# Leveled Hierarchical Identity-Based Fully Homomorphic Encryption from Learning with Rounding

Fucai Luo[1,2(✉)], Kunpeng Wang[1,2], and Changlu Lin[3]

[1] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
luofucai@iie.ac.cn, kpwang@sina.cn
[3] College of Mathematic and Informatics, Fujian Normal University, Fuzhou, China
cllin@fjnu.edu.cn

**Abstract.** Hierarchical identity-based fully homomorphic encryption (HIBFHE) aggregates the advantages of both fully homomorphic encryption (FHE) and hierarchical identity-based encryption (HIBE) that permits data encrypted by HIBE to be processed homomorphically. This paper mainly constructs a new leveled HIBFHE scheme based on Learning with Rounding (LWR) problem, which removes Gaussian noise sampling in encryption process. In more detail, we use the lattice basis delegation method proposed by Agrawal, Boneh and Boyen at CRYPTO 2010 to generate delegated basis, while cleverly exploit a scaled rounding function of LWR problem to hide plaintext rather than adding an auxiliary Gaussian noise matrix. Besides, Gentry, Sahai and Waters constructed the first leveled LWE-based HIBFHE schemes from identity-based encryption scheme at CRYPTO 2013, in this work, however, we also focus on improving their leveled HIBFHE scheme, using Alperin-Sheriff and Peikert's technically simpler method. We prove that our schemes are adaptively secure under classic lattice hardness assumptions.

**Keywords:** FHE · Hierarchical identity-based encryption
Learning with Rounding

## 1 Introduction

Fully Homomorphic Encryption (FHE) is a very attractive cryptographic primitive that allows computations of arbitrary programs on encrypted data without decrypting it first, and then is a powerful tool for handling many core problems in cloud computing, e.g., private outsourcing of computation, SQL query, private information retrieval, secure multi-party computation (MPC), etc. The first candidate lattice-based FHE scheme is based on ideal lattices proposed by Gentry [19] in 2009. In particular, he put forward a remarkable "bootstrapping"


C. Su and H. Kikuchi (Eds.): ISPEC 2018, LNCS 11125, pp. 101–115, 2018.
https://doi.org/10.1007/978-3-319-99807-7_7

theorem for the first time, which implies that if a scheme is capable of evaluating its own (augmented) decryption circuit (it needs an "encryption" of the secret key) and added with the "circular security" assumption made in [19], then one can transform it into a full fledged one which enables arbitrarily large homomorphic computations on encrypted data. However, his solution is complicated and involves relatively untested cryptographic assumptions.

The more attractive and implementable lattice-based FHEs (see [3,9,10,12,21]) started with the work of Brakerski and Vaikuntanathan (BV11b) [12], who devised *relinearization* and *dimension-modulus reduction* techniques that play a key role in their construction. The optimized version of the scheme [10] proposed by Brakerski, Gentry and Vaikuntanathan (BGV) is Halevi and Shoup's scheme [23], which was recognized as one of the most efficient leveled FHE[1] schemes, using the *dimension reduction* and *modulus reduction* iteratively and gradually. It is worth mentioning that Gentry, Sahai and Waters [21] (GSW) used a novel technique of so-called *approximate eigenvector* method to construct a conceptually simpler leveled FHE scheme with simpler and more directly homomorphic operations. Moreover, this GSW needs no user's "evaluation key" and has an interesting property of asymmetric noise growth because of its GSW-style matrix operations. The GSW was subsequently improved by Alperin-Sheriff and Peikert [3] (GSW variant) who leveraged a "gadget matrix" $\mathbf{G}$ developed by Micciancio and Peikert [24].

In fact, the above lattice-based FHEs have been enjoying the intensive study for their faster implementation, stronger malleability and applicability; and more importantly, stronger security, since these schemes are based on Learning with Errors (LWE) problem [27] which was proved to be at least as hard as some worst-case lattice problems [11,27] (e.g., GapSVP, which was regarded to be secure even after the advance of quantum computers). Therefore, these lattice-based FHEs are very attractive and conductive for the studying of the post-quantum cryptography.

**IBE and HIBE.** Identity-Based Encryption (IBE) is a generalization of public key encryption (PKE) that allows a sender to encrypt a message using the recipient's identity − any arbitrary string such as an e-mail address − as a public key, which was first proposed by Shamir [28] in 1984. The ability to use identities as public keys avoids the need to distribute public key certificates, which is very useful in many applications such as email where the recipient is often off-line and unable to present a public-key certificate while the sender encrypts a message. The first construction of IBE is based on bilinear maps assumption [7] or quadratic residue assumption [17]. Since then, a series of schemes, which are based on bilinear maps assumption [31], quadratic residue assumption [8] and LWE assumption [1,2,14,20], have been proposed.

Hierarchical Identity-Based Encryption (HIBE) is an extension of IBE scheme where entities are arranged in a directed tree [22]. Specifically, each entity in the tree obtains a private key from its "parent" (higher-level) and then

[1] Leveled FHE is capable of evaluating arbitrary polynomial-depth circuits, without Gentry's bootstrapping procedure.

delegates private keys for its "children" (lower-level) so that a child entity can decrypt plaintext intended for it, or for its children, but cannot decrypt plaintext intended for any other nodes in the tree; this delegation process is one-way: a child node cannot use its private key to recover the key of its parent or its siblings. Based on this kind of framework, a few HIBEs based on LWE problem (see [1,2,14]) and (H)IBEs based on the LWR problem (see [18,32]) have been presented. We will give a formal introduction for LWR problem [5] in Sect. 2. As far as the efficiency of HIBEs is concerned, the lattice basis delegation problem is the main bottleneck, although the problems that existed in IBEs, e.g., the size of ciphertext and parameters, also affect the efficiency.

**HIBFHE.** Hierarchical Identity-Based FHE (HIBFHE) as an extension of HIBE, as a matter of fact, has captured researchers' attentions as it aggregates the advantages of both FHE and HIBE [21]. Roughly speaking, the data encrypted by HIBE support arbitrarily complex evaluations without being decrypted, and such properties of hierarchy and homomorphism are very useful in access control of encrypted data [15]. However, there are a few results. In fact, Gentry, Sahai and Waters [21] also used their "flatten" technique to compile all HIBEs [1,2,14], which thus results in leveled HIBFHE schemes. After that, Wang *et al.* [30] used the MP12-trapdoor for lattices [24] to improve the IBE scheme in [1], then compiled this improved IBE and obtained a leveled IBFHE. However, if we extend their leveled IBFHE to leveled HIBFHE, it is very easy to find that the dimension of lattice will expand when the delegation mechanism is used to generate delegated basis for the identity of lower-level; or more precisely, the dimension will increase linearly with the depth of hierarchy. Consequently, private keys and ciphertexts become longer and longer as one descends into the hierarchy. This problem also resides in Sun *et al.*' [29] RLWE-based leveled IBFHE (which is selective-ID secure). Actually, this RLWE-based leveled IBFHE is based on the structure of GSW and thus is impractical, because the GSW is not fully compatible with RLWE problem due to its asymmetric noise growth [21].

It is worth noting that all (H)IBFHEs aforementioned are leveled homomorphic, which means that they can only bear homomorphic computations of a priori polynomial-depth circuits, except the first non-leveled IBFHE scheme proposed by Clear and McGoldrick [16] under the existential hypothesis of indistinguishable obfuscator. This is because we cannot use bootstrapping theorem to transform a leveled (H)IBFHE scheme into "pure" one, for bootstrapping in the identity-based setting needs to non-interactively derive from the public parameters an "encryption" of the secret key for an arbitrary identity. But this "encryption" is user-specific and is not identity-based, in the sense that it only can be obtained interactively from user-specific. While obtaining this "encryption" interactively undermines the main appeal of IBE: its non-interactivity.

**Our Contributions.** We present two leveled HIBFHE schemes with fixed dimensions and short ciphertexts. Our first and main scheme, which is based on LWR problem [5] and is proved to be secure against adaptive chosen-identity attack, needs no Gaussian noise sampling in encryption process. In our

LWR-based leveled HIBFHE scheme, we use the basis delegation technique in [2] to generate identity-specific basis without increasing the dimension of the lattice in derive phase, and then use the preimage sampleable algorithm in [20] to yield the identity-specific secret key in extract phase. In encryption process, we cleverly use the scaled rounding function of LWR problem to hide plaintext rather than adding an auxiliary Gaussian noise matrix. The resulting ciphertexts have constant size and are not relevant to the depth of hierarchy. Our LWR-based leveled HIBFHE scheme gets rid of Gaussian noise sampling merely in encryption process, but this is enough for improving the efficiency. Because the generating processes of public keys and secret keys, which involve Gaussian sampling, are implemented only once in general case, while there are a large number of times for the encryption process. More importantly, removing the Gaussian noise sampling in encryption process will strengthen safety, due to some potential side-channel vulnerabilities (result in complete leakage of the secret key) incurred by Gaussian noise sampling in every encryption process [13,26]. Although it is possible to create good implementations which protect against side-channel attacks, these implementations are very complex. However, such improvements are obtained with a penalty: the size of the secret key, the public key and the ciphertext of the LWR-based leveled HIBFHE scheme are all slightly bigger than that of our improvement on the LWE-based leveled HIBFHE scheme [21] (up to a small polynomial in $n$), and the security reduction loss of our LWR-based leveled HIBFHE scheme is also bigger due to the reduction between LWE and LWR (up to a polynomial). These can be seen from the Table 1 in the full version of the paper.

We also present a more efficient leveled HIBFHE scheme based on LWE problem. In our LWE-based leveled HIBFHE scheme, we use a technically simpler variant method [3] of GSW to generate ciphertext with constant length, and then we obtain more compact parameters due to the simple and tight noise analysis technique when performing homomorphic evaluations. In fact, that we present this improved construction is meant to help us compare the LWE-based leveled HIBFHE scheme with our novel LWR-based leveled HIBFHE scheme more clearly.

**Organization.** In Sect. 2, we give the preliminaries including notations, hardness assumptions and some related algorithms to be used in this paper. The definition of hierarchical identity-based FHE, the lattices and discrete Gaussians can be found in the full version of the paper. In Sect. 3, we present our construction of LWR-based leveled HIBFHE scheme. Section 4 follows an improvement on the previous LWE-based leveled HIBFHE. Finally, we conclude the paper with future direction in Sect. 5.

## 2 Preliminaries

**Notations.** We say that a function $\mathrm{negl}(n)$ is negligible if $\mathrm{negl}(n)$ is smaller than all polynomial fractions for sufficiently large $n$. For a positive integer $q$, we define the set $\mathbb{Z}_q \triangleq [-q/2, q/2) \cap \mathbb{Z}$, and all logarithms on $q$ are base 2. All

arithmetics are performed over $\mathbb{Z}$ or $\mathbb{Q}$ when division is used, and for ease of use, we let $[n] \triangleq \{1, \cdots, n\}$. We denote vectors in bold lowercase (e.g., $\mathbf{x}$) and matrices in bold uppercase (e.g., $\mathbf{A}$); $\mathbf{x}^t$ (resp. $\mathbf{A}^t$) denotes the transpose of the vector $\mathbf{x}$ (resp. $\mathbf{A}$). For any $x \in \mathbb{Q}$, we denote by $\lfloor x \rfloor$, $\lceil x \rceil$, $\lceil x \rfloor$ the rounding of $x$ down, up, or to the nearest integer; these notations also apply to vector and matrix. The multiplication between two vectors $\mathbf{x}$, $\mathbf{y}$ over $\mathbb{Z}_q$ is denoted by $<\mathbf{x}, \mathbf{y}>_q$ (i.e., $<\mathbf{x}, \mathbf{y}>$ *mod* $q$). In this paper, $||\cdot||$ denotes Euclidean norm unless otherwise stated, and for a $n$-dimensional vector $\mathbf{x} = \{x_1, \cdots, x_n\}$, we denote its magnitude by $|\mathbf{x}| \triangleq \max\{|x_i|\}_{i\in[n]}$ where $|x_i|$ refers to $x_i'$ s magnitude, moreover, vectors (e.g., $\mathbf{a}$) are treated as columns. We let $x \xleftarrow{\$} \mathcal{D}$ denote that $x$ is randomly sampled from a distribution $\mathcal{D}$ and $x \xleftarrow{\$} \mathcal{S}$ denote that $x$ is uniform over a set $\mathcal{S}$. For any matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{A} \in \mathcal{X}^{n\times m}$ (resp. $\mathbf{A} \xleftarrow{\$} \mathcal{X}^{n\times m}$) denotes that for $i \in [n], j \in [m]$ its entry $\mathbf{A}[i][j] \in \mathcal{X}$ (resp. $\mathbf{A}[i][j] \xleftarrow{\$} \mathcal{X}$) where $\mathcal{X}$ is a set or distribution. This also applies to vector.

### 2.1 Hardness Assumptions

**Learning with Errors (LWE).** The well-known learning with errors (LWE) problem has been enjoying a fame for its versatility in the constructions of lattice-based schemes, and was conjectured to be secure in quantum setting ever since Regev [27] introduced it and gave a quantum reduction from some standard lattice problems to the LWE problem (subsequently followed by some classical reduction [11,25]). The binLWE problem is a specific form of LWE where the secret $\mathbf{s}$ is chosen uniformly from $\{0,1\}^n$, or generating the binLWE problem directly from $\mathsf{LWE}_{n,q,m,\chi}(\mathcal{D})$ by letting $\mathcal{D} = \{0,1\}^n$. As for the security of binLWE problem, Brakerski *et al.* [11] proved that the binLWE problem is at least as hard as the original LWE problem.

**Definition 1 ($B$-Bounded Distributions [6,9]).** *A distribution ensemble $\{\chi_n\}_{n\in\mathbb{N}}$, supported over the integers, is called $B$-bounded if $Pr[e \xleftarrow{\$} \chi_n \mid ||e|| > B] = \mathrm{negl}(n)$. We say a $B$-bounded distribution $e$ is balanced if $Pr[e \geq 0] \geq \frac{1}{2}$ and $Pr[e \leq 0] \geq \frac{1}{2}$.*

**Learning with Rounding (LWR).** As a deterministic variant of LWE problem, Learning with Rounding (LWR) problem, was firstly proposed by Banerjee, Peikert and Rosen [5] for improving the efficiency of pseudorandom generator (PRG) based on the LWE problem. Interestingly enough, the implicit noise in LWR is deterministic which derandomizes the random noise in LWE. Meanwhile, the single implicit noise in LWR is smaller than that in LWE. Specifically, the noise in LWE is $B$-bounded, while the implicit noise has magnitude less than $\frac{1}{2}$ in LWR.

For the positive integers $n$, $m$ and $p < q$, we firstly recall the scaled rounding function [5] $\lceil\cdot\rfloor_p$ which will be used in encryption process in Sect. 3. It is defined as follows:

$$\begin{aligned} \left\lceil \cdot \right\rfloor_p \quad &: \mathbb{Z}_q \longrightarrow \mathbb{Z}_p \\ &a \mapsto \left\lceil \tfrac{p}{q} \cdot a \right\rfloor. \end{aligned}$$

The scaled rounding function $\lceil \cdot \rfloor_p$ denotes the component-wise rounding if the entry is a vector or matrix.

For a $n$-dimensional vector $\mathbf{s}$ sampled from a distribution $\mathcal{D} \subset \mathbb{Z}_q^n$, we define the LWR distribution $\mathsf{LWR}_{n,q,p}(\mathcal{D}) \triangleq \{(\mathbf{a}_i, \lceil \langle \mathbf{a}_i, \mathbf{s} \rangle \rfloor_p) \in \mathbb{Z}_q^n \times \mathbb{Z}_p | \mathbf{a}_i \xleftarrow{\$} \mathbb{Z}_q^n\}$ in which the pair $(\mathbf{a}_i, \lceil \langle \mathbf{a}_i, \mathbf{s} \rangle \rfloor_p)$ denotes a LWR sample (instance). As with the LWE problem, LWR problem can be also divided into two problems: the search and decision problems. The search LWR problem is defined as finding the secret $\mathbf{s}$ given $m$ independent instances chosen from $\mathsf{LWR}_{n,q,p}(\mathcal{D})$. While the decision LWR problem, denoted by $\mathsf{DLWR}_{n,m,q,p}(\mathcal{D})$, is to distinguish (with non-negligible advantage) $m$ samples $(\mathbf{a}_i, \lceil \langle \mathbf{a}_i, \mathbf{s} \rangle \rfloor_p)$ chosen from $\mathsf{LWR}_{n,q,p}(\mathcal{D})$, from $m$ independent samples chosen according to the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_p$. The $\mathsf{LWR}_{n,q,p}(\mathcal{D})$ assumption implies that the $\mathsf{DLWR}_{n,m,q,p}(\mathcal{D})$ problem is infeasible. As with the binLWE problem, we can also get binLWR problem from $\mathsf{LWR}_{n,q,p}(\mathcal{D})$ by letting $\mathcal{D} = \{0,1\}^n$.

As for the hardness of the LWR problem, Banerjee *et al.* [5] presented an efficient reduction from LWE problem to LWR problem for super-polynomial modulus $q$. Subsequently, Alwen *et al.* [4] gave a reduction that allows for a polynomial modulus $q$, but that restricts the number of samples and fails to apply to all values of the modulus $q$. In 2016, the reduction in [4] was extended by Bogdanov *et al.* [6] who eliminated the theoretic restriction on the modulus $q$, though the number of samples in [6] is required to be less than $O(q/Bp)$ (weaker than that in [4]). For completeness, we give the Theorem 1 that is adapted from [6]. Note that the reduction from LWE to binLWE was shown in [11], hence by combining the reduction with Theorem 1, we can safely reduce the hardness of binLWR problem to LWE problem.

**Theorem 1** ([6]). *For every $\epsilon > 0$, positive integers $n$, $m$, $q > 2mpB$, $p|q$, and if there is an algorithm $\mathcal{A}$ such that*

$$\left| Pr_{\mathbf{A},\mathbf{s}}[\mathcal{A}(\mathbf{A}, \lceil \mathbf{A}\mathbf{s} \rfloor_p) = 1] - Pr_{\mathbf{A},\mathbf{v}}[\mathcal{A}(\mathbf{A}, \mathbf{v}) = 1] \right| \geq \epsilon,$$

*where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$, $\mathbf{s} \xleftarrow{\$} \{0,1\}^n$ and $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_p^m$, then there exists another algorithm $\mathcal{B}$ that runs in time polynomial in $n$, $m$, the number of divisors of $q$, and the running time of $\mathcal{A}$ such that*

$$Pr_{\mathbf{A},\mathbf{s}}[\mathcal{B}(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}) = \mathbf{s}] \geq \left( \frac{\epsilon}{4qm} - \frac{2^n}{p^m} \right)^2 \cdot \frac{1}{(1 + 2Bp/q)^m}$$

*for noise distribution $\mathbf{e}$ that is $B$-bounded and balanced in each coordinate, where it requires that $B \geq 2\sqrt{n}$ due to the reduction (quantum or classical) from certain lattice problems to* LWE *problem* [11,27].

Note that Theorem 1 concerns the search bin-LWE problem, which is not easier than its decision problem. Moreover, we remark that the term $Pr_{\mathbf{A},\mathbf{s}}[\mathcal{A}(\mathbf{A}, \lceil \mathbf{A}\mathbf{s} \rfloor_p) = 1] - Pr_{\mathbf{A},\mathbf{v}}[\mathcal{A}(\mathbf{A}, \mathbf{v}) = 1]$ in Theorem 1 can be interpreted as the decision $\mathsf{DLWR}_{n,m,q,p}(\mathcal{D})$ problem for the fixed $\mathbf{s} \xleftarrow{\$} \{0,1\}^n$ (set $\mathcal{D} = \{0,1\}^n$).

### 2.2 Gadget Matrices and Some Algorithms

In this subsection, we recall the gadget matrix [24] and four important algorithms that will be used in our constructions and security proofs. Roughly speaking, we generate the master public matrix together with a short basis by employing the trapdoor generation algorithm [24] and then use the lattice basis delegation algorithm [2] to generate delegated basis. At last, output the identity-specific secret key by utilizing the preimage sampleable algorithm [20].

For the integer $q$, we define the gadget matrix $\mathbf{G} := \mathbf{I}_{m+1} \otimes \mathbf{g}^t$, where $\mathbf{g}^t := (1, 2, \cdots, 2^{\lceil \log q \rceil - 1}) \in \mathbb{Z}_q^{\lceil \log q \rceil}$ and $\mathbf{I}_{m+1}$ denotes the $(m+1)$-dimensional identity matrix. Moreover, we define the deterministic inversion function $\mathbf{G}^{-1} : \mathbb{Z}_q^{(m+1)\times m'} \to \{0,1\}^{m' \times m'}$ where $m' = (m+1) \cdot \lceil \log q \rceil$, which is equal to bit decomposition that decomposes $x$ into its bit representation over $\mathbb{Z}_q$ and has the property that for any matrix $\mathbf{A} \in \mathbb{Z}_q^{(m+1)\times m'}$ it holds that $\mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{A}) = \mathbf{A}$. Since there are two moduli $q$, $p$ in LWR problem, here we construct another gadget matrix $\widehat{\mathbf{G}}$ constructed as $\widehat{\mathbf{G}} := \mathbf{I}_{m+1} \otimes \widehat{\mathbf{g}}^t$ where $\widehat{\mathbf{g}}^t := (1, 2, \cdots, 2^{\lceil \log p \rceil - 1}) \in \mathbb{Z}_p^{\lceil \log p \rceil}$. The deterministic inversion function $\widehat{\mathbf{G}}^{-1}$ is defined by the same method as above.

**Lemma 1** ([24]). *Let $n$, $q > 2$ and $m \approx 2n \log q$ be positive integers, there is a PPT algorithm $\mathsf{GenTrap}(1^n, 1^m, q)$ that outputs a parity-check matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a trapdoor $\mathbf{X}$ with a tag $\mathbf{H}$ such that the distribution of $\mathbf{A}$ is statistically close to the uniform. Then one can use the trapdoor and any basis $\mathbf{S}$ for $\Lambda_q^{\perp}(\mathbf{G})$ to generate a short basis $\mathbf{T_A}$ for lattice $\Lambda_q^{\perp}(\mathbf{A})$, and the parameters satisfy $s_1(\mathbf{X}) \leq 1.6\sqrt{n \log q}$ and $||\widetilde{\mathbf{T}}_{\mathbf{A}}|| \leq 3.8\sqrt{n \log q}$, where $s_1(\mathbf{X})$ is the largest singular value of $\mathbf{X}$.*

*Remark 1.* Note that it is easy to compute a basis $\mathbf{S}$ for $\Lambda_q^{\perp}(\mathbf{G})$, whenever the modulus $q$ is power-of-two or not, since $\mathbf{G}$ is gadget matrix whose trapdoor is publicly known.

The following SampleRwithBasis lemma plays a key role in our security proofs, this is due to the fact that the simulator (challenger) calls the SampleRwithBasis algorithm to generate short basis, and then uses this basis to generate identity-specific secret key for answering the secret key query. While the Lattices Basis Delegation lemma is of crucial importance in the constructions of our schemes. In the lattices basis delegation mechanism, it is required that the matrix $\mathbf{R}$ is invertible mod $q$ in $\mathbb{Z}_q^{m \times m}$ where all the columns of $\mathbf{R}$ are "low norm". Similarly with [2], we denote by $\mathcal{D}_{m \times m}$ the distribution $(\mathcal{D}_{\mathbb{Z}_q^m, \sigma_{\mathbf{R}}})^m$ conditioned on the matrix $\mathbf{R}$ being invertible mod $q$ in $\mathbb{Z}_q^{m \times m}$, where $\sigma_{\mathbf{R}} = \sqrt{n \log q} \cdot \omega(\sqrt{\log m})$.

**Lemma 2** ([2]). *Let $q > 2$ be a prime and $m \geq 2n \log q$. For all but at most a $q^{-1}$ fraction of rank $n$ matrices $\mathbf{A}$ in $\mathbb{Z}_q^{n \times m}$, there exists a PPT algorithm $\mathsf{SampleRwithBasis}(\mathbf{A})$ that outputs a matrix $\mathbf{R} \in \mathbb{Z}^{n \times m}$ sampled from a distribution statistically close to $\mathcal{D}_{m \times m}$ and a basis $\mathbf{T_B}$ for lattice $\Lambda_q^{\perp}(\mathbf{B})$ with the parameter $\sigma_{\mathbf{R}} \geq ||\widetilde{\mathbf{T}}_{\mathbf{B}}|| \cdot \omega(\sqrt{\log m})$ with overwhelming probability, where it holds that $\mathbf{B} = \mathbf{A} \cdot \mathbf{R}^{-1} (mod\ q)$.*

**Lemma 3** ([2]). *Let $q > 2$ and let $\mathbf{A}$ be a matrix in $\mathbb{Z}_q^{n\times m}$ with $m \geq 2n\log q$. Let $\mathbf{T_A}$ be a basis for lattice $\Lambda_q^{\perp}(\mathbf{A})$. Given a matrix $\mathbf{R}$ sampled from the distribution $\mathcal{D}_{m\times m}$ and the parameter $\sigma > ||\widetilde{\mathbf{T}}_{\mathbf{A}}|| \cdot \sigma_{\mathbf{R}} \cdot \sqrt{m} \cdot \omega(\log^{3/2} m)$, there is a PPT algorithm $\mathsf{BasisDel}$ $(\mathbf{A}, \mathbf{T_A}, \mathbf{R}, \sigma)$ that outputs a basis $\mathbf{T}_{\mathbf{AR}^{-1}}$ for the lattice $\Lambda_q^{\perp}(\mathbf{AR}^{-1})$ with overwhelming probability, where $\mathbf{T}_{\mathbf{AR}^{-1}}$ satisfies $||\mathbf{T}_{\mathbf{AR}^{-1}}|| \leq \sigma \cdot \sqrt{m}$.*

One can generate identity-specific secret keys for all identities in hierarchy via the following preimage sampleable algorithm [20].

**Lemma 4.** *Let $n$ and $q$ be positive integers with $q \geq 2$, and let $m > n$. Let $\mathbf{T_A}$ be a short basis for lattice $\Lambda_q^{\perp}(\mathbf{A})$ and $\sigma \geq ||\widetilde{\mathbf{T}}_{\mathbf{A}}|| \cdot \omega(\sqrt{\log m})$. Then for $\mathbf{c} \in \mathbb{R}^m$ and $\mathbf{u} \in \mathbb{Z}_q^n$:*

1. *$Pr[\ \mathbf{x} \xleftarrow{\$} \mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma} \quad | \quad ||\mathbf{x}|| > \sqrt{m} \cdot \sigma\ ] \leq \mathrm{negl}(n)$.*
2. *There is a PPT algorithm $\mathsf{SamplePre}(\mathbf{A}, \mathbf{T_A}, \sigma, \mathbf{u})$ that outputs $\mathbf{x} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$ sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma}$.*

## 3 Our LWR-Based Scheme

In this section, based on LWR problem, we use the three algorithms outlined in Sect. 2.2 to construct a leveled hierarchical identity-based FHE in the random oracle model. Similarly to [2], we also utilize a hash function $H : (\{0,1\}^*)^{\leq d} \rightarrow \mathbb{Z}_q^{m\times m} \quad | \quad \mathbf{id} \mapsto H(\mathbf{id}) \sim \mathcal{D}_{m\times m}$ for mapping the identity $\mathbf{id}$ to a matrix in $\mathbb{Z}_q^{m\times m}$, where the requirement is that the $H(\mathbf{id})$ is distributed as $\mathcal{D}_{m\times m}$ over the choice of the random oracle $H$.

### 3.1 Leveled Hierarchical Identity-Based FHE from LWR

As what mentioned before, the leveled HIBFHEs have the properties of hierarchy and homomorphism, thus we assume the maximal depth of the hierarchy is $d$ and the maximal homomorphically evaluable depth is $L$. Similarly to [2], we choose a Gaussian parameter $\sigma = (\sigma_1, \cdots, \sigma_d)$ needed in **Derive** and **Extract** processes, where it holds that

$$\begin{cases} \sigma_\ell > \sigma_{\ell-1} \cdot m^{3/2} \cdot \omega(\log^2 m) > \sigma_1 \cdot \left(m^{3/2} \cdot \omega(\log^2 m)\right)^{\ell-1} \\ \sigma_1 > ||\widetilde{\mathbf{T}}_{\mathbf{A}}|| \cdot \sigma_{\mathbf{R}} \cdot \sqrt{m} \cdot \omega(\log^{3/2} m). \end{cases}$$

Comparing to the LWE-based scheme, our LWR-based leveled HIBFHE scheme uses the scaled rounding function to hide plaintext instead of Gaussian noise sampled from a discrete Gaussian distribution, and therefore it doesn't need the Gaussian noise parameter $\alpha = (\alpha_1, \cdots, \alpha_d)$ any more.

– **Setup**$(1^\lambda, 1^d, 1^L)$. Choose a lattice dimension parameter $n = n(\lambda, d, L)$, moduli $q = q(\lambda, d, L)$ and $p = p(\lambda, d, L)$ that satisfies $p|q$. Also, choose parameter $m = m(\lambda, d, L) \geq 2n\log q$. Let $k = \lceil \log p \rceil$ and $N = (m+1) \cdot k$. Then

call the PPT algorithm $\mathsf{GenTrap}(1^n, 1^m, q)$ to generate a parity-check matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a trapdoor $\mathbf{X}$ with a tag $\mathbf{H}$ such that the distribution of $\mathbf{A}$ is statistically close to the uniform. Based on Lemma 1, use the trapdoor $\mathbf{X}$ and a random basis $\mathbf{S}$ for $\Lambda_q^{\perp}(\mathbf{G})$ to generate a short basis $\mathbf{T_A}$ for $\Lambda_q^{\perp}(\mathbf{A})$. Choose uniformly at random a vector $\mathbf{u} \in \mathbb{Z}_q^n$. Finally, the master public parameters is $mpk := (\mathbf{A}, \mathbf{u})$, and the corresponding master secret key is $msk := (\mathbf{T_A})$.

- **Derive**$(mpk, \mathbf{T_{id|\ell}}, \mathbf{id})$. Take as input public parameters $mpk$, a private basis $\mathbf{T_{id|\ell}}$ corresponding to a "parent" identity $\mathbf{id}_{|\ell} = (\mathbf{id}_1, \cdots, \mathbf{id}_\ell)$ at level $\ell$ and a "child" identity $\mathbf{id} = (\mathbf{id}_1, \cdots, \mathbf{id}_\ell, \cdots, \mathbf{id}_k)$ of a lower level $k$ where $k \leq d$, do the following processes:
  1. For $i \in [\ell]$, compute $H(\mathbf{id}_i)$, and set $\mathbf{R_{id|\ell}} = H(\mathbf{id}_\ell) \cdots H(\mathbf{id}_1) \in \mathbb{Z}^{m\times m}$. Then compute $\mathbf{B_{id|\ell}} = \mathbf{A} \cdot \mathbf{R}_{\mathbf{id}|\ell}^{-1} \in \mathbb{Z}_q^{n\times m}$. Let $\mathbf{T_{id|\ell}}$ be the short basis for $\Lambda_q^{\perp}(\mathbf{B_{id|\ell}})$.
  2. Compute $\mathbf{R} = H(\mathbf{id}_k) \cdots H(\mathbf{id}_{\ell+1}) \in \mathbb{Z}^{m\times m}$ and set $\mathbf{B_{id}} = \mathbf{B_{id|\ell}} \cdot \mathbf{R}^{-1} \in \mathbb{Z}_q^{n\times m}$.
  3. Invoke $\mathbf{T}' \leftarrow \mathsf{BasisDel}(\mathbf{B_{id|\ell}}, \mathbf{T_{id|\ell}}, \mathbf{R}, \sigma_k)$ to obtain a short random basis for $\Lambda_q^{\perp}(\mathbf{B_{id}})$.
  4. Output the delegated basis $\mathbf{T_{id}} = \mathbf{T}'$.
- **Extract**$(mpk, \mathbf{B_{id}}, \mathbf{T_{id}}, \mathbf{id})$. Take as input public parameters $mpk$, and an identity $\mathbf{id}$ of depth $|\mathbf{id}| = \ell$. Run the PPT algorithm $\mathsf{SamplePre}(\mathbf{B_{id}}, \mathbf{T_{id}}, \sigma_\ell, \mathbf{u})$ to sample a short vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{B_{id}} \cdot \mathbf{x} = \mathbf{u} \pmod q$. Then output identity-specific public key $pk_{\mathbf{id}} : \mathbf{P} = \begin{bmatrix} \mathbf{B}_{\mathbf{id}}^t \\ \mathbf{u}^t \end{bmatrix}$, and the identity-specific secret key $sk_{\mathbf{id}} : \mathbf{s} = (-\mathbf{x}, 1)$. Note that $\mathbf{s}^t \cdot \mathbf{P} = 0 \pmod q$.
- **Enc**$(pk_{\mathbf{id}}, \mathbf{id}, \mu)$. To encrypt a message $\mu \in \{0, 1\}$, sample a small matrix $\mathbf{M} \xleftarrow{\$} \{0, 1\}^{n\times N}$. Output a ciphertext

$$\mathbf{C} = \lceil \mathbf{P} \cdot \mathbf{M} \rfloor_p + \mu \widehat{\mathbf{G}} \in \mathbb{Z}_p^{(m+1)\times N}.$$

- **Dec**$(\mathbf{C}, sk_{\mathbf{id}})$. Choose the penultimate column vector $\mathbf{c}$ of ciphertext $\mathbf{C}$, and then compute

$$\mu = \left| \lceil \frac{2}{p} \cdot \langle \mathbf{s}, \mathbf{c} \rangle_p \rfloor \right|.$$

- **Add**$(\mathbf{C}_1, \mathbf{C}_2)$. For two ciphertext matrices $\mathbf{C}_1$ and $\mathbf{C}_2$ decrypting to plaintexts $\mu_1$ and $\mu_2$ under identical identity, output

$$\mathbf{C}_{\mathrm{Add}} \triangleq \mathbf{C}_1 + \mathbf{C}_2.$$

- **Mult**$(\mathbf{C}_1, \mathbf{C}_2)$. For two ciphertext matrices $\mathbf{C}_1$ and $\mathbf{C}_2$ decrypting to plaintexts $\mu_1$ and $\mu_2$ under identical identity, the multiplication is defined as

$$\mathbf{C}_{\mathrm{Mult}} \triangleq \mathbf{C}_1 \cdot \widehat{\mathbf{G}}^{-1}(\mathbf{C}_2).$$

### 3.2 Correctness and Parameters

Firstly, according to Lemma 4, $\mathbf{x} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$ is sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma_\ell}$ that satisfies $||\mathbf{x}|| \leq \sqrt{m} \cdot \sigma_\ell$ with overwhelming probability. Combining Lemmas 1 and 3 with the parameters set in Sect. 3.1, we can set $\sigma_\ell = m^{\frac{3}{2}\ell} \cdot \omega(\log^{2\ell} m)$. Next, we analyze the correctness and the magnitude of noise. The penultimate column vector of $\widehat{\mathbf{G}}$ is $(0, 0, \cdots, v) \in \mathbb{Z}_p^{m+1}$ where $v \in (p/4, p/2]$. We write $\mathbf{E} = \lceil \mathbf{P} \cdot \mathbf{M} \rfloor_p - \frac{p}{q} \cdot \mathbf{P} \cdot \mathbf{M} \in [-1/2, 1/2]^{(m+1)\times N}$, and then its penultimate column vector is $\mathbf{e} \in [-1/2, 1/2]^{m+1}$. According to the **Dec** algorithm, we have

$$\mu = \Big| \Big\lceil \frac{2}{p} \cdot \langle \mathbf{s}, \mathbf{c} \rangle_p \Big\rfloor \Big| = \Big| \Big\lceil \frac{2}{p} \cdot \big( \langle \mathbf{s}, \mathbf{e} \rangle + \mu v \big) \Big\rfloor \Big|,$$

as long as

$$|e'| = |\langle \mathbf{s}, \mathbf{e} \rangle| \leq ||\mathbf{e}|| \cdot (||\mathbf{x}|| + 1) \leq m^{\frac{3}{2}\ell+1} \cdot \omega(\log^{2\ell} m) < p/4. \tag{1}$$

Since the homomorphic addition is obvious, we mainly analyze homomorphic multiplication.

**Homomorphic Multiplication.** To multiply two ciphertext matrices $\mathbf{C}_1, \mathbf{C}_2 \in \mathbb{Z}_p^{(m+1)\times N}$ designated for messages $\mu_1, \mu_2 \in \{0, 1\}$, we have

$$\begin{aligned} \mathbf{s}^t \cdot \mathbf{Mult}(\mathbf{C}_1, \mathbf{C}_2) = \mathbf{s}^t \cdot \mathbf{C}_1 \cdot \widehat{\mathbf{G}}^{-1}(\mathbf{C}_2) &= (\mathbf{s}^t \cdot \mathbf{E}_1 + \mu_1 \mathbf{s}^t \cdot \widehat{\mathbf{G}}) \cdot \widehat{\mathbf{G}}^{-1}(\mathbf{C}_2) \\ &= (\mathbf{e}_1' \cdot \widehat{\mathbf{G}}^{-1}(\mathbf{C}_2) + \mu_1 \mathbf{e}_2') + \mu_1 \mu_2 \mathbf{s}^t \cdot \widehat{\mathbf{G}}, \end{aligned}$$

where $\widehat{\mathbf{G}}^{-1}(\mathbf{C}_2) \in \{0, 1\}^{N \times N}$. Then $\mathbf{e}_1' \cdot \widehat{\mathbf{G}}^{-1}(\mathbf{C}_2) + \mu_1 \mathbf{e}_2'$ is the total noise which is of magnitude

$$|\mathbf{e}_1' \cdot \widehat{\mathbf{G}}^{-1}(\mathbf{C}_2) + \mu_1 \mathbf{e}_2'| \leq m^{\frac{3}{2}\ell+1} \cdot \omega(\log^{2\ell} m) \cdot (N + 1)$$

by Eq. (1). It is clear that the noise growth factor is $N + 1$, and therefore after $L$ levels of homomorphic multiplication, the noise grows from an initial magnitude of $m^{\frac{3}{2}\ell+1} \cdot \omega(\log^{2\ell} m)$, to $m^{\frac{3}{2}\ell+1} \cdot \omega(\log^{2\ell} m) \cdot (N + 1)^L$.

Our LWR-based scheme removes Gaussian noise sampling in encryption process, but there are two moduli $p$, $q$ satisfying $q > 2mpB$ and $p|q$ where $B \geq 2\sqrt{n}$ (according to Theorem 1). In fact, it is sufficient to set $q = pn^{\frac{3}{2}}$ due to $m \geq 2n \log q$, and then we have $m \geq 2n \log q = 2n \log p + 3n \log n$. Therefore, we can get the the following theorem.

**Theorem 2.** *For the parameters $\lambda$, $d$, $L$, $n = n(\lambda, d, L)$ and $m = m(\lambda, d, L) \geq 2n \log q$, if the polynomial size moduli $p \geq (4n \log^2 p)^{\frac{3}{2}d+L+1} \cdot \omega\big((2 \log n)^{2d}\big)$ and $q = pn^{\frac{3}{2}}$, our* LWR*-based scheme is a correct $L$-*leveled HIBFHE.

Overall, the moduli $p$ and $q$ are both of polynomial size in parameter $n$, and then combining the Theorem 1 with the reductions between LWE problem and certain standard lattice problems (e.g., GapSVP), we can base the security of our LWR-based leveled HIBFHE scheme on these worst-case lattice problems with polynomial approximation factors.

### 3.3 Security

We prove that our LWR-based leveled HIBFHE scheme is INDr-ID-CPA secure. More precisely, the challenger in our simulated attack model can answer any type of query sent by the adaptive adversary. Comparing to the security proof in [2], the setup of simulated attack model and the random oracle hash $H$ query are almost the same as theirs (for simplicity, we omit them in our security proof), but the challenger needs to run PPT algorithm SamplePre to obtain the secret key for answering the identity-specific secret key query in our security proof. The full proof of Theorem 3 is given in the full version of the paper.

**Theorem 3.** *Let $\mathcal{A}$ be a PPT adversary that attacks our* LWR*-based scheme, and $Q_H$ be the number of hash $H$ queries made by $\mathcal{A}$ and $d$ be the maximal hierarchy depth, where $H$ is a hash function modeled as a random oracle. Then there is a PPT algorithm $\mathcal{B}$ that solves the* $\mathsf{DLWR}_{n,m,q,p}(\mathcal{D})$ *problem with advantage $\epsilon$, such that, if $\mathcal{A}$ is an adaptive adversary (*INDr-ID-CPA*) with advantage $\epsilon'$, then it holds that $\epsilon' \leq \epsilon \cdot (d \cdot Q_H^d) + \mathrm{negl}(n)$.*

## 4 Improvement on Previous LWE-Based Scheme

### 4.1 Our Leveled Hierarchical Identity-Based FHE from LWE

Here, we also assume the maximal depth of the hierarchy is $d$ and the maximal homomorphically evaluable depth is $L$, and we choose a Gaussian parameter $\sigma = (\sigma_1, \cdots, \sigma_d)$ (the same as that in Sect. 3.1) and a Gaussian noise parameter $\alpha = (\alpha_1, \cdots, \alpha_d)$ needed in the encryption process. We omit the corresponding homomorphic addition and multiplication, since they are identical to that of LWR-based scheme presented in Sect. 3.

- **Setup**$(1^\lambda, 1^d, 1^L)$. Choose a lattice dimension parameter $n = n(\lambda, d, L)$, modulus $q = q(\lambda, d, L)$, also, choose parameter $m = m(\lambda, d, L) \geq 2n \log q$. Let $k = \lceil \log q \rceil$ and $N = (m+1) \cdot k$. Call the PPT algorithm $\mathsf{GenTrap}(1^n, 1^m, q)$ to generate a parity-check matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a trapdoor $\mathbf{X}$ with a tag $\mathbf{H}$ such that the distribution of $\mathbf{A}$ is statistically close to the uniform. As per Lemma 1, use the trapdoor $\mathbf{X}$ and a random basis $\mathbf{S}$ for $\Lambda_q^\perp(\mathbf{G})$ to generate a short basis $\mathbf{T_A}$ for $\Lambda_q^\perp(\mathbf{A})$. Choose uniformly at random a vector $\mathbf{u} \in \mathbb{Z}_q^n$. Finally, the master public parameter is $mpk := (\mathbf{A}, \mathbf{u})$, and the corresponding master secret key is $msk := (\mathbf{T_A})$.
- **Derive**$(mpk, \mathbf{T}_{\mathbf{id}|\ell}, \mathbf{id})$. Take as input public parameter $mpk$, a private basis $\mathbf{T}_{\mathbf{id}|\ell}$ corresponding to a "parent" identity $\mathbf{id}_{|\ell} = (\mathbf{id}_1, \cdots, \mathbf{id}_\ell)$ of level $\ell$ and a "child" identity $\mathbf{id} = (\mathbf{id}_1, \cdots, \mathbf{id}_\ell, \cdots, \mathbf{id}_k)$ of lower level $k$ where $k \leq d$, do the following processes:
  1. For $i \in [\ell]$, compute $\mathbf{H}(\mathbf{id}_i)$ and set $\mathbf{R}_{\mathbf{id}|\ell} = \mathbf{H}(\mathbf{id}_\ell) \cdots \mathbf{H}(\mathbf{id}_1) \in \mathbb{Z}^{m \times m}$. Then compute $\mathbf{B}_{\mathbf{id}|\ell} = \mathbf{A} \cdot \mathbf{R}_{\mathbf{id}|\ell}^{-1} \in \mathbb{Z}_q^{n \times m}$. Let $\mathbf{T}_{\mathbf{id}|\ell}$ be the short basis for $\Lambda_q^\perp(\mathbf{B}_{\mathbf{id}|\ell})$.
  2. Compute $\mathbf{R} = \mathbf{H}(\mathbf{id}_k) \cdots \mathbf{H}(\mathbf{id}_{\ell+1}) \in \mathbb{Z}^{m \times m}$ and then set $\mathbf{B_{id}} = \mathbf{B}_{\mathbf{id}|\ell} \cdot \mathbf{R}^{-1} \in \mathbb{Z}_q^{n \times m}$.

3. Invoke $\mathbf{T}' \leftarrow \mathsf{BasisDel}(\mathbf{B}_{\mathbf{id}|\ell}, \mathbf{T}_{\mathbf{id}|\ell}, \mathbf{R}, \sigma_k)$ to obtain a short random basis for $\Lambda_q^{\perp}(\mathbf{B}_{\mathbf{id}})$.
4. Output the delegated basis $\mathbf{T}_{\mathbf{id}} = \mathbf{T}'$.

– $\mathbf{Extract}(mpk, \mathbf{B}_{\mathbf{id}}, \mathbf{T}_{\mathbf{id}}, \mathbf{id})$. Take as input public parameter $mpk$, and an identity $\mathbf{id}$ of depth $|\mathbf{id}| = \ell$. Run the PPT algorithm $\mathsf{SamplePre}(\mathbf{B}_{\mathbf{id}}, \mathbf{T}_{\mathbf{id}}, \sigma_\ell, \mathbf{u})$ to sample a short vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{B}_{\mathbf{id}} \cdot \mathbf{x} = \mathbf{u} \pmod q$. Then output identity-specific public key $pk_{\mathbf{id}} : \mathbf{P} = \begin{bmatrix} \mathbf{u}^t \\ \mathbf{B}_{\mathbf{id}}^t \end{bmatrix}$, and the identity-specific secret key $sk_{\mathbf{id}} : \mathbf{s} = (1, -\mathbf{x})$. Note that $\mathbf{s}^t \cdot \mathbf{P} = 0 \pmod q$.
– $\mathbf{Enc}(pk_{\mathbf{id}}, \mathbf{id}, \mu)$. To encrypt a message $\mu \in \{0, 1\}$, sample a small matrix $\mathbf{M} \xleftarrow{\$} \{0,1\}^{n \times N}$ and a small noise matrix $\mathbf{E} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}, \alpha_\ell q}^{(m+1) \times N}$. Output a ciphertext $\mathbf{C} = \mathbf{P} \cdot \mathbf{M} + 2\mathbf{E} + \mu \mathbf{G} \in \mathbb{Z}_q^{(m+1) \times N}$.
– $\mathbf{Dec}(sk_{\mathbf{id}}, \mathbf{C})$. Choose the first column vector $\mathbf{c}$ of ciphertext $\mathbf{C}$. Output $\mu = \langle \mathbf{s}, \mathbf{c} \rangle_q \pmod 2$.

### 4.2 Correctness, Parameters and Security

Performing the decryption procedure on ciphertext in the scheme, we have $\langle \mathbf{s}, \mathbf{c} \rangle \equiv \mu + 2\langle \mathbf{e}, \mathbf{s} \rangle \bmod q$. According to Lemma 4, the noise term $\mathbf{e}$ is the column vector of $\mathbf{E} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}, \alpha_\ell q}^{(m+1) \times N}$ that satisfies $||\mathbf{e}|| \leq \sqrt{m+1} \cdot \alpha_\ell q$ with overwhelming probability, while $\mathbf{x} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$ is sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}), \sigma_\ell}$ that satisfies $||\mathbf{x}|| \leq \sqrt{m} \cdot \sigma_\ell$ with overwhelming probability. As with that in Sect. 3.2, we can set $\sigma_\ell = m^{\frac{3}{2}\ell} \cdot \omega(\log^{2\ell} m)$ and then $\alpha_\ell = \left(m^{\frac{3}{2}\ell + 2L + 1} \cdot \omega(\log^{2\ell+1} m)\right)^{-1}$. While according to Regev's reduction [27] which requires $\alpha_{\ell+1} q > 2\sqrt{n}$, we can choose $q$ of polynomial size such that $\alpha_\ell q = O(\sqrt{n}) > 2\sqrt{n}$. It follows that

$$|2\langle \mathbf{e}, \mathbf{s} \rangle| \leq 2||\mathbf{e}|| \cdot (||\mathbf{x}|| + 1) = O(\sqrt{n}) \cdot m^{\frac{3}{2}\ell + 1} \cdot \omega(\log^{2\ell} m) < q/2.$$

Moreover, similarly with our LWR-based leveled HIBFHE and [3], after performing homomorphic evaluations on ciphertexts, the noise grows linearly in $N + 1$ and asymmetrically in the ciphertexts' respective noises. For simplicity, we just present the result by the following theorem.

**Theorem 4.** *For the parameters $\lambda$, $d$, $L$, $n = n(\lambda, d, L)$ and $m = m(\lambda, d, L) \geq 2n \log q$, if the polynomial size modulus $q \geq (3n \log^2 q)^{\frac{3}{2}d + L + 1} \cdot \omega\big((2 \log n)^{2d}\big)$, our construction based on* LWE *is a correct $L$-leveled* HIBFHE.

The modulus $q$ is of polynomial size and the Gaussian noise rate $\alpha$ is of inverse-polynomial size in the parameter $n$, this allows the security to be based on certain worst-case lattice problems with polynomial approximation factors. As for the security, we note that the main difference between our LWR-based scheme and LWE-based scheme depends on **Enc** algorithm. The LWR-based scheme uses the scaled rounding function to hide plaintext contrast to the Gaussian noise

used in the LWE-based scheme, therefore the security proofs for both are almost identical, except that they are based on different hard problems. For completeness, we give the following theorem.

**Theorem 5.** *Let $\mathcal{A}$ be a PPT adversary that attacks our* LWE*-based scheme, and $Q_H$ be the number of hash $H$ queries made by $\mathcal{A}$ and $d$ be the maximal hierarchy depth, where $H$ is a hash function modeled as a random oracle. Then there is a PPT algorithm $\mathcal{B}$ that solves the* $\mathsf{DLWE}_{n,q,m,\chi}(\mathcal{D})$ *problem with advantage $\epsilon$, such that, if $\mathcal{A}$ is an adaptive adversary (*INDr-ID-CPA*) with advantage $\epsilon'$, then it holds that $\epsilon' \leq \epsilon \cdot (d \cdot Q_H^d) + \mathrm{negl}(n)$.*

## 5 Conclusion and Future Direction

We presented two leveled HIBFHE schemes from LWR and LWE. Our LWE-based leveled HIBFHE scheme is an improvement on the previous LWE-based leveled HIBFHE scheme. Our novel leveled HIBFHE scheme is based on LWR problem, which is, to the best of our knowledge, the first LWR-based leveled HIBFHE scheme. Our proposed LWR-based leveled HIBFHE scheme has bigger parameters than the previous LWE-based leveled HIBFHE scheme and our improved scheme, but it does not need Gaussian noise sampling in encryption process. Thus, the LWR-based leveled HIBFHE scheme still has advantage and can be seen as an alternative one. Furthermore, in this work we proved that our two leveled HIBFHE schemes are both secure against adaptive chosen-identity attack. However, the bootstrapping method cannot be used to transform our leveled HIBFHE into non-leveled (pure) HIBFHE, due to IBE's property of non-interactivity. Therefore, a subject of our future work is to design a pure IBFHE without indistinguishable obfuscator.

**Acknowledgments.** The authors would like to thank the anonymous reviewers for their detailed reviews and helpful comments. This research is supported in part by the National Nature Science Foundation of China (Nos. 61672030, 61272040 and U1705264; Nos. 61572132 and U1705264).

## References

1. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_28
2. Agrawal, S., Boneh, D., Boyen, X.: Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 98–115. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_6
3. Alperin-Sheriff, J., Peikert, C.: Faster bootstrapping with polynomial error. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 297–314. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_17

4. Alwen, J., Krenn, S., Pietrzak, K., Wichs, D.: Learning with rounding, revisited. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 57–74. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_4
5. Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 719–737. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_42
6. Bogdanov, A., Guo, S., Masny, D., Richelson, S., Rosen, A.: On the hardness of learning with rounding over small modulus. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9562, pp. 209–224. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49096-9_9
7. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
8. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: 48th Annual IEEE Symposium on Foundations of Computer Science 2007. FOCS 2007, pp. 647–657. IEEE (2007)
9. Brakerski, Z.: Fully homomorphic encryption without modulus switching from classical GapSVP. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 868–886. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_50
10. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In: Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, 8–10 January 2012, pp. 309–325 (2012)
11. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical hardness of learning with errors. In: Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, pp. 575–584. ACM (2013)
12. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: IEEE 52nd Annual Symposium on Foundations of Computer Science. FOCS 2011, Palm Springs, CA, USA, 22–25 October 2011, pp. 97–106 (2011)
13. Groot Bruinderink, L., Hülsing, A., Lange, T., Yarom, Y.: Flush, gauss, and reload – a cache attack on the BLISS lattice-based signature scheme. In: Gierlichs, B., Poschmann, A.Y. (eds.) CHES 2016. LNCS, vol. 9813, pp. 323–345. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53140-2_16
14. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_27
15. Clear, M., Hughes, A., Tewari, H.: Homomorphic encryption with access policies: characterization and new constructions. In: Youssef, A., Nitaj, A., Hassanien, A.E. (eds.) AFRICACRYPT 2013. LNCS, vol. 7918, pp. 61–87. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38553-7_4
16. Clear, M., McGoldrick, C.: Bootstrappable identity-based fully homomorphic encryption. In: Gritzalis, D., Kiayias, A., Askoxylakis, I. (eds.) CANS 2014. LNCS, vol. 8813, pp. 1–19. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-12280-9_1
17. Cocks, C.: An Identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45325-3_32

18. Fang, F., Li, B., Lu, X., Liu, Y., Jia, D., Xue, H.: (Deterministic) hierarchical identity-based encryption from learning with rounding over small modulus. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pp. 907–912. ACM (2016)
19. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. STOC 2009, Bethesda, MD, USA, 31 May–2 June 2009, pp. 169–178 (2009)
20. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, pp. 197–206. ACM (2008)
21. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 75–92. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_5
22. Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36178-2_34
23. Halevi, S., Shoup, V.: Bootstrapping for `HElib`. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 641–670. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_25
24. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_41
25. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, pp. 333–342. ACM (2009)
26. Pessl, P.: Analyzing the shuffling side-channel countermeasure for lattice-based signatures. In: Dunkelman, O., Sanadhya, S.K. (eds.) INDOCRYPT 2016. LNCS, vol. 10095, pp. 153–170. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-49890-4_9
27. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM (JACM) **56**(6), 34 (2009)
28. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
29. Sun, X., Yu, J., Wang, T., Sun, Z., Zhang, P.: Efficient identity-based leveled fully homomorphic encryption from RLWE. Secur. Commun. Netw. **9**(18), 5155–5165 (2016)
30. Wang, F., Wang, K., Li, B.: An efficient leveled identity-based FHE. Network and System Security. LNCS, vol. 9408, pp. 303–315. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25645-0_20
31. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_36
32. Xie, X., Xue, R., Zhang, R.: Deterministic public key encryption and identity-based encryption from lattices in the auxiliary-input setting. In: Visconti, I., De Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 1–18. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32928-9_1