IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024EAP1105

Publicized:2024/10/08

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

Construction of Compact Lattice-based IBE with equality test

Chunfeng FU[†], **Renjie JIN**[†], **Longjiang QU**[†], ***and*** **Zijian ZHOU**[†], ***Nonmembers***

SUMMARY
Identity-based encryption with equality test (IBE-ET) allows the detection of whether two different ciphertexts encrypt the same plaintext without decryption within the conventional identity-based encryption (IBE) model. This property ensures the confidentiality of communication and reduces the storage overhead of ciphertexts in cryptosystems. However, IBE-ET schemes based on traditional assumptions, such as discrete logarithm and integer factoring, are vulnerable to quantum algorithm attacks, highlighting the importance of designing lattice-based IBE-ET schemes. To address this, researchers have proposed several lattice-based IBE-ET schemes that utilize outdated lattice IBE paradigms and are inefficient in terms of parameter size. In this work, we construct a new lattice-based IBE-ET scheme using the most compact lattice IBE framework known to date. Our new proposal significantly improves the parameters compared to previous constructions. Furthermore, we provide a security reduction in the random oracle model, along with corresponding parameter selection and the comparison between our scheme and known constructions. The results imply that our scheme is efficient.

key words: *Equality test, identity-based encryption, learning with errors.*

1. Introduction

IBE-ET [11] is an IBE scheme that enables users to perform equality test on ciphertexts, allowing the detection of whether different ciphertexts encrypt the same message, where these ciphertexts do not necessarily need to be encrypted under the same user's public key. In this primitive, any recipient can independently compute secret information using their own private key in a one-way manner. They can simply upload the ciphertexts to be tested along with the secret information to a cloud server and delegate it to perform equality test with other ciphertexts. The advantage of this primitive is that it avoids the requirement for a central authority to collect all users' private keys for unified ciphertext equality test, thereby completing the decentralization process. Another advantage is that it significantly enhances the security of the secret key of users. Users do not need to upload their private keys to a central authority, instead, they only provide a delegated trapdoor, which is a one-way function derived from the private key, as auxiliary information for equality test. This means that even if the trapdoor is leaked, the confidentiality of the private key remains intact.

Ma [11] first proposed the syntax and corresponding security model for IBE-ET. Subsequently, he proposed the first IBE-ET scheme based on the Boneh-Franklin IBE [3] framework in the random oracle model, and designed a mechanism for delegating trapdoors (from secret keys) based on the discrete logarithm problem.

To achieve more robust security, Lee et al. [10] first proposed a framework of IBE-ET in the standard model. They used a hierarchical IBE (HIBE) as the encryption algorithm, with the difference being that their ciphertext not only contains the encrypted result of the message, but also the encrypted result of the hashed message. Such a construction undoubtedly has security redundancy, allowing us to prove the security in the standard model. However, it also significantly increases the size of the ciphertext, which leads to low efficiency of the general construction.

In order to instantiate the scheme in the lattice and achieve post-quantum security, based on the work of Lee et al. [10], Duong et al. [6] used a fully secure lattice-based IBE framework [1] and a PKE-ET scheme [5] to construct a lattice-based IBE-ET scheme in the standard model. They improved the idea of using a lattice-based IBE and the framework of Lee et al. to instantiate a lattice-based IBE-ET directly. Instead, the proposed scheme does not employ a "double chain" encryption method, thus effectively reducing the size of the ciphertext. Their proposal only achieved IND-ID-CPA security, and also do not support flexible authorization. Subsequently, Nguyen et al. [14] proposed another lattice-based IBE-ET scheme that supports flexible authorization in the standard model based on the idea of [4] and [6]. Compared with Duong et al. [6] work, their construction can support flexible authorization in the standard model, this gives the users more options in controlling the equality test. However, this comes at the cost of increasing the size of the ciphertexts and keys. In addition, to achieve IND-ID-CCA security, the ciphertext size will be increased even more. Later, Susilo [16] improved the construction of [14] to obtain an efficient IBE-ET construction in the standard model, and achieved a tight reduction. Compared with the previous schemes, their proposal cannot support flexible authorization, but it reduced the size of the public key and ciphertexts by using a more efficient trapdoor sampling algorithm which is introduced by Micciancio and Peikert [12]. This scheme reduces the ciphertext and key size to a certain extent. Based on [1], Yang et al. [17] introduced an even more efficient IBE-ET scheme. Unlike the previous schemes, this scheme reduces the ciphertext size by embedding the hash value of the plaintext into the test trapdoor rather than encrypting it directly, requiring approximately half the storage compared to other lattice-based IBE-ET schemes. It also reduces the execution time for encryption and decryption processes by

[†]The Faculty ...

50%, and maintains a constant computational amount for the test algorithm. However, from other perspectives, although the size of the ciphertext has been reduced to a certain extent and the efficiency has been improved, the size of the key is still relatively large. There is still a significant room for performance improvement compared to the current practical engineering requirements.

To sum up, the above schemes have their own advantages and disadvantages, but their constructions appear to be inefficient. And regardless of whether the framework of Lee et al. is used or not, the above schemes require the trapdoor sampling [2] and basis delegation techniques in [1]. The public key includes a $n \times m$ public matrix, where $m > \lceil 6n \cdot \log\ q \rceil$, wihch is inefficient. Moreover, the trapdoor (or the short basis) can be delegated, but it needs to significantly increase the dimension of underlying lattice. Therefore, the key to improving the efficiency and reducing the storage overhead of lattice-based IBE-ET schemes lies in enhancing the efficiency of trapdoor sampling and delegation algorithms.

1.1 Our Contribution

In this work, we proposed an efficient lattice-based IBE-ET scheme in the random oracle model, which utilized an efficient gadget trapdoor framework proposed by Jia et al.[9]. Compared with the previous schemes constructed based on [1], our new proposal reduces the parameter size and improves computational efficiency. Moreover, we provided concrete parameter selection and comparisons between our work and known constructions. The results show that our scheme is practical.

1.2 Technique Overview

Our construction is based on GPV-IBE framework [8], and employs an efficient preimage sampling algorithm in the process of the extraction of secret keys. We briefly summarized the technique as follows.

We use a compact lattice gadget trapdoor framework [9] which is suitable for IBE which allows us to efficiently sample a short preimage for ISIS instance. They utilized a compact lattice gadget trapdoor framework to implement the key generation algorithm in GPV-IBE, and we briefly describe their gadget trapdoor framework. Given a gadget vector $\mathbf{f} = p \cdot (1, b, \cdots, b^{\beta-1}) \in \mathbb{Z}_Q^{\beta}$ where p is a positive integer, the gadget matrix is $\mathbf{G} = \mathbf{I}_n \otimes \mathbf{f} \mod Q$. The trapdoor is $\mathbf{R} \in \mathcal{D}_{\mathbb{Z}^{2n\times m},r}$ where $m = \beta \cdot n$ ($\beta \geq 2$). Choose $\mathbf{A} \leftarrow \mathbb{Z}_Q^{n\times n}$ uniformly, they defined a new form of public matrix $\mathbf{F} := [\mathbf{I}_n \mid \mathbf{A} \mid \mathbf{G} - (\mathbf{I}_n \mid \mathbf{A})\mathbf{R}] \in \mathbb{Z}_Q^{n\times(m+2n)}$, which is (computationally) indistinguishable from uniform. Then define $\mathbf{T} := \left[\mathbf{R}^{\top} \mid \mathbf{I}_m^{\top}\right]^{\top} \in \mathbb{Z}^{(m+2n)\times m}$, one can check

$$\mathbf{F} \cdot \mathbf{T} = \mathbf{G} = \mathbf{I}_n \otimes \mathbf{f} \mod Q.$$

We note that in the optimal case ($\beta = 2$), the public matrix $\mathbf{F} \in \mathbb{Z}_Q^{n\times 4n}$, and the trapdoor $\mathbf{R} \in \mathbb{Z}^{2n\times 2n}$. Such an improvement in the size of the trapdoor would significantly enhance the efficiency of lattice-based IBE-ET.

Organization. In Section 2, we introduce the lattice background, the syntax and security model of IBE-ET. In Section 3, we give the specific IBE-ET construction, the security reduction and the concrete parameter selection. In Section 4, we summarize the full paper.

2. Preliminaries

2.1 Basic Notations

In this work, bold lowercase letters (e.g. $\mathbf{a}$) are used to represent vectors, and bold uppercase letters (e.g. $\mathbf{A}$) are used to represent matrices. The Euclidean inner product between vectors $\mathbf{a}$ and $\mathbf{b}$ is denoted by $\langle \mathbf{a}, \mathbf{b} \rangle$. The symbol functions $\lfloor \cdot \rfloor$, $\lceil \cdot \rceil$ and $\lfloor \cdot \rceil$ are denoted by rounding down, rounding up and rounding operations, respectively. For the distribution χ, $x \leftarrow \chi$ represents the value x sample from χ uniformly. "Probabilistic Polynomial Time" is abbreviated as "PPT". For positive integer $q > 2$, $\mathbb{Z}_q$ denotes a ring of integers of modulo q.

The transpose of vector $\mathbf{a}$ (matrix $\mathbf{A}$) is represented by $\mathbf{a}^{\top}$ ($\mathbf{A}^{\top}$), respectively. For matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{B} \in \mathbb{Z}_q^{n\times m'}$, $[\mathbf{A} \mid \mathbf{B}] \in \mathbb{Z}_q^{n\times(m+m')}$ is the cascade of $\mathbf{A}$ and $\mathbf{B}$. Let $\otimes$ denote the tensor product and $\mathbf{A} \oplus \mathbf{B}$ denote the block diagonal concatenation of $\mathbf{A}$ and $\mathbf{B}$. For the parameter λ, the negligible function $\mathrm{negl}(\lambda)$ is less than the reciprocal of any polynomial of λ.

2.2 Lattices

Definition 1. *Lattice Λ is the set of all integer-coefficient linear combinations of a set of linearly independent vectors $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ in Euclidean space $\mathbb{R}^m$, i.e*

$$\Lambda = \left\{ \sum_{i=1}^{n} x_i \cdot \boldsymbol{b}_i \mid \forall i = 1, 2, \ldots, n,\ x_i \in \mathbb{Z} \right\},$$

where n is the rank of lattice Λ, the vectors $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ is a set of lattice bases.

If $n = m$ we say the lattice Λ is full-rank lattice. In this paper, we mainly use the integer lattice $\mathbb{Z}_q^m$, which is also called q-ary lattice.

Definition 2. *For matrix $\boldsymbol{A} \in \mathbb{Z}^{n\times m}$ and vector $\boldsymbol{u} \in \mathbb{Z}_q^n$,*

$$\Lambda_q(\boldsymbol{A}) = \left\{ \boldsymbol{e} \in \mathbb{Z}^m \mid \exists \boldsymbol{s} \in \mathbb{Z}_q^n, \boldsymbol{A}^{\top}\boldsymbol{s} = \boldsymbol{e} \mod q \right\},$$
$$\Lambda_q^{\perp}(\boldsymbol{A}) = \left\{ \boldsymbol{e} \in \mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{e} = \boldsymbol{0} \mod q \right\},$$
$$\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}) = \left\{ \boldsymbol{e} \in \mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{e} = \boldsymbol{u} \mod q \right\}.$$

If $\mathbf{t} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$, then $\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \Lambda_q^{\perp}(\mathbf{A}) + \mathbf{t}$. Therefore, $\Lambda_q^{\mathbf{u}}(\mathbf{A})$ can be seen as a coset of $\Lambda_q^{\perp}(\mathbf{A})$.

2.3 Discrete Gaussian

For a parameter $r > 0$ and a vector $\mathbf{x}$ chosen from $\mathbb{R}^n$ randomly, define the following function over $\mathbb{R}^n$ as

$$\rho_{r,\mathbf{c}}(\mathbf{x}) := \exp\left(\frac{-\pi\|\mathbf{x}-\mathbf{c}\|^2}{r^2}\right)$$

where $\mathbf{c}$ is the center. We remark that r and $\mathbf{c}$ are omitted when the value of the two parameters equal 1 and $\mathbf{0}$ respectively. For a lattice Λ with dimension n and a vector $\mathbf{x}$ chosen from Λ randomly, the *discrete Gaussian* distribution over Λ is:

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

For $\mathbb{Z}^m$ with dimension m and a vector $\mathbf{x}$ chosen from $\mathbb{Z}^m$ randomly, the *discrete Gaussian* distribution over $\mathbb{Z}^m$ is:

$$\mathcal{D}_{\mathbb{Z}^m,r,\mathbf{c}}(\mathbf{x}) := \frac{\rho_{r,\mathbf{c}}(\mathbf{x})}{\rho_{r,\mathbf{c}}(\mathbb{Z}^m)} = \frac{\rho_{r,\mathbf{c}}(\mathbf{x})}{\sum_{\mathbf{y}\in\mathbb{Z}^m}\rho_{r,\mathbf{c}}(\mathbf{y})}.$$

The *discrete Gaussian* distribution over $\mathbb{Z}^{n\times m}$ is taking m integer vectors in $\mathcal{D}_{\mathbb{Z}^n,r,\mathbf{c}}$ as the columns in the matrix of $\mathbb{Z}^{n\times m}$.

Definition 3. ([13, *Definition* 3.1]) *For any n-dimensional lattice Λ and positive real ϵ>0, the smoothing parameter $\eta_\epsilon(\Lambda)$ is the smallest real r>0 such that $\rho_{1/r}(\Lambda^* - \{\mathbf{0}\}) \le \epsilon$.*

2.4 LWE Problem

In this subsection we introduce learning with errors (LWE) problem, which is proposed by Regev [15]. For noise distribution χ and vector $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathcal{A}_{\mathbf{s},\chi}$ is the LWE distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, take $\mathbf{u} \leftarrow \mathbb{Z}_q^n$ and $e \leftarrow \chi$, and output $(\mathbf{u}, \mathbf{u}^\top\mathbf{s}+e)$ mod q. In general, in the case of modulo q, χ is the discrete Gaussian $\mathcal{D}_{\mathbb{Z},\alpha q}$, for some α<1.

Definition 4. *For $q \ge 2$ and some suitable parameters n, and some distribution χ (discrete Gaussian distribution), the decision-LWE is stated as follows:*
(1) Given the pair $(\boldsymbol{u}, \boldsymbol{u}^\top\mathbf{s}+e)$, where $\boldsymbol{u} \in \mathbb{Z}_q^n$ is chosen uniformly, $\mathbf{s} \in \mathbb{Z}_q^n$ is a uniformly random vector and $\mathbf{e} \in \chi$ is sampled from discrete Gaussian distribution.
(2) Given another pair $(\boldsymbol{u}, v)$, where $\boldsymbol{u}$ is chosen uniformly random from $\mathbb{Z}_q^n$ and $v \in \mathbb{Z}_q$ is a uniformly-random value.
The decision-LWE problem (we called $LWE_{n,q,\chi}$) is to distinguish the two cases.

2.5 IBE-ET System Model

In this subsection, we review the IBE-ET model and its security model.

- $(mpk,\ msk) \leftarrow \mathbf{Setup}(1^n)$: It generates and returns master public key mpk and master secret key msk.
- $usk_{id} \leftarrow \mathbf{Extract}(mpk, msk, id)$: Give mpk, msk and id, it generates and returns a user secret key usk_{id}.
- $\mathbf{CT}_{id} \leftarrow \mathbf{Enc}(mpk, id, \mathbf{m})$: It encrypts a user plaintext $\mathbf{m}$ with mpk and outputs the ciphertext as $\mathbf{CT}_{id}$.
- $\mathbf{m}' \leftarrow \mathbf{Dec}(mpk, usk_{id}, \mathbf{CT}_{id})$: It is to decrypt a ciphertext $\mathbf{CT}_{id}$ with usk_{id} and mpk and output a plaintext $\mathbf{m}$ or $\perp$.
- $\mathbf{td}_{id} \leftarrow \mathbf{Trap}(mpk, usk_{id}, \mathbf{CT}_{id})$: With $\mathbf{CT}_{id}$, usk_{id} and mpk, this algorithm generates and returns a testing trapdoor $\mathbf{td}_{id}$.
- 0 or 1 $\leftarrow$ $\mathbf{Test}(\mathbf{td}_{id}, \mathbf{CT}_{id}, \mathbf{td}_{id'}, \mathbf{CT}_{id'})$: Given $(\mathbf{CT}_{id}, \mathbf{td}_{id})$ and $(\mathbf{CT}_{id'}, \mathbf{td}_{id'})$ from two different users, it outputs 1 if the underlying plaintexts of $\mathbf{CT}_{id}$ and $\mathbf{CT}_{id'}$ are the same. Otherwise, it returns 0.

Correctness. We say that the IBE-ET scheme is correct if the following conditions are true:

1. If $usk_{id} \leftarrow \mathbf{Extract}(mpk, msk, id)$ and $\mathbf{m}$ is a plaintext within the message space, the equation
$$\mathbf{Dec}(mpk, usk_{id}, \mathbf{Enc}(mpk, id, \mathbf{m})) = \mathbf{m}$$
will hold with overwhelm probability.
2. Suppose we have two distinct users, id and id', and $\mathbf{m} \leftarrow \mathcal{M}$, we obtian $\mathbf{CT}_{id} \leftarrow \mathbf{Enc}(mpk, id, \mathbf{m})$ and $\mathbf{td}_{id} \leftarrow \mathbf{Trap}(mpk, usk_{id}, \mathbf{CT}_{id})$, where $usk_{id} \leftarrow \mathbf{Extract}(mpk, msk, id)$. The same process generates $(\mathbf{CT}_{id'}, \mathbf{td}_{id'})$ for another set of values. Then the equation
$$\mathbf{Test}(\mathbf{td}_{id}, \mathbf{CT}_{id}, \mathbf{td}_{id'}, \mathbf{CT}_{id'}) = 1$$
will hold with overwhelm probability.
3. $\mathbf{m}$ and $\mathbf{m}'$ are two distinct messages and $\mathbf{CT}_{id} \leftarrow \mathbf{Enc}(mpk, id, \mathbf{m})$, $\mathbf{CT}_{id'} \leftarrow \mathbf{Enc}(mpk, id', \mathbf{m}')$. The equation
$$\mathbf{Test}(\mathbf{td}_{id}, \mathbf{CT}_{id}, \mathbf{td}_{id'}, \mathbf{CT}_{id'}) = 1$$
will hold with negligible probability.

Security Model. To assess the IBE-ET scheme's resistance to various security threats, we examine its ability to maintain the indistinguishability of encrypted tags from statistical noise under a chosen-plaintext attack. In this scenario, a PPT adversary $\mathcal{A}$ seeks to determine which specific plaintext was encrypted into the challenge ciphertext $\mathbf{CT}$ by engaging in interactions with the challenger C. It is assumed that adversary $\mathcal{A}$ is targeting a particular user id_θ. Given this intention, the PPT adversary $\mathcal{A}$ will proceed as follows:

1. **Setup**: The challenger C runs the algorithm $\mathbf{Setup}(1^n)$ and then receives mpk and msk. C forwards mpk to $\mathcal{A}$, while keeping msk.
2. **Phase1**: Adversary $\mathcal{A}$ can perform the following classical queries polynomial times in arbitrary order.
   - $O^{\mathbf{Ext}}$: Enter the user $id \ne id_\theta$, $O^{\mathbf{Ext}}$ outputs the user U_i secret key usk_{id}.
   - $O^{\mathbf{Td}}$: Enter the user $id \ne id_\theta$, $O^{\mathbf{Td}}$ outputs the user U_i tag $\mathbf{td}_{id}$.
3. **Challenge**: The adversary $\mathcal{A}$ takes two more messages $\mathbf{m}_0$ and $\mathbf{m}_1$ of the same length and sends to C, then C chooses random bit $b \in \{0,1\}$, finally returns $\mathbf{CT}_\theta \leftarrow \mathbf{Enc}(mpk_\theta, id_\theta, \mathbf{m}_b)$ to $\mathcal{A}$.
4. **Phase 2**: This stage of query is same as **Phase 1**, except that $\mathcal{A}$ cannot query user U_θ with oracles $O^{\mathbf{Ext}}$ and $O^{\mathbf{Td}}$.

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

The PPT adversary $\mathcal{A}$ is said to win the IND-sID-CPA game when $b = b^{'}$. Therefore, the security of IBE-ET scheme against PPT adversary is formally described below.
An IBE-ET scheme is secure under IND-sID-CPA attack if $\mathcal{A}$ wins the above game with advantage

$$\mathrm{Adv}^{\text{IND-sID-CPA}}_{\mathcal{A},\text{IBE-ET}} = \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|,$$

and it is negligible.

2.6 Dual Regev PKE and GPV-IBE Framework

We recall the dual version of Regev-PKE scheme, which is proposed by Gentry, Peikert and Vaikuntanathan[8], and it is well-suited for the construction of lattice-based IBE.

Given a share matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ chosen uniformly at random, which is the index of the function $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{Ae} \mod q$, where the function is a one-way function with trapdoor [8, Theorem 4.9]. All operations are performed over $\mathbb{Z}_q$.

- **DualKeyGen**: Choose an error vector $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,r}$ (i.e., the input distribution to $f_{\mathbf{A}}$), which is the secret key. The public key is $\mathbf{u} = f_{\mathbf{A}}(\mathbf{e})$.
- **DualEnc**$(\mathbf{u}, b)$: To encrypt a bit $b \in \{0,1\}$, choose $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ uniformly. Output the ciphertext $(\mathbf{c}_1 = \mathbf{A}^\top\mathbf{s} + \mathbf{x} \in \mathbb{Z}_q^m, c_2 = \mathbf{u}^\top\mathbf{s}+x+b\lfloor\frac{q}{2}\rceil) \in \mathbb{Z}_q^m\times\mathbb{Z}_q$, where $\mathbf{x} \leftarrow \chi^m$ and $x \leftarrow \chi$.
- **DualDec**$(\mathbf{e}, (\mathbf{c}_1, c_2))$: Compute $b^{'} = c_2 - \mathbf{e}^\top\mathbf{c}_1 \in \mathbb{Z}_q$. Output 0 if $b^{'}$ is closer to 0 than to $\lfloor\frac{q}{2}\rceil \mod q$, otherwise output 1.

Theorem 1. ([8, *Theorem* 7.1]) *Suppose* $q \geq 5r(m+1)$, $\alpha \leq \frac{1}{r\sqrt{m+1}\cdot\omega(\sqrt{\log n})}$ *and* $\chi = \overline{\Psi}_\alpha$, *and let* $m \geq 2n\log q$. *Then the dual cryptosystem is IND-CPA secure, assuming that LWE* $_{n,m,q,\chi}$ *is hard.*

GPV-IBE System. The IBE system uses a random oracle $H : \{0,1\}^* \to \mathbb{Z}_q^n$ that maps identities to public keys of the dual cryptosystem, which is instantiated with a Gaussian parameter $r \geq L\cdot\omega(\sqrt{\log m})$ so as to guarantee the preimage sampling property as proved in [8, Theorem 4.9].

- **IBESetup**(1^n): Generating $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a short basis $\mathbf{S}$ of $\Lambda_q^\perp(\mathbf{A})$. The master public key is $\mathbf{A}$, which is taken as the shared matrix for the dual cryptosystem, and the master secret key is $\mathbf{S}$.
- **IBEExtract**$(\mathbf{A}, \mathbf{S}, id)$: If the pair $(id, \mathbf{e})$ is in local storage (from a prior query on id), then return $\mathbf{e}$. Otherwise, let $\mathbf{u} = H(id)$ and choose a decryption key $\mathbf{e} \leftarrow f_{\mathbf{A}}^{-1}(\mathbf{u})$ using the preimage sampler with trapdoor $\mathbf{S}$. Store $(id, \mathbf{e})$ locally and return $\mathbf{e}$.
- **IBEEnc**$(\mathbf{A}, id, b)$: To encrypt a bit $b \in \{0,1\}$ to identity id, let $\mathbf{u} = H(id) \in \mathbb{Z}_q^n$, and output a ciphertext $(\mathbf{c}_1, c_2) \leftarrow$ **DualEnc**$(\mathbf{u}, b)$.
- **IBEDec**$(\mathbf{e}, (\mathbf{c}_1, c_2))$: Output **DualDec**$(\mathbf{e}, (\mathbf{c}_1, c_2))$.

Theorem 2. ([8, *Theorem* 7.2]) *Suppose the dual cryptosystem is IND-CPA-secure in the standard model, and that its public keys are statistically close to uniform over* $\mathbb{Z}_q^n$ *for all but a negligible fraction of shared matrices* $\mathbf{A}$. *Then the IBE system described above is IND-CPA-secure in the random oracle model.*

3. Proposed Lattice-based IBE-ET

3.1 Approximate gadget trapdoor framework

In this subsection, we recall the preimage sampling algorithm proposed by Jia et al.[9]. First, we introduce the gadget trapdoor. Their gadget works with a composite modulus $Q = pq$ where p, q are positive integers. In more detail, b is a small integer, $\beta = \lceil\log_b q\rceil$, $m = \beta n$ and $\mathbf{g} = (1, b, \ldots, b^{\beta-1})$. Given a target $\mathbf{V} \in \mathbb{Z}_Q^{n\times n}$, the sampler outputs some $\mathbf{Z} \in \mathcal{D}_{\mathbb{Z}^{m\times n},r}$ following discrete Gaussian such that $\mathbf{G}\cdot\mathbf{Z} = \mathbf{V} - \mathbf{E} \mod Q$ for some small $\mathbf{E} \in \mathbb{Z}_p^n$, where $\mathbf{G} = \mathbf{I}_n \otimes \mathbf{f} \mod Q$ is the gadget matrix in the sampler. The bijection $\tau : \mathbb{Z}_Q^{n\times n} \to \mathbb{Z}_p^{n\times n} \times \mathbb{Z}_q^{n\times n}$ is defined by $\tau(\mathbf{V}) = (\mathbf{V}_p, \mathbf{V}_q)$ such that $\mathbf{V} = p\mathbf{V}_q + \mathbf{V}_p$. In detail, for $i, j = 1, 2, \ldots, n$, $\mathbf{V}^{i,j} = p\mathbf{V}_q^{i,j} + \mathbf{V}_p^{i,j}$. The primary objective of the algorithm outlined below is to treat the remainder $\mathbf{V}_p$ as a deterministic approximation error $\mathbf{E}$, and then to sample $\mathbf{Z}$ from the coset $\Lambda_{\mathbf{V}_q}^\perp(\mathbf{B}^\top)$.

Algorithm 3.1 ApproxGadget$(\mathbf{V}, r, p, q)$

Input: a target $\mathbf{V} \in \mathbb{Z}_Q^{n\times n}$, a positive real $r>0$ and integers $p, q>0$ with $Q = pq$;
Output: a matrix $\mathbf{Z} \sim \mathcal{D}_{\mathbb{Z}^{m\times n},r}$ conditioned on $\mathbf{G}\cdot\mathbf{Z} = \mathbf{V} - \mathbf{E} \mod Q$ for some $\mathbf{E} \in \mathbb{Z}_p^{n\times n}$.
1: $(\mathbf{V}_p, \mathbf{V}_q) \leftarrow \tau(\mathbf{V})$
2: sample $\mathbf{Z} \leftarrow \mathcal{D}_{\Lambda_{\mathbf{V}_q}^\perp(\mathbf{B}^\top),r}$, $\mathbf{B} = \mathbf{I}_n \otimes \mathbf{g} \mod Q$
3: **return Z**

Lemma 1. *Algorithm 3.1 is correct. More precisely, let* $p, q>0$ *be integers,* $Q = pq, r>0$ *and* $\boldsymbol{V} \in \mathbb{Z}_Q^{n\times n}$ *such that* $\tau(\boldsymbol{V}) = (\boldsymbol{V}_p, \boldsymbol{V}_q)$. *Then* ***ApproxGadget***$(\boldsymbol{V}, r, p, q)$ *outputs* $\boldsymbol{Z}$ *such that* $\boldsymbol{Z} \sim \mathcal{D}_{\mathbb{Z}^{m\times n},r}$ *and* $\boldsymbol{G}\cdot\boldsymbol{Z} = \boldsymbol{V} - \boldsymbol{T}_p \mod Q$.

Let $\Gamma = (n, m, p, q, Q, \chi)$ denote the global parameters where $Q = pq$, $m = \beta n$ and χ is the distribution of secrets. We set $\Sigma>0$, when a symmetric matrix $\Sigma \in \mathbb{R}^{n\times n}$ is positive definite. When the context allows, we use $\sqrt{\Sigma}$ to represent any square root of Σ. In the following, let $\Sigma = \sigma_1^2\cdot\mathbf{I}\oplus\sigma_2^2\cdot\mathbf{I}$ and $\Sigma_{\mathbf{P}} = \Sigma - r^2\cdot\mathbf{T}\cdot\mathbf{T}^\top$, where σ_1 and σ_2 are standard deviation of the preimage. Let $\mathbf{F} \in \mathbb{Z}_Q^{n\times(m+2n)}$ be a public matrix. The approximate trapdoor for $\mathbf{F}$ is a matrix $\mathbf{T} \in \mathbb{Z}^{(m+2n)\times m}$, they are defined as follows $\mathbf{F} := [\mathbf{I}_n \mid \mathbf{A} \mid \mathbf{G} - (\mathbf{I}_n \mid \mathbf{A})\mathbf{R}]$, $\mathbf{T} := \left[\mathbf{R}^\top \mid \mathbf{I}_m^\top\right]^\top$, and $\mathbf{F}\cdot\mathbf{T} = \mathbf{G} = \mathbf{I}_n \otimes \mathbf{f} \mod Q$, where $\mathbf{G}$ is the gadget matrix, $\mathbf{A} \leftarrow \mathbb{Z}_Q^{n\times n}$ uniformly, and $\mathbf{R} \leftarrow \mathcal{D}_{\mathbb{Z}^{2n\times m},r}$ uniformly random.

Algorithm 3.2 ApproxPreSamp$(\mathbf{F}, \mathbf{T}, \mathbf{U}, r, \Sigma)$

Input: $(\mathbf{F}, \mathbf{T}) \in \mathbb{Z}_Q^{n\times(m+2n)} \times \mathbb{Z}_Q^{(m+2n)\times n}$ such that $\mathbf{F}\cdot\mathbf{T} = \mathbf{G} \mod Q$, a matrix $\mathbf{U} \in \mathbb{Z}_Q^{n\times n}$, $r \geq \eta_\epsilon(\Lambda_q^\perp(\mathbf{B}^\top))$ and Σ such that $\Sigma_{\mathbf{P}}>0$;
Output: an approximate preimage $\mathbf{Y}$ of $\mathbf{U}$ for $\mathbf{F}$.

1: $\mathbf{P} \leftarrow \mathcal{D}_{\mathbb{Z}^{(m+2n)\times n}, \sqrt{\Sigma_{\mathbf{P}}}}$
2: $\mathbf{V} = \mathbf{U} - \mathbf{F}\cdot\mathbf{P} \mod Q$
3: $\mathbf{Z} \leftarrow$ **ApproxGadget**$(\mathbf{V}, r, p, q)$
4: **return** $\mathbf{Y} = \mathbf{P} + \mathbf{T}\cdot\mathbf{Z}$

In the foundation of Algorithm 3.1, Jia et al. proposed another algorithm (Algorithm 3.2) whose inputs a public matrix $\mathbf{F}$, an approximate trapdoor $\mathbf{T}$ of $\mathbf{F}$, a target $\mathbf{U}$, and Gaussian parameters r and outputs an approximate preimage $\mathbf{Y}$ such that

$$\mathbf{F}\cdot\mathbf{Y} = \mathbf{F}\cdot\mathbf{P}+\mathbf{F}\cdot\mathbf{T}\cdot\mathbf{Z} = \mathbf{F}\cdot\mathbf{P}+\mathbf{G}\cdot\mathbf{Z} = \mathbf{F}\cdot\mathbf{P}+\mathbf{V}-\mathbf{E} = \mathbf{U}-\mathbf{E} \mod Q.$$

3.2 Lattice-based IBE-ET in the Random Oracle

Our IBE system uses a random orace $H : \{0,1\}^* \to \mathbb{Z}_Q^{n\times n}$ that maps identities to public keys of the dual cryptosystem.

- **Setup**(1^n): Takes as input n as the security parameter:
  1. Choose a matrix $\mathbf{A} \in \mathbb{Z}_Q^{n\times n}$ randomly.
  2. Sample $\mathbf{R} \leftarrow \mathcal{D}_{\mathbb{Z}^{2n\times m}, r}$.
  3. $H^{'}$ is a random permutation over $\{0,1\}^n$.
  4. Return mpk as $\mathbf{F} = [\mathbf{I}_n \mid \mathbf{A} \mid \mathbf{G} - (\mathbf{I}_n \mid \mathbf{A})\mathbf{R}] \in \mathbb{Z}_Q^{n\times(m+2n)}$ and msk as $\mathbf{T} = \left[\mathbf{R}^\top \mid \mathbf{I}_m^\top\right]^\top \in \mathbb{Z}_Q^{(m+2n)\times m}$.
- **Extract**(mpk, msk, id): With $id \in \{0,1\}^*$, mpk and msk:
  1. Sample a short approximate preimage $\mathbf{Y}^{'} \leftarrow$ **ApproxPreSamp**$(\mathbf{F}, \mathbf{T}, \mathbf{U}, r, \Sigma)$ such that
  $$\mathbf{F}\cdot\mathbf{Y}^{'} = \mathbf{U} - \mathbf{E} \mod Q$$
  for some small $\mathbf{E} \in \mathbb{Z}_Q^{n\times n}$, where $\mathbf{U} = H(id)$.
  2. Write
  $$\mathbf{Y}^{'} = \begin{bmatrix}\mathbf{Y}_1\\ \mathbf{Y}_2\\ \mathbf{Y}_3\end{bmatrix},$$
  where $\mathbf{Y}_1 \in \mathbb{Z}_Q^{n\times n}, \mathbf{Y}_2 \in \mathbb{Z}_Q^{n\times n}$ and $\mathbf{Y}_3 \in \mathbb{Z}_Q^{m\times n}$, construct $\mathbf{Y}$ such that $\mathbf{F}\cdot\mathbf{Y} = \mathbf{U} \mod Q$, where
  $$\mathbf{Y} = \begin{bmatrix}\mathbf{Y}_1 + \mathbf{E}\\ \mathbf{Y}_2\\ \mathbf{Y}_3\end{bmatrix}.$$
  3. Return the user secret key usk_{id} as $\mathbf{Y} \in \mathbb{Z}_Q^{(m+2n)\times n}$.
- **Enc**$(mpk, id, \mathbf{m})$: With $\mathbf{m}, id$ and mpk:
  1. Sample vector $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ from $\mathbb{Z}_Q^n$ randomly where the first component s_1 is a nonzero integer.
  2. Sample vectors $\mathbf{e}_1 \leftarrow \chi^{m+2n}$ and $\mathbf{e}_2 \leftarrow \chi^n$ randomly.
  3. Compute
  $$\begin{cases}\mathbf{c}_1 = \mathbf{F}^\top\mathbf{s} + \mathbf{e}_1 \in \mathbb{Z}_Q^{m+2n}\\ \mathbf{c}_2 = \mathbf{U}^\top\mathbf{s} + \mathbf{e}_2 + \mathbf{m}\lfloor\frac{Q}{2}\rceil \in \mathbb{Z}_Q^n.\end{cases}$$
  4. Output the ciphertext $\mathbf{CT}_{id}$ as $(\mathbf{c}_1, \mathbf{c}_2, s_1)$.
- **Dec**$(mpk, usk_{id}, \mathbf{CT}_{id})$: With mpk, usk_{id} and $\mathbf{CT}_{id}$:
  1. Compute
  $$\mathbf{w} = \mathbf{c}_2 - \mathbf{Y}^\top\mathbf{c}_1 = \mathbf{m}\lfloor\frac{Q}{2}\rceil + \mathbf{e}_2 - \mathbf{Y}^\top\mathbf{e}_1 \in \mathbb{Z}_Q^n.$$
  2. For $i = 1, \ldots, n$, set $m_i = 0$ if the value $|w_i - \lfloor\frac{Q}{2}\rceil| \leq \lfloor\frac{Q}{4}\rfloor$, otherwise $m_i = 1$.
  3. Output the plaintext as $\mathbf{m}$.
- **Trap**$(mpk, usk_{id}, \mathbf{CT}_{id}, H^{'}(\mathbf{m}))$: With mpk, usk_{id}, $\mathbf{CT}_{id}$ and $H^{'}(\mathbf{m})$:
  1. Phrase $H^{'}(\mathbf{m}) = (H^{'}(\mathbf{m})_1, H^{'}(\mathbf{m})_2, \ldots, H^{'}(\mathbf{m})_n) \in \{0,1\}^n$.
  2. For $j = 1, 2, \ldots, n$, compute $v_j = H^{'}(\mathbf{m})_j \cdot \lfloor\frac{Q}{2}\rceil \cdot s_1^{-1} \mod Q$.
  3. Let $\mathbf{V}$ be a matrix in $\mathbb{Z}_Q^{n\times n}$ with
  $$\mathbf{V} = \begin{pmatrix} v_1 & v_2 & v_3 & \cdots & v_n\\ 0 & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & 0\end{pmatrix} \in \mathbb{Z}_Q^{n\times n}.$$
  4. Sample a short approximate preimage $\mathbf{X}^{'} \leftarrow$ **ApproxPreSamp**$(\mathbf{F}, \mathbf{T}, \mathbf{V}, r, \Sigma)$ such that $\mathbf{F}\cdot\mathbf{X}^{'} = \mathbf{V} - \mathbf{E}^{'} \mod Q$ for some small $\mathbf{E}^{'} \in \mathbb{Z}_Q^{n\times n}$.
  5. We set
  $$\mathbf{X}^{'} = \begin{bmatrix}\mathbf{X}_1\\ \mathbf{X}_2\\ \mathbf{X}_3\end{bmatrix},$$
  where $\mathbf{X}_1 \in \mathbb{Z}_Q^{n\times n}, \mathbf{X}_2 \in \mathbb{Z}_Q^{n\times n}$ and $\mathbf{X}_3 \in \mathbb{Z}_Q^{m\times n}$. Then $\mathbf{F}\cdot\mathbf{X} = \mathbf{V} \mod Q$, where
  $$\mathbf{X} = \begin{bmatrix}\mathbf{X}_1 + \mathbf{E}^{'}\\ \mathbf{X}_2\\ \mathbf{X}_3\end{bmatrix}.$$
  6. Output the testing trapdoor $\mathbf{td}_{id}$ as $\mathbf{X} \in \mathbb{Z}_Q^{(m+2n)\times n}$.
- **Test**$(\mathbf{td}_{id}, \mathbf{CT}_{id}, \mathbf{td}_{id'}, \mathbf{CT}_{id'})$: Given ciphertexts $\mathbf{CT}_{id}, \mathbf{CT}_{id'}$ from two different users and related trapdoors $\mathbf{td}_{id}, \mathbf{td}_{id'}$:
  1. Phrases $\mathbf{CT}_{id} = (\mathbf{c}_1, \mathbf{c}_2, s_1), \mathbf{td}_{id} = \mathbf{X}_{id}$ and $\mathbf{CT}_{id'} = (\mathbf{c}_1^{'}, \mathbf{c}_2^{'}, s_1^{'}), \mathbf{td}_{id'} = \mathbf{X}_{id'}$.
  2. Compute $\bar{\mathbf{w}} = \mathbf{X}_{id}^\top \cdot \mathbf{c}_1$ and $\bar{\mathbf{w}}^{'} = \mathbf{X}_{id'}^\top \cdot \mathbf{c}_1^{'}$.
  3. For $i = 1, 2, \ldots, n$, set $\bar{\mathrm{m}}_i = 0$ if the value $\left|\bar{\mathrm{w}}_i - \lfloor\frac{Q}{2}\rceil\right|$ is less to $\frac{Q}{4}$ and $\bar{\mathrm{m}}_i = 1$ otherwise.

The vector $\bar{\mathbf{m}}^{'}$ is generated in the similar way.

4. Output 1 if $\bar{\mathbf{m}} = \bar{\mathbf{m}}^{'}$ and 0 otherwise.

3.3 Correctness

Theorem 3. *Assuming that the above $H^{'}$ is collision resistant and the appropriate relevant parameters are selected, the newly constructed IBE-ET scheme is correct.*

Proof. First of all, we state that the **Decryption** algorithm is correct. When $\mathbf{w}$ is generated as described above, we can get

$$\mathbf{w} = \mathbf{c}_2 - \mathbf{Y}^{\top}\mathbf{c}_1 = \mathbf{m}\lfloor\frac{Q}{2}\rceil + \mathbf{e}_2 - \mathbf{Y}^{\top}\mathbf{e}_1 \in \mathbb{Z}_Q^n,$$

where $\mathbf{e}_2 - \mathbf{Y}^{\top}\mathbf{e}_1$ is the error term. In order to decrypt correctly, we need $\left|\mathbf{e}_2 - \mathbf{Y}^{\top}\mathbf{e}_1\right| < \lfloor\frac{Q}{4}\rceil$, we choose $Q > 5r(m+1)$, and the standard deviation α of $LWE_{n,m+2n,Q,\chi}$ satisfies

$$\alpha \leq 1/(r(m+2n+1)\omega(\sqrt{\log n})).$$

In this case, the **Decryption** algorithm can always return the correct plaintext $\mathbf{m}$.

Second, during the equality test, when $\bar{\mathbf{w}}$ is generated as described above, we can get

$$\bar{\mathbf{w}} = \mathbf{X}^{\top} \cdot \mathbf{c}_1 = H(\mathbf{m})^{'}\lfloor\frac{Q}{2}\rceil + \mathbf{X}^{\top}\mathbf{e}_1 \in \mathbb{Z}_Q^n.$$

The distribution of $\mathbf{X}^{\top}$ is identical to $\mathbf{Y}^{\top}$, the norm of $\mathbf{X}^{\top}\mathbf{e}_1$ will be less to $\lfloor\frac{Q}{4}\rceil$ under the same parameters. Therefore, the vector $\bar{\mathbf{m}}$ calculated in the **Test** algorithm is equivalent to $H^{'}(\mathbf{m})$. The same goes for vector $\bar{\mathbf{m}}^{'}$, which is the same as $H^{'}(\mathbf{m}^{'})$. Because $H^{'}$ is a collision resistant hash function, the equation $\bar{\mathbf{m}} = \bar{\mathbf{m}}^{'}$ holds if and only if $\mathbf{m} = \mathbf{m}^{'}$. □

3.4 Security

To begin with, we introduce the following theorem.

Theorem 4. ([9, *Theorem* 2]) *Let $(\boldsymbol{F}, \boldsymbol{T})$ be a matrix-approximate trapdoor pair, $\boldsymbol{C} = \begin{pmatrix}\boldsymbol{T}\\ \boldsymbol{I}\end{pmatrix}$ and (r, Σ) such that $\sqrt{\Sigma_p \oplus r^2\boldsymbol{I}} > \eta_\epsilon(\mathcal{L}(\boldsymbol{C}))$. Denote by $\boldsymbol{F}^{-1}(\cdot)$ the shorthand of **ApproxPreSamp**$(\boldsymbol{F}, \boldsymbol{T}, \cdot, r, \Sigma)$. Then the following two distributions are statistically indistinguishable:*

1. $(\boldsymbol{F}, \boldsymbol{X}, \boldsymbol{U}, \boldsymbol{E}) : \boldsymbol{U} \leftarrow \mathcal{U}(\mathbb{Z}_Q^{n\times n}), \boldsymbol{X} \leftarrow \boldsymbol{F}^{-1}(\boldsymbol{U}), \boldsymbol{E} = \boldsymbol{U} - \boldsymbol{F}\cdot\boldsymbol{X} \mod Q$.
2. $(\boldsymbol{F}, \boldsymbol{X}, \boldsymbol{U}, \boldsymbol{E}) : \boldsymbol{X} \leftarrow \mathcal{D}_{\mathbb{Z}^{(m+2n)\times n}, \sqrt{\Sigma}}, \boldsymbol{E} \leftarrow \mathcal{U}(\mathbb{Z}_p^{n\times n}), \boldsymbol{U} = \boldsymbol{F}\cdot\boldsymbol{X} + \boldsymbol{E} \mod Q$.

Theorem 5. *Let IBE-ET be the scheme proposed above and $H^{'}$ be collision resistant. If the $LWE_{n,m+2n,Q,\chi}$ assumption holds, then the IBE-ET is IND-sID-CPA secure in the random oracle model.*

Proof. We define a series of game sequence and prove that adjacent games are indistinguishable.

Game 0: This is the original IND-sID-CPA game, all the algorithms are the same as the original scheme. This game is an interaction between a PPT adversary $\mathcal{A}$ and a IND-sID-CPA challenger C.

Game 1: The challenger C in *Game* 0 gets outputs of **Setup** algorithm and sends the master public key mpk to the adversary $\mathcal{A}$, while keeping the master secret key. The challenger first randomly samples a matrix $\mathbf{Y}^{'}$ from $\mathcal{D}_{\mathbb{Z}^{(m+2n)\times n}, \sqrt{\Sigma}}$, a matrix $\mathbf{E}$ from $\mathcal{U}(\mathbb{Z}_p^{n\times n})$ and $\mathbf{U} = \mathbf{F}\cdot\mathbf{Y}^{'} + \mathbf{E} \mod Q$, then $\mathbf{Y}$ is calculated using $\mathbf{Y}^{'}$ and $\mathbf{E}$ in the same way as *Game* 0 and answers the queries issued by the adversary. The rest part of *Game* 1 keeps the same to *Game* 0. Therefore, the way in which the user's private key usk_{id} is generated in *Game* 0 is different from that in *Game* 1. From Theorem 4, it can be seen that $(\mathbf{F}, \mathbf{Y}^{'}, \mathbf{U}, \mathbf{E}) : \mathbf{U} \leftarrow \mathcal{U}(\mathbb{Z}_Q^{n\times n}), \mathbf{Y}^{'} \leftarrow \mathbf{F}^{-1}(\mathbf{U}), \mathbf{E} = \mathbf{U} - \mathbf{F}\cdot\mathbf{Y}^{'} \mod Q$ and $(\mathbf{F}, \mathbf{Y}^{'}, \mathbf{U}, \mathbf{E}) : \mathbf{Y}^{'} \leftarrow \mathcal{D}_{\mathbb{Z}^{(m+2n)\times n}, \sqrt{\Sigma}}, \mathbf{E} \leftarrow \mathcal{U}(\mathbb{Z}_p^{n\times n}), \mathbf{U} = \mathbf{F}\cdot\mathbf{Y}^{'} + \mathbf{E} \mod Q$ are statistically indistinguishable. In this case, *Game* 0 and *Game* 1 can not be distinguished by $\mathcal{A}$ with non-negligible advantage.

Game 2: Let $(\mathbf{c}_{1\theta}, \mathbf{c}_{2\theta}, s_{1\theta})$ be challenge ciphertext in *Game* 2, which changes into random independent element in $\mathbb{Z}_Q^{m+2n} \times \mathbb{Z}_Q^n \times \mathbb{Z}_Q^*$. The rest part of this game remains unchanged. In this case, the advantage of winning the IND-sID-CPA game is equal to the advantage of guessing the plaintext $\mathbf{m}$ correctly, which is exactly $\frac{1}{2^n}$ and hence negligible.

To finish the proof, one should show that any PPT adversary can not distinguish *Game* 1 from *Game* 2. Otherwise, the LWE problem can be solved.

Reduction From LWE. Assuming that a PPT algorithm $\mathcal{A}^*$ has the ability to distinguish *Game* 1 from *Game* 2 with non-negligible probability, one can construct an efficient LWE problem solver $\mathcal{B}$ by taking $\mathcal{A}^*$ as a subroutine. Particularly, given $3n+m$ samples $(\mathbf{u}_i^{'}, v_i^{'}) \in \mathbb{Z}_Q^{n-1} \times \mathbb{Z}_Q$, the LWE problem is to determine if they are sampled from $A_{\mathbf{s},\chi}$ for some fixed secret $\mathbf{s} \in \mathbb{Z}_Q^{n-1}$ or a truly random oracle. With the algorithm $\mathcal{A}^*$, it is assumed that adversary $\mathcal{A}^*$ is targeting a particular user id_θ, the algorithm $\mathcal{B}$ processes as follows:

For $i = 1, 2, \ldots, m, m+1, \ldots, m+3n$, let $(\mathbf{u}_i, v_i) \in \mathbb{Z}_Q^{n-1} \times \mathbb{Z}_Q$ be samples provided in the LWE problem.

- **Setup**: By exploiting those samples, $\mathcal{B}$ generates the master public key mpk below:
  1. Let u_i and $s_1 \neq 0$ be random vectors sampled from $\mathbb{Z}_Q$, denote
  $$\mathbf{u}_i = (u_i \mid \mathbf{u}_i^{'\top})^{\top} \in \mathbb{Z}_Q^n,$$
  and
  $$v_i = v_i^{'} + u_i s_1 \in \mathbb{Z}_Q,$$
  where $i = 1, 2, \ldots, m, m+1, \ldots, m+3n$.
  2. Construct the matrix $\mathbf{F} = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{m+2n}) \in \mathbb{Z}_Q^{n\times(m+2n)}$.

3. Construct the matrix

$$\mathbf{U} = (\mathbf{u}_{m+2n+1}, \mathbf{u}_{m+2n+2}, \ldots, \mathbf{u}_{m+3n}) \in \mathbb{Z}_Q^{n\times n}.$$

4. Sample a matrix $\mathbf{Y}'$ from $\mathcal{D}_{\mathbb{Z}^{(m+2n)\times n},\sqrt{\Sigma}}$ and a matrix $\mathbf{E}$ from $\mathcal{U}(\mathbb{Z}_p^{n\times n})$.

- **Phase 1**: In response to each user secret key query, $\mathcal{B}$ only needs to sample a matrix $\mathbf{Y}'$ from $\mathcal{D}_{\mathbb{Z}^{(m+2n)\times n},\sqrt{\Sigma}}$ as in $Game$ 1.
- **Challenge**: The adversary $\mathcal{A}^*$ takes two more messages $\mathbf{m}_0$ and $\mathbf{m}_1$ of the same length and sends2 to $\mathcal{B}$, then $\mathcal{B}$ chooses random bit $b \in \{0,1\}$ and constructs a challenge ciphertext $\mathbf{CT}_\theta$ for the user id_θ below:
  1. Construct the vector $\mathbf{v}' = (v_1, v_2, \ldots, v_{m+2n})^\top \in \mathbb{Z}_Q^{m+2n}$.
  2. Construct the vector

$$\mathbf{v} = (v_{m+2n+1}, v_{m+2n+2}, \ldots, v_{m+3n})^\top \in \mathbb{Z}_Q^n.$$

  3. Set $\mathbf{c}_{1\theta} = \mathbf{v}' \in \mathbb{Z}_Q^{m+2n}$.
  4. Set $\mathbf{c}_{2\theta} = \mathbf{v} + \mathbf{m}_b\lfloor\frac{Q}{2}\rceil \in \mathbb{Z}_Q^n$.
  5. $s_{1\theta}$ is set to be s_1.
  6. Sample b from $\{0,1\}$ randomly. Let $\mathbf{CT}_\theta$ be random element in $\mathbb{Z}_Q^{m+2n} \times \mathbb{Z}_Q^n \times \mathbb{Z}_Q^*$ if $b = 0$, otherwise, set $\mathbf{CT}_\theta = (\mathbf{c}_{1\theta}, \mathbf{c}_{2\theta}, s_{1\theta})$. Send $\mathbf{CT}_\theta$ to $\mathcal{A}^*$.

  If all the vectors $\{\mathbf{u}_i', v_i'\}_{i=1}^{m+3n}$ are sampled from $A_{\mathbf{s},\chi}$ with $\mathbf{s} \in \mathbb{Z}_Q^{n-1}$, the equation $\mathbf{v}' = \mathbf{F}^\top\mathbf{s} + \mathbf{e}_1$ will hold for some $\mathbf{e}_1 \leftarrow \chi^{m+2n}$ and $\mathbf{s} = (s_1 \mid *)$. The vector $\mathbf{c}_{1\theta}$ can be rewrote as

$$\mathbf{c}_{1\theta} = \mathbf{v}' = \mathbf{F}^\top\mathbf{s} + \mathbf{e}_1.$$

  As for the vector $\mathbf{c}_{2\theta}$, it is equal to $\mathbf{U}^\top\mathbf{s} + \mathbf{e}_2 + \mathbf{m}_b\lfloor\frac{Q}{2}\rceil$, where $\mathbf{e}_2$ denotes the error term of the last n LWE samples. Therefore, $\mathbf{CT}_\theta = (\mathbf{c}_{1\theta}, \mathbf{c}_{2\theta}, s_{1\theta})$ is precisely a challenge ciphertext in $Game$ 1.
  When all samples are randomly distributed in $\mathbb{Z}_Q^n \times \mathbb{Z}_Q$, then the vectors $\mathbf{c}_{1\theta}$ and $\mathbf{c}_{2\theta}$ are also randomly distributed in $\mathbb{Z}_Q^{m+2n}$ and $\mathbb{Z}_Q^n$. Hence, the challenge ciphertext $\mathbf{CT}_\theta$ is uniform and independent in $\mathbb{Z}_Q^{m+2n} \times \mathbb{Z}_Q^n \times \mathbb{Z}_Q^*$ and is identical to that in $Game2$.
- **Phase 2**: Same as Phase 1, but $\mathcal{A}^*$ has the following limitations: $\mathcal{A}^*$ cannot query user U_θ with oracles $O^{\mathbf{Ext}}$ and $O^{\mathbf{Td}}$.
- **Guess**: After interacting with the game, the adversary $\mathcal{A}^*$ returns its guess about the game. $\mathcal{B}$ answers the LWE problem with $\mathcal{A}^*$'s guess.

In summary, we can conclude that

$$|\Pr[Game\,0] - \Pr[Game\,1]| \le \epsilon$$

(for some negeligible ϵ) and

$$|\Pr[Game\,1] - \Pr[Game\,2]| \le Adv[LWE_{n,m+2n,Q,\chi}].$$

Hence the advantage of the PPT adversary $\mathcal{A}$ can be summarized as

$$Adv[\mathcal{A}, \text{IBE-ET}] \le Adv[\mathcal{A}^*, \text{LWE}_{n,m+2n,Q,\chi}] + negl(n),$$

which completes the proof.

□

Comparison with Known Constructions. We present a comparison of the relevant parameter sizes between the scheme in this work and known constructions. The details are listed in Table 1.

Table 1. Comparison of our IBE-ET with other IBE-ET constructions. Data sizes are in number of field elements. Here l is the length of identity, t is the length of plaintext, λ is the security paramater, $m = 6n\log q$ and $\beta = \lceil\log_b q\rceil$ where b is a small integer.

Scheme	mpk	usk	CT
Duong [6]	$(l+3)mn + nt$	$4mt$	$2t + 4m$
Nguyen [14]	$(l+3)mn + nt$	$4m^2$	$m^2 + 2t + 6m + \lambda$
Ours	$(\beta+2)n^2$	$(\beta+2)n^2$	$(\beta+3)n + 1$

To better compare with known schemes, we unified the parameterization of our work and known works. The specific details can be found in Table 2. Our parameter selection are $b = 2, q = 2^{16}, \beta = \lceil\log_2 2^{16}\rceil = 16, t = n$ and $m = 6n\log_2 2^{16} = 96n$. Since definitions of parameters l and λ require that both of them belong to positive integers, we assume $l \ge 2$ and $\lambda \ge 2$.

Table 2. Instantiated parameter size comparison of IBE-ET

Scheme	mpk	usk	CT
Duong [6]	$481n^2$	$384n^2$	$386n$
Nguyen [14]	$481n^2$	$36864n^2$	$9216n^2 + 578n + 2$
Ours	$18n^2$	$18n^2$	$19n + 1$

Through the analysis, it can be found that compared with schemes [6] and [14], the size of the parameters is greatly reduced, and in terms of ciphertext, the parameter size reduces from $O(n^2)$ to $O(n)$ compared with [14], where $O(n)$ indicates a polynomial about n. Therefore, the size of our scheme is relatively compact.

3.5 Achieving IND-sID-CCA security

We note that the lattice-based IBE-ET scheme in this work could achieve IND-sID-CCA security via a general transformation. Fujiaski and Okamoto [7] proposed a very efficient transformation (FO transformation for short), which aims to achieve IND-sID-CCA security for any OW-CPA secure public key encryption scheme (also suitable for IBE) through hybriding a symmetric encryption scheme. We apply this transformation to directly achieve the IND-sID-CCA secure

scheme from the proposal of this paper. For simplicity, we no longer provide specific details.

4. Conclusion

In this paper we propose an efficient construction for lattice-based IBE-ET in the random oracle model. At the core of our construction is the use of compact lattice gadget trapdoor framework. By comparing the size of the keys and the ciphertexts, we can see that the size of our scheme with this technique is relatively compact. Moreover, apply FO transformation our proposal achieves IND-sID-CCA security. Therefore, the scheme has strong practicality. Our future work is to construct an efficient lattice-based IBE-ET in the standard model.

References

[1] Shweta Agrawal, Dan Boneh, and Xavier Boyen. “Efficient lattice (H) IBE in the standard model.” Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29. Springer Berlin Heidelberg, 2010.

[2] Jo¨el Alwen, and Chris Peikert. “Generating shorter bases for hard random lattices.” Theory of Computing Systems 48 (2011): 535-553.

[3] Dan Boneh, and Matthew Franklin. “Identity-based encryption from the Weil pairing.” Annual international cryptology conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001.

[4] Dung Hoang Duong, Kazuhide Fukushima, Shinsaku Kiyomoto, Partha Sarathi Roy, Arnaud Sipasseuth, and Willy Susilo. “Lattice-based public-key encryption with equality test supporting flexible authorization in standard model.” Theoretical Computer Science 929 (2022): 124-139.

[5] 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.” Information Security and Privacy: 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3–5, 2019, Proceedings 24. Springer International Publishing, 2019.

[6] Dung Hoang Duong, Quoc Huy Le, Partha Sarathi Roy, and Willy Susilo. “Lattice-based IBE with equality test in standard model.” Provable Security: 13th International Conference, ProvSec 2019, Cairns, QLD, Australia, October 1–4, 2019, Proceedings 13. Springer International Publishing, 2019.

[7] Eiichiro Fujisaki and Tatsuaki Okamoto. “Secure integration of asymmetric and symmetric encryption schemes.” Annual international cryptology conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999.

[8] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. “Trapdoors for hard lattices and new cryptographic constructions.” Proceedings of the fortieth annual ACM symposium on Theory of computing. 2008.

[9] Huiwen Jia, Yupu Hu, Chunming Tang and Lin Wang. “Towards Compact Identity-Based Encryption on Ideal Lattices.” Cryptographers’ Track at the RSA Conference. Cham: Springer Nature Switzerland, 2024.

[10] Hyung Tae Lee, San Ling, Jae Hong Seo, Huaxiong Wang, and Taek-Young Youn. “Public key encryption with equality test in the standard model.” Information Sciences 516 (2020): 89-108.

[11] Sha Ma. “Identity-based encryption with outsourced equality test in cloud computing.” Information Sciences 328 (2016): 389-402.

[12] Daniele Micciancio and Chris Peikert. “Trapdoors for lattices: Simpler, tighter, faster, smaller.” Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[13] Daniele Micciancio, and Oded Regev. “Worst-case to average-case reductions based on Gaussian measures.” SIAM Journal on Computing 37.1 (2007): 267-302.

[14] Giang L. D. Nguyen, Willy Susilo, Dung Hoang Duong, Huy Quoc Le, and Fuchun Guo. “Lattice-based IBE with equality test supporting flexible authorization in the standard model.” Progress in Cryptology–INDOCRYPT 2020: 21st International Conference on Cryptology in India, Bangalore, India, December 13–16, 2020, Proceedings 21. Springer International Publishing, 2020.

[15] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography.” Journal of the ACM (JACM) 56.6 (2009): 1-40.

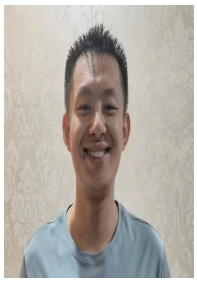
[16] Willy Susilo, Dung Hoang Duong, Huy Quoc Le. “Efficient post-quantum identity-based encryption with equality test.” 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2020.

[17] Zhichao Yang, Debiao He, Longjiang Qu, and Qing Ye Yang. “An Efficient Identity-Based Encryption with Equality Test in Cloud Computing.” IEEE Transactions on Cloud Computing (2023).

Chunfeng FU is a MS student in National University of Defense Technology, Changsha, China. Her research interest is lattice based cryptography.

Renjie JIN recevied MS degree in mathematics from Central China Normal University, Wuhan, China, in 2021. He is now a phD student in National University of Defense Technology, Changsha, China. His research interest is lattice based cryptography.

Longjiang QU received the BA and PhD degrees in mathematics from the National University of Defense Technology, Changsha, China, in 2002 and 2007, respectively. He is now a professor with the faculty of Science, National University of Defense Technology of China. His research interests are cryptography and coding theory.



Zijian ZHOU received the BA and MS degrees from the National University of Defense Technology, Changsha, China, in 2012 and 2014, respectively. And received the PhD degree from the University of Amsterdam, the Netherlands in 2019. He is now an associate professor in the National University of Defense Technology. His research interests are algebraic geometry and cryptography.