigma)\\
&\qquad s.t.\ F_{\mathsf{ID}.1}\cdot E_{\mathsf{ID}.1} = U\\
E_{\mathsf{ID}.0.vk_s} &\leftarrow \mathsf{SampleBasisLeft}(F_{\mathsf{ID}.0}, A_3 + H'(0)\cdot B, E_{\mathsf{ID}.0}, U, \sigma)\\
&\qquad s.t.\ F_{\mathsf{ID}.0.vk_s}\cdot E_{\mathsf{ID}.0.vk_s} = U\\
E_{\mathsf{ID}.1.vk_s} &\leftarrow \mathsf{SampleBasisLeft}(F_{\mathsf{ID}.1}, A_3 + H'(1)\cdot B, E_{\mathsf{ID}.1}, U, \sigma)\\
&\qquad s.t.\ F_{\mathsf{ID}.1.vk_s}\cdot E_{\mathsf{ID}.1.vk_s} = U.
\end{aligned}$$

6. Compute $\mathbf{w} \leftarrow \mathbf{c}_1 - E^T_{\mathsf{ID}.0.vk_s}\mathbf{c}_3 \in \mathbb{Z}_q^t$.
7. For each $i = 1, \cdots, t$, compare $w_i$ and $\lfloor \frac{q}{2} \rfloor$. If they are close, output $m_i = 1$ and otherwise output $m_i = 0$. We then obtain the message $\mathbf{m}$.
8. Compute $\mathbf{w}' \leftarrow \mathbf{c}_2 - E^T_{\mathsf{ID}.1.vk_s}\mathbf{c}_4 \in \mathbb{Z}_q^t$.
9. For each $i = 1, \cdots, t$, compare $w'_i$ and $\lfloor \frac{q}{2} \rfloor$. If they are close, output $h_i = 1$ and otherwise output $h_i = 0$. We then obtain the vector $\mathbf{h}$.
10. If $\mathbf{h} = H(\mathbf{m})$ then output $\mathbf{m}$, otherwise output $\perp$.

$\mathsf{Td}(\mathsf{SK}_i)$

On input the secret key $\mathsf{SK}_i(= E_i)$ of a user $U_i$, run

$$\mathsf{td}_i \leftarrow \mathsf{SampleBasisLeft}(F_{\mathsf{ID}}, A_2 + H'(1)\cdot B, E_i, U, \sigma).$$

$\mathsf{Test}(\mathsf{td}_i, \mathsf{td}_j, \mathsf{CT}_i, \mathsf{CT}_j)$

On input trapdoors $\mathsf{td}_i, \mathsf{td}_j$ and ciphertexts $\mathsf{CT}_i, \mathsf{CT}_j$ of users $U_i$ and $U_j$ respectively, for $k = i, j$, do the following

1. Parse $\mathsf{CT}_k$ into
$$(vk_k, \mathbf{c}_{k,1}, \mathbf{c}_{k,2}, \mathbf{c}_{k,3}, \mathbf{c}_{k,4}, \mathbf{e}_k).$$
2. Sample $E_{\mathsf{ID}_k.1.vk_s} \in \mathbb{Z}_q^{5m\times t}$ from
$$\mathsf{SampleBasisLeft}(F_{\mathsf{ID}_k.1}, A_{k,3} + H'(1)\cdot B_k, E_{\mathsf{ID}_k.1}, U, \sigma).$$
3. Use $E_{\mathsf{ID}_k.1.vk_s}$ to decrypt $\mathbf{c}_{k,2}$, $\mathbf{c}_{k,4}$ as in Step 8-9 of $\mathsf{Dec}(\mathsf{SK}, \mathsf{CT})$ above to obtain the hash value $\mathbf{h}_k$.
4. If $\mathbf{h}_i = \mathbf{h}_j$ then ouput 1; otherwise output 0.

**Theorem 5** (Correctness)**.** *The above IBEET is correct if the hash function $H$ is collision resistant.*

*Proof.* Since we employ the multi-bit HIBE and signature scheme from [1], their correctness follow from [1]. The Theorem follows from [7, Theorem 1]. □

### 5.2 Parameters

We follow [1, Section 8.3] for choosing parameters for our scheme. Now for the system to work correctly we need to ensure

- the error term in decryption is less than $q/5$ with high probability, i.e., $q = \Omega(\sigma m^{3/2})$ and $\alpha < [\sigma l m \omega(\sqrt{\log m})]^{-1}$,
- that the $\mathsf{TrapGen}$ can operate, i.e., $m > 6n \log q$,
- that $\sigma$ is large enough for $\mathsf{SampleLeft}$ and $\mathsf{SampleRight}$, i.e., $\sigma > lm\omega(\sqrt{\log m})$,
- that Regev's reduction applies, i.e., $q > 2\sqrt{n}/\alpha$,

Hence the following choice of parameters $(q, m, \sigma, \alpha)$ from [1] satisfies all of the above conditions, taking $n$ to be the security parameter:

$$\begin{aligned} m = 6n^{1+\delta} \quad &, \quad q = \max(2Q, m^{2.5}\omega(\sqrt{\log n})) \\ \sigma = ml\omega(\sqrt{\log n}) \quad &, \quad \alpha = [l^2 m^2 \omega(\sqrt{\log n})] \end{aligned} \tag{3}$$

and round up $m$ to the nearest larger integer and $q$ to the nearest larger prime. Here we assume that $\delta$ is such that $n^{\delta} > \lceil \log q \rceil = O(\log n)$.

**Theorem 6.** *The IBEET constructed in Section 5.1 with paramaters as in* (3) *is* IND-ID-CCA2 *secure provided that* $H_1$ *is collision resistant.*

*Proof.* The HIBE is IND-sID-CPA secure by [1, Theorem 33] and the signature is strongly unforgeable by [1, Section 7.5]. The result follows from [7, Theorem 5]. □

**Theorem 7** ([7, Theorem 3])**.** *The IBEET with parameters* $(q, n, m, \sigma, \alpha)$ *as in* (3) *is* OW-ID-CCA2 *provided that* $H$ *is one-way and* $H_1$ *is collision resistant.*

*Proof.* The HIBE is IND-sID-CPA secure by [1, Theorem 33] and the signature is strongly unforgeable by [1, Section 7.5]. The result follows from [7, Theorem 6]. □