IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received December 18, 2019, accepted January 21, 2020, date of publication February 3, 2020, date of current version February 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2971342

Leveled Certificateless Fully Homomorphic Encryption Schemes From Learning With Errors

MINGXIANG LI
Institute of Financial Research, Hebei Finance University, Baoding 071051, China
Science and Technology Finance Key Laboratory of Hebei Province, Baoding 071051, China

e-mail: limingxiang@hbfu.edu.cn

This work was supported by the Science and Technology Research Project of Higher Education of Hebei Province under Grant ZD2017228.

ABSTRACT Fully homomorphic encryption (FHE) is a form of public-key encryption that allows the computation of arbitrary functions on encrypted data without decrypting the data. As a result, it is a useful tool with numerous applications. Certificateless encryption (CLE) is a type of public-key encryption that combines the advantages of PKI-based public-key encryption with those of identity-based encryption (IBE). Thus, certificateless fully homomorphic encryption (CLFHE) has aroused considerable research interest. Recently, Chen, Hu, and Lian proposed a leveled certificateless homomorphic encryption (CLHE) scheme and proved its semantic security based on the learning with errors (LWE) problem in the random oracle model. However, their scheme supports only homomorphic addition, but not homomorphic multiplication. In this work, we construct two leveled CLFHE schemes using the approximate eigenvector method presented by Gentry, Sahai, and Waters. Based on the hardness of the LWE problem, we prove that one scheme satisfies adaptive semantic security and anonymity in the random oracle model, whereas the other satisfies selective semantic security and anonymity in the standard model.

INDEX TERMS Certificateless fully homomorphic encryption, learning with errors, random oracle model, standard model.

I. INTRODUCTION

Fully homomorphic encryption (FHE) [1], [2] is a variant of public-key encryption. It allows anyone to perform arbitrary computation on encrypted data. Hence, it is a useful tool with a number of attractive applications, such as private outsourcing of computation, privacy-preserving machine learning, and secure multiparty computation. Leveled FHE is a special variant of FHE. In a leveled FHE scheme, the system parameters may depend on the depth of the circuits that the system can evaluate. In 2013, Gentry, Sahai and Waters [3] (GSW) proposed a new technique for building FHE schemes of so-called approximate eigenvector method, and accordingly constructed a leveled FHE scheme based on the learning with errors (LWE) problem [4]. In the GSW scheme, the homomorphic evaluator does not need to obtain the user's evaluation key. Alperin-Sheriff and Peikert [5] subsequently provided a technically simpler variant of the GSW scheme by utilizing a gadget matrix $\mathbf{G}$ developed in [6].

Certificateless encryption (CLE) [7] is also a variant of public-key encryption. In a CLE scheme, a semi-trusted third party, referred to as the key generation center (KGC), calculates partial private keys for users in the system according to their identities. In this way, the CLE removes the need to distribute digital certificates. Moreover, a user also generates a public/private key pair by itself. Since the private key of a user is not available to the KGC, the CLE does not suffer from the key escrow problem that is inherent in identity-based encryption (IBE) [8], [9]. Consequently, CLE is public-key encryption with unique characteristics. Dent [10], [11] provided a review of the syntax and security models for the CLE scheme. Recently, several CLE schemes based on the LWE problem have been proposed in the random oracle model [12] or standard model [13].

Certificateless fully homomorphic encryption (CLFHE) has drawn considerable attention from researchers. In 2013, Guang, Gu, and Zhu [14] proposed a leveled CLFHE scheme

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

using the re-linearization technique presented in [15] and proved that it was semantically secure based on the hardness of the LWE problem in the random oracle model. However, their scheme incurs a very high computational complexity. Thus, Chen, Hu, and Lian [16] proposed a leveled certificateless homomorphic encryption (CLHE) scheme using the approximate eigenvector method presented in [3] and proved its semantic security based on the hardness of the LWE problem in the random oracle model. This scheme has a relatively lower time complexity in comparison with the scheme proposed by Guang et al. However, the scheme proposed by Chen et al. supports only homomorphic addition, but not homomorphic multiplication. Thus, constructing an efficient leveled CLFHE scheme is a problem that remains to be addressed.

A. OUR CONTRIBUTIONS

In this work, we focus on designing leveled CLFHE schemes. By utilizing the approximate eigenvector method [3], a lot of leveled identity-based FHE schemes [17]–[20] have been proposed. Considering that the approximate eigenvector method can be used to eliminate a user's evaluation key, we adopt it to design leveled CLFHE schemes. The contributions of this work are as follows:

1) We propose a leveled CLFHE scheme in the random oracle model. Specifically, we first construct a leveled CLFHE scheme using the technically simpler GSW variant presented in [5] and the preimage sampling algorithm SamplePre presented in [21]. Next, we provide a parameter setting for the proposed CLFHE scheme. Finally, we prove that the proposed CLFHE scheme is semantically secure and anonymous for adaptive chosen-identity based on the hardness of the LWE problem in the random oracle model.
2) We remove the random oracles and propose a leveled CLFHE scheme in the standard model. We first construct a leveled CLFHE scheme using the technically simpler GSW variant presented in [5] and the Gaussian sampling algorithm SampleLeft presented in [22]. We then provide a parameter setting for the proposed CLFHE scheme. Finally, by exploiting the Gaussian sampling algorithm SampleRight presented in [22], we prove that the proposed CLFHE scheme is semantically secure and anonymous for selective-identity based on the hardness of the LWE problem in the standard model.

B. PAPER ORGANIZATION

The remainder of this paper is organized as follows. In Section II, we give the preliminaries including notations, lattice backgrounds, and the LWE problem. We describe the syntax and security models for CLFHE schemes in Section III. In Section IV, we put forth a leveled CLFHE scheme based on the LWE problem in the random oracle model. In Section V, we put forward a leveled CLFHE scheme based on the LWE problem in the standard model. Finally, we conclude and outline some future work in Section VI.

II. PRELIMINARIES

A. NOTATIONS

For a positive integer k, we let $[k] = \{1, \ldots, k\}$. For an integer modulus q, we let $\mathbb{Z}_q = (-q/2, q/2] \cap \mathbb{Z}$. We treat vectors as column vectors and denote them with bold lowercase letters, e.g., $\mathbf{x}$. We denote matrices with bold uppercase letters, e.g., $\mathbf{X}$, and view a matrix $\mathbf{X}$ as the set $\{\mathbf{x}_i\}$ of its column vectors. We denote by $\widetilde{\mathbf{X}}$ the Gram-Schmidt ordered orthogonalization of a matrix $\mathbf{X}$. We denote the Euclidean norm of a vector $\mathbf{x}$ by $\|\mathbf{x}\|$. For a matrix $\mathbf{X}$, the Euclidean norm of $\mathbf{X}$ is defined as $\|\mathbf{X}\| = \max_j \|\mathbf{x}_j\|$. Hence, for an $n \times m$ matrix $\mathbf{X}$ and an $n \times m'$ matrix $\mathbf{Y}$, it holds that

$$\|\mathbf{X}^{\mathrm{T}} \cdot \mathbf{Y}\| \leq \sqrt{m} \cdot \|\mathbf{X}\| \cdot \|\mathbf{Y}\|.$$

Throughout this paper, we let λ denote a security parameter and $\mathrm{negl}(\lambda)$ denote a negligible function. The statistical distance between two random variables X and Y over a countable domain S is defined as $\Delta(X; Y) = \max_{A \subseteq S} |\Pr[X \in A] - \Pr[Y \in A]|$. Two ensembles of random variables $\{X_\lambda\}$ and $\{Y_\lambda\}$ are said to be statistically close if $\Delta(X_\lambda; Y_\lambda) = \mathrm{negl}(\lambda)$. Two ensembles of random variables $\{X_\lambda\}$ and $\{Y_\lambda\}$ are computationally indistinguishable if for every polynomial-time attacker $\mathcal{A}$, $\left|\Pr\left[\mathcal{A}\left(1^\lambda, X_\lambda\right) = 1\right] - \Pr\left[\mathcal{A}\left(1^\lambda, Y_\lambda\right) = 1\right]\right| = \mathrm{negl}(\lambda)$.

B. LATTICE BACKGROUNDS

1) INTEGER LATTICES

Definition 1: Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m) \in \mathbb{R}^{m \times m}$ be a matrix whose columns are linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \mathbb{R}^m$. The m-dimensional lattice Λ generated by the basis $\mathbf{B}$ is defined as the set

$$\Lambda = \mathcal{L}(\mathbf{B}) = \left\{\mathbf{y} \in \mathbb{R}^m : \exists \mathbf{s} \in \mathbb{Z}^m,\ \mathbf{y} = \mathbf{B}\mathbf{s} = \sum_{i=1}^{m} s_i \mathbf{b}_i\right\}.$$

Definition 2: For a positive integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, define two m-dimensional integer lattices:

$$\Lambda_q^{\perp}(\mathbf{A}) = \left\{\mathbf{e} \in \mathbb{Z}^m : \mathbf{A}\mathbf{e} = \mathbf{0} \mod q\right\} \subseteq \mathbb{Z}^m,$$
$$\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \left\{\mathbf{e} \in \mathbb{Z}^m : \mathbf{A}\mathbf{e} = \mathbf{u} \mod q\right\} \subseteq \mathbb{Z}^m.$$

We observe that if $\mathbf{x} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$, then $\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \Lambda_q^{\perp}(\mathbf{A}) + \mathbf{x}$, and hence $\Lambda_q^{\mathbf{u}}(\mathbf{A})$ is a shift of $\Lambda_q^{\perp}(\mathbf{A})$.

Proposition 1 ([23], [24]): There is a PPT algorithm GenBasis $(1^n, 1^m, q)$ that, for $m \geq 6n \log q$, outputs $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{T} \in \mathbb{Z}^{m \times m}$ such that the distribution of $\mathbf{A}$ is statistically close to uniform over $\mathbb{Z}_q^{n \times m}$, $\mathbf{T}$ is a basis of $\Lambda_q^{\perp}(\mathbf{A})$, and $\|\widetilde{\mathbf{T}}\| \leq O(\sqrt{n \log q})$.

2) GAUSSIANS ON LATTICES

Definition 3: For any vector $\mathbf{c} \in \mathbb{R}^m$ and real $\sigma > 0$, the Gaussian function on $\mathbb{R}^m$ with center $\mathbf{c}$ and parameter σ is defined as

$$\forall \mathbf{y} \in \mathbb{R}^m,\ \rho_{\sigma,\mathbf{c}}(\mathbf{y}) = \exp\left(-\pi \|\mathbf{y} - \mathbf{c}\|^2/\sigma^2\right).$$

For any $\mathbf{c} \in \mathbb{R}^m$, $\sigma > 0$, and m-dimensional lattice Λ, the discrete Gaussian distribution over Λ is defined as

$$\forall \mathbf{y} \in \Lambda,\ D_{\Lambda,\sigma,\mathbf{c}}(\mathbf{y}) = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{y})}{\rho_{\sigma,\mathbf{c}}(\Lambda)}.$$

The subscripts σ and $\mathbf{c}$ are taken as 1 and 0 when omitted.

Proposition 2 ([25]): For any m-dimensional lattice Λ, vector $\mathbf{c} \in \mathbb{R}^m$, and reals $0 < \epsilon < 1$, $\sigma \geq \eta_\epsilon(\Lambda)$, we have

$$\Pr\left[\mathbf{y} \leftarrow D_{\Lambda,\sigma,\mathbf{c}} : \|\mathbf{y} - \mathbf{c}\| > \sigma\sqrt{m}\right] \leq \frac{1+\epsilon}{1-\epsilon} \cdot 2^{-m},$$

where $\eta_\epsilon(\Lambda)$ is the smoothing parameter of Λ and for any basis $\mathbf{B}$ of Λ, $\eta_\epsilon(\Lambda) \leq \|\widetilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log m})$.

3) SAMPLING ALGORITHMS

Proposition 3 ([21]): Let $q \geq 2$ and $m > n$. Then there exists a PPT algorithm $\mathsf{SamplePre}(\mathbf{A}, \mathbf{T_A}, \mathbf{u}, \sigma)$ that, given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a basis $\mathbf{T_A}$ of $\Lambda_q^{\perp}(\mathbf{A})$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and a parameter $\sigma \geq \|\widetilde{\mathbf{T_A}}\| \cdot \omega(\sqrt{\log m})$, outputs a vector $\mathbf{x} \in \mathbb{Z}^m$ sampled from a distribution that is statistically close to $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma}$.

Proposition 4 ([22]): Let $q \geq 2$ and $m \geq 2n \log q$. There exists a PPT algorithm $\mathsf{SampleLeft}(\mathbf{A}, \mathbf{A}_1, \mathbf{T_A}, \mathbf{u}, \sigma)$ that, given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a matrix $\mathbf{A}_1 \in \mathbb{Z}_q^{n\times m}$, a basis $\mathbf{T_A}$ of $\Lambda_q^{\perp}(\mathbf{A})$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and a parameter $\sigma \geq \|\widetilde{\mathbf{T_A}}\| \cdot \omega(\sqrt{\log m})$, outputs a vector $\mathbf{x} \in \mathbb{Z}^{2m}$ sampled from a distribution that is statistically close to $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}|\mathbf{A}_1),\sigma}$.

Proposition 5 ([22]): Let $q \geq 2$ and $m > n$. Then there exists a PPT algorithm $\mathsf{SampleRight}(\mathbf{A}, \mathbf{B}, \mathbf{R}, \mathbf{T_B}, \mathbf{u}, \sigma)$ that, given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$, a matrix $\mathbf{R} \in \mathbb{Z}^{m\times m}$ sampled from $D^{m\times m}_{\mathbb{Z},\omega(\sqrt{\log m})}$, a basis $\mathbf{T_B}$ of $\Lambda_q^{\perp}(\mathbf{B})$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and a parameter $\sigma \geq \|\widetilde{\mathbf{T_B}}\| \cdot m \cdot \omega(\sqrt{\log m})^2$, outputs a vector $\mathbf{x} \in \mathbb{Z}^{2m}$ sampled from a distribution that is statistically close to $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}|\mathbf{AR}+\mathbf{B}),\sigma}$.

C. THE LWE Problem

The LWE problem was introduced by Regev [4]. For positive integers n and $q \geq 2$, a vector $\mathbf{s} \in \mathbb{Z}_q^n$, and a probability distribution χ over $\mathbb{Z}$, define the LWE distribution $A_{\mathbf{s},\chi}$ to be the distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing a vector $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ uniformly at random and an error term $e \leftarrow \chi$, and outputting $(\mathbf{a}, b = \mathbf{a}^{\mathrm{T}} \cdot \mathbf{s} + e \mod q)$. The decisional LWE (DLWE) is defined as follows.

Definition 4: Let $n = n(\lambda)$ be an integer dimension, let $q = q(\lambda) \geq 2$ be an integer modulus, and let $\chi = \chi(\lambda)$ be an error distribution over $\mathbb{Z}$. The average-case $\mathsf{DLWE}_{n,q,\chi}$ problem is to distinguish between any desired number of samples $(\mathbf{a}_i, b_i) \leftarrow A_{\mathbf{s},\chi}$, and the same number of samples chosen from the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$. The $\mathsf{DLWE}_{n,q,\chi}$ assumption is that the $\mathsf{DLWE}_{n,q,\chi}$ problem is infeasible.

There are reductions between the $\mathsf{DLWE}_{n,q,\chi}$ assumption and the standard lattice assumptions as follows. These reductions take the error distribution χ to be a discrete Gaussian distribution $D_{\mathbb{Z},\alpha q}$ that has parameter αq for some $\alpha \in (0, 1)$.

Proposition 6 ([4], [6], [26], [27], Stated as Corollary 1 From [28]): Let $q = q(n) \in \mathbb{N}$ be either a prime power or a product of small (size poly(n)) distinct primes, and let $\alpha \geq 2\sqrt{n}/q$. If there exists an efficient algorithm that solves the average-case $\mathsf{DLWE}_{n,q,D_{\mathbb{Z},\alpha q}}$ problem, then:

- there exists an efficient quantum algorithm that solves $\mathsf{GapSVP}_{\tilde{O}(n/\alpha)}$ and $\mathsf{SIVP}_{\tilde{O}(n/\alpha)}$ in the worst-case for any n-dimensional lattices;
- if in addition $q \geq \tilde{O}(2^{n/2})$, then there exists an efficient classical algorithm that solves $\mathsf{GapSVP}_{\tilde{O}(n/\alpha)}$ in the worst-case for any n-dimensional lattices.

We extend the LWE distribution to $w \geq 1$ secrets, defining $A_{\mathbf{S},\chi}$ for $\mathbf{S} \in \mathbb{Z}_q^{n\times w}$ to be the distribution obtained by choosing a vector $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ and an error vector $\mathbf{e} \leftarrow \chi^w$, and outputting $(\mathbf{a}, \mathbf{b}^{\mathrm{T}} = \mathbf{a}^{\mathrm{T}} \cdot \mathbf{S} + \mathbf{e}^{\mathrm{T}} \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^{1\times w}$. Clearly, distinguishing such samples from uniformly random is as hard as the $\mathsf{DLWE}_{n,q,\chi}$ problem. It is generally convenient to group many sample pairs together in matrices. We can thus express the $\mathsf{DLWE}_{n,q,\chi}$ problem as distinguish any desired number of sample pairs $(\mathbf{A}, \mathbf{B}^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}} \cdot \mathbf{S} + \mathbf{E}^{\mathrm{T}} \mod q) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times w}$ from uniformly random.

III. SYNTAX AND SECURITY MODELS FOR CLFHE

A. SYNTAX DEFINITION

Dent [10], [11] gave three formal definitions for CLE, namely, AP definition [7], BSS definition [29], and LK definition [30]. Using the BSS definition [29] in which a user cannot publish its public key until it has obtained a partial private key, we define a leveled CLFHE scheme CLFHE $=$ (Setup, $\mathsf{Extract}$, KeyGen, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$, Eval) as follows.

- **Setup**$(1^\lambda, 1^L)$: This algorithm is run by the KGC. It takes as input a security parameter λ and a circuit depth L. It outputs a master public key mpk and a master private key msk.
- **Extract**(mpk, msk, id): This algorithm is run by the KGC. It takes as input a master public key mpk, a master private key msk, and an identity $id \in \mathcal{ID}$, where $\mathcal{ID}$ is the identity space of the scheme. It outputs a partial private key psk_{id}.
- **KeyGen**(mpk, id, psk_{id}): This algorithm takes as input a master public key mpk, an identity id, and a partial private key psk_{id}. It outputs a public key pk_{id} and a private key sk_{id}.
- **Encrypt**(mpk, id, pk_{id}, μ): This algorithm takes as input a master public key mpk, an identity id, a public key pk_{id}, and a message $\mu \in \mathcal{M}$, where $\mathcal{M}$ is the message space of the scheme. It outputs a ciphertext $c \in \mathcal{C}$, where $\mathcal{C}$ is the ciphertext space of the scheme.

- **Decrypt**(mpk, sk_{id}, c): This algorithm takes as input a master public key mpk, a private key sk_{id}, and a ciphertext $c \in \mathcal{C}$. It outputs a message $\mu \in \mathcal{M}$ or a failure symbol $\perp$.
- **Eval**$(mpk, id, f, c_1, \ldots, c_\ell)$: This algorithm takes as input a master public key mpk, an identity id, a circuit $f : \mathcal{M}^\ell \to \mathcal{M}$ of depth $\leq L$, and ciphertexts $\{c_i \leftarrow \mathsf{Encrypt}(mpk, id, pk_{id}, \mu_i)\}_{i \in [\ell]}$ under the identity id. It outputs an evaluated ciphertext $c_f \in \mathcal{C}$.

Correctness. A CLFHE scheme is correct if for any identity $id \in \mathcal{ID}$, circuit $f : \mathcal{M}^\ell \to \mathcal{M}$ of depth $\leq L$, and messages $\{\mu_i \in \mathcal{M}\}_{i \in [\ell]}$, it holds that

$$\Pr\left[\mathsf{Decrypt}(mpk, sk_{id}, c_f) \neq f(\mu_1, \ldots, \mu_\ell)\right] = \text{negl}(\lambda),$$

where $c_f \leftarrow \mathsf{Eval}(mpk, id, f, c_1, \ldots, c_\ell)$.

Compactness. A CLFHE scheme is compact if there exists a polynomial $p(\lambda, L)$ such that

$$|c_f| \leq p(\lambda, L).$$

That is to say, the size of the evaluated ciphertext c_f should be independent of f and ℓ, but can depend on λ and L.

Security. The security model for CLFHE is the same as that for CLE. There are two types of attackers, Type I attacker (denoted by $\mathcal{A}_I$) and Type II attacker (denoted by $\mathcal{A}_{II}$), for the CLE scheme. A Type I attacker acts as an outsider that can replace the public keys, whereas a Type II attacker acts as the KGC that cannot replace the public keys, but can access the master private key. According to the security models for CLE given by Dent [10], [11], we define the indistinguishability from random under an adaptive-identity chosen-plaintext attack (INDr-ID-CPA) model and the indistinguishability from random under a selective-identity chosen-plaintext attack (INDr-sID-CPA) model for CLFHE in the following two sections. The concept of the indistinguishability from random under a chosen-plaintext attack implies both semantic security and recipient anonymity. The selective-identity security is a weaker variant of the adaptive-identity security. In the selective-identity security model, the attacker must fix an identity it intends to attack before seeing the master public key.

B. ADAPTIVE-IDENTITY SECURITY MODEL FOR CLFHE

The INDr-ID-CPA security for CLFHE against Type I attacks is defined by the following game.

Setup: The challenger runs $(mpk, msk) \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$ and sends mpk to the attacker $\mathcal{A}_I$.

Phase 1: $\mathcal{A}_I$ may adaptively make the following queries:

- Extract partial private key: If $\mathcal{A}_I$ submits an identity $id \in \mathcal{ID}$ to the challenger, the challenger runs $psk_{id} \leftarrow \mathsf{Extract}(mpk, msk, id)$ and returns the partial private key psk_{id} to $\mathcal{A}_I$.
- Request public key: If $\mathcal{A}_I$ submits an identity $id \in \mathcal{ID}$ to the challenger, the challenger runs $(pk_{id}, sk_{id}) \leftarrow \mathsf{KeyGen}(mpk, id, psk_{id})$ and $psk_{id} \leftarrow \mathsf{Extract}(mpk, msk, id)$ (as necessary) and returns the public key pk_{id} to $\mathcal{A}_I$. The challenger also stores the tuple (id, pk_{id}, sk_{id}).
- Replace public key: If $\mathcal{A}_I$ submits an identity $id \in \mathcal{ID}$ and a public key pk'_{id} to the challenger, the challenger replaces the public key of id with pk'_{id} and updates the corresponding information in the storage.

Challenge: Once $\mathcal{A}_I$ decides that Phase 1 is over, it outputs a target identity $id^* \in \mathcal{ID}$ and a message $\mu \in \mathcal{M}$ on which it wishes to be challenged. The challenger randomly chooses a bit $b \leftarrow \{0, 1\}$ and a ciphertext $c \leftarrow \mathcal{C}$. If $b = 0$, it sets the challenge ciphertext to $c_0^* = \mathsf{Encrypt}(mpk, id^*, pk_{id^*}, \mu)$, where pk_{id^*} can be the replaced public key pk'_{id^*}. If $b = 1$, it sets the challenge ciphertext to $c_1^* = c$. The challenger sends c_b^* to $\mathcal{A}_I$.

Phase 2: $\mathcal{A}_I$ may continue to make the queries as described in Phase 1.

Guess: Finally, $\mathcal{A}_I$ outputs a guess $b' \in \{0, 1\}$.

In the above game, $\mathcal{A}_I$ is not allowed to replace the public key of id^* in Phase 1 and request the partial private key of id^* in Phase 1 or 2 because it can then compute a full private key for id^*.

The attacker $\mathcal{A}_I$ wins the game if $b = b'$. We define the advantage of $\mathcal{A}_I$ in attacking the CLFHE scheme as

$$\text{Adv}^{\text{INDr-ID-CPA}}_{\text{CLFHE},\mathcal{A}_I}(\lambda) = \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|.$$

The CLFHE scheme is considered INDr-ID-CPA secure against Type I attacks if $\text{Adv}^{\text{INDr-ID-CPA}}_{\text{CLFHE},\mathcal{A}_I}(\lambda) = \text{negl}(\lambda)$.

The INDr-ID-CPA security for CLFHE against Type II attacks is defined by the following game.

Setup: The challenger runs $(mpk, msk) \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$ and sends mpk and msk to the attacker $\mathcal{A}_{II}$.

Phase 1: $\mathcal{A}_{II}$ may adaptively make the following queries:

- Request public key: If $\mathcal{A}_{II}$ submits an identity $id \in \mathcal{ID}$ and a partial private key psk_{id} to the challenger, the challenger runs $(pk_{id}, sk_{id}) \leftarrow \mathsf{KeyGen}(mpk, id, psk_{id})$ and returns the public key pk_{id} to $\mathcal{A}_{II}$.

Challenge: $\mathcal{A}_{II}$ outputs a target identity $id^* \in \mathcal{ID}$ and a message $\mu \in \mathcal{M}$. The challenger picks a random bit $b \leftarrow \{0, 1\}$ and a random ciphertext $c \leftarrow \mathcal{C}$. If $b = 0$, it sets the challenge ciphertext to $c_0^* = \mathsf{Encrypt}(mpk, id^*, pk_{id^*}, \mu)$. If $b = 1$, it sets the challenge ciphertext to $c_1^* = c$. The challenger sends c_b^* to $\mathcal{A}_{II}$.

Phase 2: $\mathcal{A}_{II}$ may continue to make the queries as described in Phase 1.

Guess: $\mathcal{A}_{II}$ outputs a guess $b' \in \{0, 1\}$.

The attacker $\mathcal{A}_{II}$ wins the game if $b = b'$. We define the advantage of $\mathcal{A}_{II}$ in attacking the CLFHE scheme as

$$\text{Adv}^{\text{INDr-ID-CPA}}_{\text{CLFHE},\mathcal{A}_{II}}(\lambda) = \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|.$$

The CLFHE scheme is considered INDr-ID-CPA secure against Type II attacks if $\text{Adv}^{\text{INDr-ID-CPA}}_{\text{CLFHE},\mathcal{A}_{II}}(\lambda) = \text{negl}(\lambda)$.

C. SELECTIVE-IDENTITY SECURITY MODEL FOR CLFHE

The INDr-sID-CPA security for CLFHE against Type I attacks is defined by the following game.

Init: The attacker $\mathcal{A}_I$ outputs an identity $id^* \in \mathcal{ID}$ on which it wishes to be challenged.

Setup: The challenger runs $(mpk, msk) \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$ and sends mpk to $\mathcal{A}_I$.

Phase 1: $\mathcal{A}_I$ may adaptively make partial private key extraction, public key request, and public key replacement queries. The challenger responds to these queries as outlined in Section III-B.

Challenge: Once $\mathcal{A}_I$ decides that Phase 1 is over, it outputs a message $\mu \in \mathcal{M}$ on which it wishes to be challenged. The challenger randomly chooses a bit $b \leftarrow \{0, 1\}$ and a ciphertext $c \leftarrow \mathcal{C}$. If $b = 0$, it sets the challenge ciphertext to $c_0^* = \mathsf{Encrypt}(mpk, id^*, pk_{id^*}, \mu)$, where pk_{id^*} may be the replaced public key pk'_{id^*}. If $b = 1$, it sets the challenge ciphertext to $c_1^* = c$. The challenger sends c_b^* to $\mathcal{A}_I$.

Phase 2: $\mathcal{A}_I$ may continue to make the queries as described in Phase 1.

Guess: Finally, $\mathcal{A}_I$ outputs a guess $b' \in \{0, 1\}$.

In the above game, $\mathcal{A}_I$ cannot replace the public key of id^* in Phase 1 and request the partial private key of id^* in Phase 1 or 2 because this would otherwise make it possible to compute the full private key for id^*.

The attacker $\mathcal{A}_I$ wins the game if $b = b'$. We define the advantage of $\mathcal{A}_I$ in attacking the CLFHE scheme as

$$\mathrm{Adv}^{\mathrm{INDr-sID-CPA}}_{\mathrm{CLFHE},\mathcal{A}_I}(\lambda) = \left|\Pr\big[b = b'\big] - \frac{1}{2}\right|.$$

The CLFHE scheme is said to be INDr-sID-CPA secure against Type I attacks if $\mathrm{Adv}^{\mathrm{INDr-sID-CPA}}_{\mathrm{CLFHE},\mathcal{A}_I}(\lambda) = \mathrm{negl}(\lambda)$.

The INDr-sID-CPA security for CLFHE against Type II attacks is defined by the following game.

Init: The attacker $\mathcal{A}_{II}$ outputs an identity $id^* \in \mathcal{ID}$.

Setup: The challenger runs $(mpk, msk) \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$ and sends mpk and msk to $\mathcal{A}_{II}$.

Phase 1: $\mathcal{A}_{II}$ may adaptively make public key request queries. The challenger responds to these queries as outlined in Section III-B.

Challenge: $\mathcal{A}_{II}$ outputs a message $\mu \in \mathcal{M}$. The challenger picks a random bit $b \leftarrow \{0, 1\}$ and a random ciphertext $c \leftarrow \mathcal{C}$. If $b = 0$, it sets the challenge ciphertext to $c_0^* = \mathsf{Encrypt}(mpk, id^*, pk_{id^*}, \mu)$. If $b = 1$, it sets the challenge ciphertext to $c_1^* = c$. The challenger sends c_b^* to $\mathcal{A}_{II}$.

Phase 2: $\mathcal{A}_{II}$ may continue to make the queries as described in Phase 1.

Guess: $\mathcal{A}_{II}$ outputs a guess $b' \in \{0, 1\}$.

The attacker $\mathcal{A}_{II}$ wins the game if $b = b'$. We define the advantage of $\mathcal{A}_{II}$ in attacking the CLFHE scheme as

$$\mathrm{Adv}^{\mathrm{INDr-sID-CPA}}_{\mathrm{CLFHE},\mathcal{A}_{II}}(\lambda) = \left|\Pr\big[b = b'\big] - \frac{1}{2}\right|.$$

The CLFHE scheme is said to be INDr-sID-CPA secure against Type II attacks if $\mathrm{Adv}^{\mathrm{INDr-sID-CPA}}_{\mathrm{CLFHE},\mathcal{A}_{II}}(\lambda) = \mathrm{negl}(\lambda)$.

IV. A LEVELED CLFHE SCHEME IN THE RANDOM ORACLE MODEL

A. CONSTRUCTION

The proposed leveled CLFHE scheme in the random oracle model is described as follows.

Setup$(1^\lambda, 1^L)$: On input a security parameter λ and a circuit depth L, do:

1) Set the parameters $n = n(\lambda, L)$, $m = m(\lambda, L)$, $\alpha = \alpha(\lambda, L)$, $q = q(\lambda, L)$, $\sigma_1 = \sigma_1(\lambda, L)$, and $\sigma_2 = \sigma_2(\lambda, L)$ as specified in Section IV-B below.
2) Define the gadget matrix $\mathbf{G} = \mathbf{I}_{2m+1} \otimes \mathbf{g}^{\mathrm{T}} \in \mathbb{Z}_q^{(2m+1)\times N}$, where $\mathbf{g} = \left(1, \ldots, 2^{\lceil \log q \rceil - 1}\right)^{\mathrm{T}} \in \mathbb{Z}_q^{\lceil \log q \rceil}$, $N = (2m + 1) \cdot \lceil \log q \rceil$. Define the inverse function $\mathbf{G}^{-1} : \mathbb{Z}_q^{(2m+1)\times N} \rightarrow \{0, 1\}^{N\times N}$ that expands each entry $a \in \mathbb{Z}_q$ of the input matrix into a vector $\left(a_0, \ldots, a_{\lceil \log q \rceil - 1}\right)^{\mathrm{T}}$, where a_i is the ith bit in a's binary representation. For any matrix $\mathbf{X} \in \mathbb{Z}_q^{(2m+1)\times N}$, it is clear that $\mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{X}) = \mathbf{X}$ holds. The definitions of $\mathbf{G}$ and $\mathbf{G}^{-1}$ can also be found in [31], [32].
3) Invoke the algorithm $\mathsf{GenBasis}$ $(1^n, 1^m, q)$ to generate a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a basis $\mathbf{T_A}$ for $\Lambda^\perp(\mathbf{A})$ such that $\|\widetilde{\mathbf{T_A}}\| \le O(\sqrt{n \log q})$.
4) Select two matrices $\mathbf{V}, \mathbf{W} \leftarrow \mathbb{Z}_q^{n\times m}$ at random.
5) Select a cryptographic hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^n$.
6) Output a master public key $mpk = \big(\mathbf{A}, \mathbf{V}, \mathbf{W}, H\big)$ and a master private key $msk = \mathbf{T_A}$.

Extract(mpk, msk, id): On input a master private key msk and an identity $id \in \{0, 1\}^*$, do:

1) Compute $\mathbf{u} = H(id)$.
2) Invoke the algorithm $\mathsf{SamplePre}(\mathbf{A}, \mathbf{T_A}, \mathbf{u}, \sigma_1)$ to sample a vector $\mathbf{d} \in \mathbb{Z}^m$. Note that $\mathbf{A} \cdot \mathbf{d} = \mathbf{u} \mod q$ and $\mathbf{d}$ is distributed as $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma_1}$ by Proposition 3.
3) Output a partial private key $psk_{id} = \mathbf{d}$.

KeyGen(mpk, id, psk_{id}): On input an identity $id \in \{0, 1\}^*$ and a partial private key $psk_{id} = \mathbf{d}$, do:

1) Sample a vector $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,\sigma_2}$.
2) Let $\mathbf{v} = \mathbf{V} \cdot \mathbf{x} \mod q$.
3) Let $\mathbf{w} = \mathbf{W} \cdot \mathbf{d} \mod q$.
4) Let $\mathbf{z} = \begin{pmatrix} -\mathbf{d} \\ -\mathbf{x} \\ 1 \end{pmatrix} \in \mathbb{Z}^{2m+1}$.
5) Output a public key $pk_{id} = (\mathbf{v}, \mathbf{w})$ and a private key $sk_{id} = \mathbf{z}$.

Encrypt(mpk, id, pk_{id}, μ): On input an identity $id \in \{0, 1\}^*$, a public key pk_{id}, and a message $\mu \in \{0, 1\}$, do:

1) Compute $\mathbf{u} = H(id)$.
2) Pick three matrices $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3 \leftarrow \mathbb{Z}_q^{n\times N}$ at random.
3) Sample three noise matrices $\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3 \leftarrow D^{m\times N}_{\mathbb{Z},\alpha q}$, and sample three noise vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \leftarrow D^N_{\mathbb{Z},\alpha q}$.
4) Output a ciphertext $\mathbf{C}$ given below.

$$\mathbf{C} = \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \mathbf{u}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \mathbf{v}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G} \in \mathbb{Z}_q^{(2m+1)\times N}.$$

Decrypt$(mpk, sk_{id}, \mathbf{C})$: On input a private key $sk_{id} = \mathbf{z}$ and a ciphertext $\mathbf{C}$, do:

1) Let $\mathbf{c}$ be the penultimate column of $\mathbf{C}$.
2) Output a message

$$\mu = \left\lfloor \frac{\mathbf{z}^{\mathrm{T}} \cdot \mathbf{c}}{2^{\lceil \log q \rceil - 2}} \right\rceil .$$

Add$(mpk, id, \mathbf{C}_1, \mathbf{C}_2)$: On input two ciphertexts $\mathbf{C}_1$, $\mathbf{C}_2$ under the same identity id, output

$$\mathbf{C}_{\mathrm{Add}} = \mathbf{C}_1 + \mathbf{C}_2 \in \mathbb{Z}_q^{(2m+1)\times N}.$$

Mult$(mpk, id, \mathbf{C}_1, \mathbf{C}_2)$: On input two ciphertexts $\mathbf{C}_1$, $\mathbf{C}_2$ under the same identity id, output

$$\mathbf{C}_{\mathrm{Mult}} = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \in \mathbb{Z}_q^{(2m+1)\times N}.$$

B. CORRECTNESS AND PARAMETER SELECTION

For a ciphertext $\mathbf{C} \leftarrow$ Encrypt(mpk, id, pk_{id}, μ), we have

$$\begin{aligned}\mathbf{z}^{\mathrm{T}}\mathbf{C} &= \mathbf{z}^{\mathrm{T}} \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \mathbf{u}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \mathbf{v}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} \\ &\quad + \mu \cdot \mathbf{z}^{\mathrm{T}}\mathbf{G} \\ &= \underbrace{\mathbf{e}_1^{\mathrm{T}} + \mathbf{e}_2^{\mathrm{T}} + \mathbf{e}_3^{\mathrm{T}} - \mathbf{d}^{\mathrm{T}}\mathbf{E}_1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}_2 - \mathbf{d}^{\mathrm{T}}\mathbf{E}_3}_{\text{error term}} \\ &\quad + \mu \cdot \mathbf{z}^{\mathrm{T}}\mathbf{G}.\end{aligned}$$

We write $\mathbf{r}^{\mathrm{T}} = \mathbf{e}_1^{\mathrm{T}} + \mathbf{e}_2^{\mathrm{T}} + \mathbf{e}_3^{\mathrm{T}} - \mathbf{d}^{\mathrm{T}}\mathbf{E}_1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}_2 - \mathbf{d}^{\mathrm{T}}\mathbf{E}_3$. The error term is bounded by

$$\begin{aligned}\|\mathbf{r}^{\mathrm{T}}\| &= \|\mathbf{e}_1^{\mathrm{T}} + \mathbf{e}_2^{\mathrm{T}} + \mathbf{e}_3^{\mathrm{T}} - \mathbf{d}^{\mathrm{T}}\mathbf{E}_1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}_2 - \mathbf{d}^{\mathrm{T}}\mathbf{E}_3\| \\ &\le \|\mathbf{e}_1^{\mathrm{T}} + \mathbf{e}_2^{\mathrm{T}} + \mathbf{e}_3^{\mathrm{T}}\| + \|\mathbf{d}^{\mathrm{T}}\mathbf{E}_1 + \mathbf{x}^{\mathrm{T}}\mathbf{E}_2 + \mathbf{d}^{\mathrm{T}}\mathbf{E}_3\| \\ &\le 3\alpha q + \|\mathbf{d}\| \cdot \|\mathbf{E}_1\| + \|\mathbf{x}\| \cdot \|\mathbf{E}_2\| + \|\mathbf{d}\| \cdot \|\mathbf{E}_3\| \\ &\le 3\alpha q + 2\sigma_1\sqrt{m} \cdot \alpha q\sqrt{m} + \sigma_2\sqrt{m} \cdot \alpha q\sqrt{m} \\ &= ((2\sigma_1 + \sigma_2)m + 3)\,\alpha q,\end{aligned}$$

where $\|\mathbf{d}\| \le \sigma_1\sqrt{m}$, $\|\mathbf{x}\| \le \sigma_2\sqrt{m}$. Additionally, we write $B = ((2\sigma_1 + \sigma_2)m + 3)\,\alpha q$.

For $\mathbf{C}_{\mathrm{Add}} \leftarrow$ Add$(mpk, id, \mathbf{C}_1, \mathbf{C}_2)$ and $\mathbf{C}_{\mathrm{Mult}} \leftarrow$ Mult$(mpk, id, \mathbf{C}_1, \mathbf{C}_2)$, we have

$$\begin{aligned}\mathbf{z}^{\mathrm{T}}\mathbf{C}_{\mathrm{Add}} &= \mathbf{z}^{\mathrm{T}}(\mathbf{C}_1 + \mathbf{C}_2) \\ &= \mathbf{r}_1^{\mathrm{T}} + \mathbf{r}_2^{\mathrm{T}} + (\mu_1 + \mu_2) \cdot \mathbf{z}^{\mathrm{T}}\mathbf{G}, \\ \mathbf{z}^{\mathrm{T}}\mathbf{C}_{\mathrm{Mult}} &= \mathbf{z}^{\mathrm{T}}\mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &= \left(\mathbf{r}_1^{\mathrm{T}} + \mu_1 \cdot \mathbf{z}^{\mathrm{T}}\mathbf{G}\right) \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &= \mathbf{r}_1^{\mathrm{T}} \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + \mu_1 \cdot \mathbf{z}^{\mathrm{T}}\mathbf{C}_2 \\ &= \mathbf{r}_1^{\mathrm{T}} \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + \mu_1 \cdot \mathbf{r}_2^{\mathrm{T}} + \mu_1\mu_2 \cdot \mathbf{z}^{\mathrm{T}}\mathbf{G}.\end{aligned}$$

The error terms are bounded by $\|\mathbf{r}_{\mathrm{Add}}^{\mathrm{T}}\| \le \|\mathbf{r}_1^{\mathrm{T}}\| + \|\mathbf{r}_2^{\mathrm{T}}\|$ and $\|\mathbf{r}_{\mathrm{Mult}}^{\mathrm{T}}\| \le N \cdot \|\mathbf{r}_1^{\mathrm{T}}\| + \|\mathbf{r}_2^{\mathrm{T}}\|$, respectively. If $\mathbf{C}_1$ and $\mathbf{C}_2$ are fresh ciphertexts, then the error terms are bounded by $\|\mathbf{r}_{\mathrm{Add}}^{\mathrm{T}}\| \le 2B$ and $\|\mathbf{r}_{\mathrm{Mult}}^{\mathrm{T}}\| \le (N+1)B$, respectively.

By iteratively applying Add$(mpk, id, \mathbf{C}_1, \mathbf{C}_2)$ and Mult$(mpk, id, \mathbf{C}_1, \mathbf{C}_2)$, we can homomorphically compute $\mathbf{C}_f \leftarrow$ Eval$(mpk, id, f, \mathbf{C}_1, \ldots, \mathbf{C}_\ell)$, where f is a circuit of depth $\le L$. Since $\|\mathbf{r}_{\mathrm{Add}}^{\mathrm{T}}\| < \|\mathbf{r}_{\mathrm{Mult}}^{\mathrm{T}}\|$, the error term of the evaluated ciphertext $\mathbf{C}_f$ is bounded by $\|\mathbf{r}_f^{\mathrm{T}}\| \le (N+1)^L B$. Since $2^{\lceil \log q \rceil - 2} \in [q/4, q/2)$, Decrypt$(mpk, sk_{id}, \mathbf{C}_f)$ will output the value $f(\mu_1, \ldots, \mu_\ell)$ on the condition that $(N+1)^L B < q/8$.

To work correctly, the scheme requires that:

- $m \ge 6n \log q$;
- $\sigma_1 \ge \|\widetilde{\mathbf{T}_{\mathbf{A}}}\| \cdot \omega(\sqrt{\log m})$, where $\|\widetilde{\mathbf{T}_{\mathbf{A}}}\| \le O(\sqrt{n \log q})$;
- $\sigma_2 \ge \omega(\sqrt{\log m})$;
- $(N+1)^L B < q/8$, where $B = ((2\sigma_1 + \sigma_2)m + 3)\,\alpha q$;
- $\alpha \in (0, 1)$ and $\alpha \ge 2\sqrt{n}/q$.

To satisfy the above requirements, we set the parameters $(n, m, \alpha, q, \sigma_1, \sigma_2)$ as follows:

$$\begin{aligned} n &= n(\lambda, L), \\ m &= 6n^{1+\delta}, \\ \alpha &= \left(2^{O(L \log n)} \cdot O(m^{3/2}) \cdot \omega(\sqrt{\log n})\right)^{-1}, \\ q &= 2^{O(L \log n)} \cdot O(m^2) \cdot \omega(\sqrt{\log n}), \\ \sigma_1 &= \sqrt{m} \cdot \omega(\sqrt{\log n}), \\ \sigma_2 &= \omega(\sqrt{\log n}). \end{aligned}$$

Here, we assume that δ is such that $n^\delta > \lceil \log q \rceil = O(L \log n)$.

In addition, we observe that the evaluated ciphertext $\mathbf{C}_f \in \mathbb{Z}_q^{(2m+1)\times N}$. Therefore,

$$\begin{aligned} \left|\mathbf{C}_f\right| &\le (2m+1) \cdot N \cdot \lceil \log q \rceil \\ &= (2m+1) \cdot (2m+1) \cdot \lceil \log q \rceil \cdot \lceil \log q \rceil \\ &= (2m+1)^2 \cdot \lceil \log q \rceil^2, \end{aligned}$$

where $N = (2m+1) \cdot \lceil \log q \rceil$. As a result, the proposed scheme enjoys the compactness.

C. SECURITY PROOF

Theorem 1: Suppose the hash function H is a random oracle. Then, the CLFHE scheme in Section IV-A is INDr-ID-CPA secure against Type I attacks provided that the $\mathsf{DLWE}_{n,q,\chi}$ assumption holds. Specifically, suppose there exists an attacker $\mathcal{A}_I$ that wins the INDr-ID-CPA game defined in Section III-B with advantage $\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_I}^{\mathrm{INDr-ID-CPA}}(\lambda)$, making at most Q_{r} public key request queries and Q_{h} hash queries to H, then there exists an algorithm that solves the $\mathsf{DLWE}_{n,q,\chi}$ problem with advantage $\mathrm{Adv}_{\mathsf{DLWE}}(\lambda)$, such that

$$\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_I}^{\mathrm{INDr-ID-CPA}}(\lambda) \le 2\,(Q_{\mathrm{r}} + Q_{\mathrm{h}}) \cdot \mathrm{Adv}_{\mathsf{DLWE}}(\lambda) + \mathrm{negl}(\lambda).$$

Proof: We prove this theorem using a sequence of indistinguishable games. In Game i, we let Y_i denote the event that the attacker wins the game, i.e., the event $b = b'$.

Game 0. This game is the original INDr-ID-CPA game between an attacker $\mathcal{A}_I$ attacking the CLFHE scheme and a challenger. By definition,

$$\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_I}^{\mathrm{INDr-ID-CPA}}(\lambda) = \left|\Pr\left[Y_0\right] - \frac{1}{2}\right|.$$

Game 1. Compared with Game 0, Game 1 makes two changes:

1) The challenger generates a guess $h \leftarrow \{0, 1\}$ as to whether $\mathcal{A}_I$ will request the partial private key for the target identity or not. We know that if $\mathcal{A}_I$ requests the partial private key of the target identity, then it is not allowed to replace the public key of the target identity in Phase 1. Thus, if $h = 0$, then we assume that $\mathcal{A}_I$ will request the partial private key of the target identity. If $h = 1$, then we assume that $\mathcal{A}_I$ does not request the partial private key of the target identity, and therefore it has the option of replacing the public key of the target identity in Phase 1.
2) We also change the conditions in which $\mathcal{A}_I$ wins the game. Let Ext be the event that $\mathcal{A}_I$ queries the partial private key on the target identity. The new conditions are as follows:
   - If $h = 0$ and Ext occurs, then $\mathcal{A}_I$ wins the game if $b = b'$.
   - If $h = 0$ and Ext does not occur, then $\mathcal{A}_I$ wins the game with probability $1/2$. (i.e., the value b' is ignored and $\mathcal{A}_I$ is assumed to have output a random guess for b.)
   - If $h = 1$ and Ext occurs, then $\mathcal{A}_I$ wins the game with probability $1/2$. (as above)
   - If $h = 1$ and Ext does not occur, then $\mathcal{A}_I$ wins the game if $b = b'$.

It is easy to show that

$$\left|\Pr\left[Y_0\right] - \frac{1}{2}\right| = 2 \cdot \left|\Pr\left[Y_1\right] - \frac{1}{2}\right|.$$

We note that

$$\begin{aligned}\left|\Pr\left[Y_1\right] - \frac{1}{2}\right| &= \left|\frac{1}{2} \cdot \Pr\left[Y_1 | h = 0\right]\right. \\ &\quad \left. + \frac{1}{2} \cdot \Pr\left[Y_1 | h = 1\right] - \frac{1}{2}\right| \\ &\leq \frac{1}{2} \cdot \left|\Pr\left[Y_1 | h = 0\right] - \frac{1}{2}\right| \\ &\quad + \frac{1}{2} \cdot \left|\Pr\left[Y_1 | h = 1\right] - \frac{1}{2}\right|.\end{aligned}$$

Consequently, we continue the game hopping in two different chains depending on the value of the guess $h \in \{0, 1\}$. Since the guess h is either 0 or 1 at any time, only one of these two chains will happen after Game 1.

The games under the guess $h = 0$ are as follows.

Game 2. Compared with Game 1, Game 2 makes three changes:

1) In the setup phase, the challenger picks an index $i \leftarrow [Q_r]$.
2) On $\mathcal{A}_I$'s kth distinct query id_k for a public key, assume without loss of generality that $\mathcal{A}_I$ has not queried the partial private key on id_k. If $k = i$, the challenger chooses $\mathbf{v}_i \leftarrow \mathbb{Z}_q^n$ at random, extracts the partial private key $\mathbf{d}_i \leftarrow \mathsf{Extract}(mpk, msk, id_i)$ and lets $\mathbf{w}_i = \mathbf{W} \cdot \mathbf{d}_i \mod q$, and returns $pk_{id_i} = (\mathbf{v}_i, \mathbf{w}_i)$ to $\mathcal{A}_I$. Otherwise, the challenger extracts the partial private key $\mathbf{d}_k \leftarrow \mathsf{Extract}(mpk, msk, id_k)$, generates $\left(pk_{id_k}, sk_{id_k}\right) \leftarrow \mathsf{KeyGen}(mpk, id, \mathbf{d}_k)$, and returns the public key pk_{id_k} to $\mathcal{A}_I$.
3) When $\mathcal{A}_I$ produces a target identity id^* and a message μ, assume without loss of generality that $\mathcal{A}_I$ already queried the public key on id^*. If $id^* \neq id_i$, the challenger aborts and outputs the symbol $\perp$. Otherwise, the challenger sends the challenge ciphertext $\mathbf{C}_b^*$ to $\mathcal{A}_I$, where

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \mathbf{u}_i^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \mathbf{v}_i^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}_i^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G} \in \mathbb{Z}_q^{(2m+1)\times N}.$$

By Corollary 5.4 in [21], Game 2 is statistically indistinguishable from Game 1, provided that Game 2 has not aborted and output $\perp$. Thus,

$$\left|\Pr\left[Y_1 | h = 0\right] - \frac{1}{2}\right| = Q_r \cdot \left|\Pr\left[Y_2\right] - \frac{1}{2}\right|.$$

Game 3. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger chooses $\widehat{\mathbf{V}} \leftarrow \mathbb{Z}_q^{m\times N}$ and $\widehat{\mathbf{v}}_i \leftarrow \mathbb{Z}_q^N$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \widehat{\mathbf{V}} \\ \mathbf{u}_i^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \widehat{\mathbf{v}}_i^{\mathrm{T}} + \mathbf{w}_i^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

Suppose $\mathcal{A}_I$ has a non-negligible advantage in distinguishing Game 2 from Game 3. We use $\mathcal{A}_I$ to construct an algorithm $\mathcal{B}_1$ to solve a $\mathsf{DLWE}_{n,q,\chi}$ problem instance $\left((\mathbf{F}, \mathbf{f}), \begin{pmatrix} \mathbf{P} \\ \mathbf{p}^{\mathrm{T}} \end{pmatrix}\right) \in \mathbb{Z}_q^{n\times(m+1)} \times \mathbb{Z}_q^{(m+1)\times N}$. To solve this instance using $\mathcal{A}_I$, $\mathcal{B}_1$ simulates the challenger for $\mathcal{A}_I$ as follows:

- In the setup phase, $\mathcal{B}_1$ sets $\mathbf{V} = \mathbf{F}$.
- On $\mathcal{A}_I$'s kth distinct query id_k for a public key, $\mathcal{B}_1$ does the following: if $k = i$, it lets $\mathbf{v}_i = \mathbf{f}$, extracts the partial private key $\mathbf{d}_i \leftarrow \mathsf{Extract}(mpk, msk, id_i)$ and lets $\mathbf{w}_i = \mathbf{W} \cdot \mathbf{d}_i \mod q$, and returns $pk_{id_i} = (\mathbf{f}, \mathbf{w}_i)$ to $\mathcal{A}_I$. Otherwise, the challenger extracts the partial private key $\mathbf{d}_k \leftarrow \mathsf{Extract}(mpk, msk, id_k)$, generates $\left(pk_{id_k}, sk_{id_k}\right) \leftarrow \mathsf{KeyGen}(mpk, id, \mathbf{d}_k)$, and returns the public key pk_{id_k} to $\mathcal{A}_I$.
- When $\mathcal{A}_I$ produces a target identity id^* and a message μ, $\mathcal{B}_1$ does the following: if $id^* \neq id_i$, it aborts and outputs the symbol $\perp$. Otherwise, it sends the challenge ciphertext $\mathbf{C}_b^*$ to $\mathcal{A}_I$, where

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{P} \\ \mathbf{u}_i^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \mathbf{p}^{\mathrm{T}} + \mathbf{w}_i^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

- $\mathcal{B}_1$ is otherwise the same as the Game 2 challenger.
- Finally, $\mathcal{A}_I$ guesses whether the challenger that it is interacting with is the Game 2 challenger or the Game 3 challenger. $\mathcal{B}_1$ outputs $\mathcal{A}_I$'s guess as the answer to the given DLWE instance.

It can be seen that $\mathcal{B}_1$'s advantage in solving the given DLWE instance is the same as $\mathcal{A}_I$'s advantage in distinguishing Game 2 from Game 3. Therefore,

$$\left|\Pr\left[Y_2\right] - \Pr\left[Y_3\right]\right| \leq \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_1}(\lambda).$$

Game 4. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects $\overset{\triangle}{\mathbf{V}}_i \leftarrow \mathbb{Z}_q^N$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_i^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

In Game 3, $\widehat{\mathbf{v}}_i^{\mathrm{T}}$ is uniformly random in $\mathbb{Z}_q^{1\times N}$; hence, $\mathbf{u}_i^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \widehat{\mathbf{v}}_i^{\mathrm{T}} + \mathbf{w}_i^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}}$ is also uniformly random in $\mathbb{Z}_q^{1\times N}$. Therefore,

$$\left|\Pr\left[Y_3\right] - \Pr\left[Y_4\right]\right| = \mathrm{negl}(\lambda).$$

Game 5. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger chooses $\widehat{\mathbf{W}} \leftarrow \mathbb{Z}_q^{m\times N}$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \widehat{\mathbf{W}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_i^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

Suppose $\mathcal{A}_I$ has a non-negligible advantage in distinguishing Game 4 from Game 5. We use $\mathcal{A}_I$ to construct an algorithm $\mathcal{B}_2$ to solve a $\mathsf{DLWE}_{n,q,\chi}$ problem instance $(\mathbf{F}, \mathbf{P}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times N}$. To solve this instance using $\mathcal{A}_I$, $\mathcal{B}_2$ simulates the challenger for $\mathcal{A}_I$ as follows:

- In the setup phase, $\mathcal{B}_2$ sets $\mathbf{W} = \mathbf{F}$.
- When $\mathcal{A}_I$ produces a target identity id^* and a message μ, $\mathcal{B}_2$ does the following: if $id^* \neq id_i$, it aborts and outputs the symbol $\perp$. Otherwise, it sends the challenge ciphertext $\mathbf{C}_b^*$ to $\mathcal{A}_I$, where
$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \mathbf{P} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_i^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$
- $\mathcal{B}_2$ is otherwise the same as the Game 4 challenger.
- Finally, $\mathcal{A}_I$ guesses whether the challenger that it is interacting with is the Game 4 challenger or the Game 5 challenger. $\mathcal{B}_2$ outputs $\mathcal{A}_I$'s guess as the answer to the given DLWE instance.

It can be seen that $\mathcal{B}_2$'s advantage in solving the given DLWE instance is the same as $\mathcal{A}_I$'s advantage in distinguishing Game 4 from Game 5. Therefore,

$$\left|\Pr\left[Y_4\right] - \Pr\left[Y_5\right]\right| \leq \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_2}(\lambda).$$

Game 6. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects $\overset{\triangle}{\mathbf{W}} \leftarrow \mathbb{Z}_q^{m\times N}$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \overset{\triangle}{\mathbf{W}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_i^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

In Game 5, $\widehat{\mathbf{W}}$ is uniformly random in $\mathbb{Z}_q^{m\times N}$; hence, $\mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \widehat{\mathbf{W}}$ is also uniformly random in $\mathbb{Z}_q^{m\times N}$. Therefore,

$$\left|\Pr\left[Y_5\right] - \Pr\left[Y_6\right]\right| = \mathrm{negl}(\lambda).$$

Game 7. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger chooses the challenge ciphertext $\mathbf{C}_0^* \leftarrow \mathbb{Z}_q^{(2m+1)\times N}$ at random. In Game 6, $\begin{pmatrix} \overset{\triangle}{\mathbf{W}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_i^{\mathrm{T}} \end{pmatrix}$ is a random element in $\mathbb{Z}_q^{(2m+1)\times N}$; hence, $\begin{pmatrix} \overset{\triangle}{\mathbf{W}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_i^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}$ is also a random element in $\mathbb{Z}_q^{(2m+1)\times N}$. Thus,

$$\left|\Pr\left[Y_6\right] - \Pr\left[Y_7\right]\right| = \mathrm{negl}(\lambda).$$

In addition, in Game 7, the challenge ciphertext $\mathbf{C}_0^*$ is chosen at random from $\mathbb{Z}_q^{(2m+1)\times N}$. Therefore,

$$\left|\Pr\left[Y_7\right] - \frac{1}{2}\right| = 0.$$

The games under the guess $h = 1$ are as follows.

Game 2′. Compared with Game 1, Game 2′ makes six changes:

1) In the setup phase, the challenger picks an index $j \leftarrow [Q_{\mathrm{h}}]$.
2) In the setup phase, the challenger generates $\mathbf{A}$ as a random matrix in $\mathbb{Z}_q^{n\times m}$.
3) On $\mathcal{A}_I$'s kth distinct hash query id_k to H, the challenger does the following: If $k = j$, it chooses $\mathbf{u}_j, \mathbf{w}_j \leftarrow \mathbb{Z}_q^n$ at random, locally stores the tuple $\left(id_j, \mathbf{u}_j, \mathbf{w}_j, \perp\right)$, and returns $\mathbf{u}_j$ to $\mathcal{A}_I$. Otherwise, it samples $\mathbf{d}_k \leftarrow D_{\mathbb{Z}^m,\sigma_1}$, lets $\mathbf{u}_k = \mathbf{A} \cdot \mathbf{d}_k \mod q$ and $\mathbf{w}_k = \mathbf{W} \cdot \mathbf{d}_k \mod q$, locally stores the tuple $(id_k, \mathbf{u}_k, \mathbf{w}_k, \mathbf{d}_k)$, and returns $\mathbf{u}_k$ to $\mathcal{A}_I$.
4) When $\mathcal{A}_I$ asks for a partial private key for the identity id, assume without loss of generality that $\mathcal{A}_I$ already made the hash query on id. If $id = id_j$, then the challenger aborts and outputs a random bit, i.e., $\mathcal{A}_I$ wins the game with a probability of $1/2$. Otherwise, the challenger retrieves the tuple $(id, \mathbf{u}, \mathbf{w}, \mathbf{d})$ from local storage and returns $\mathbf{d}$ to $\mathcal{A}_I$.
5) When $\mathcal{A}_I$ requests for a public key for the identity id, assume without loss of generality that $\mathcal{A}_I$ already made the hash query on id. If $id = id_j$, then the challenger samples a vector $\mathbf{x}_j \leftarrow D_{\mathbb{Z}^m,\sigma_2}$ and lets $\mathbf{v}_j = \mathbf{V} \cdot \mathbf{x}_j \mod q$, retrieves the tuple $\left(id_j, \mathbf{u}_j, \mathbf{w}_j, \perp\right)$ from local storage, and returns $pk_{id_j} = \left(\mathbf{v}_j, \mathbf{w}_j\right)$ to $\mathcal{A}_I$. Otherwise, the challenger samples a vector $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,\sigma_2}$ and lets

$\mathbf{v} = \mathbf{V} \cdot \mathbf{x} \mod q$, retrieves the tuple $(id, \mathbf{u}, \mathbf{w}, \mathbf{d})$ from local storage, and returns $pk_{id} = (\mathbf{v}, \mathbf{w})$ to $\mathcal{A}_I$.

6) When $\mathcal{A}_I$ produces a target identity id^* and a message μ, assume without loss of generality that $\mathcal{A}_I$ already queried the public key on id^*. If $id^* \neq id_j$, the challenger aborts and outputs the symbol $\perp$. Otherwise, the challenger sends the challenge ciphertext $\mathbf{C}_b^*$ to $\mathcal{A}_I$, where

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_1 + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \mathbf{u}_j^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \mathbf{v}_j^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}_j^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G} \in \mathbb{Z}_q^{(2m+1)\times N}.$$

By Proposition 3, Game $2'$ is statistically indistinguishable from Game 1, provided that Game $2'$ has not aborted and output $\perp$. Hence,

$$\left|\Pr\left[Y_1 | h = 1\right] - \frac{1}{2}\right| = Q_{\mathrm{h}} \cdot \left|\Pr\left[Y_2'\right] - \frac{1}{2}\right|.$$

Game $3'$. In this game, we change the way in which the challenge ciphertext $\mathbf{C}_0^*$ is created. The challenger chooses $\widehat{\mathbf{A}} \leftarrow \mathbb{Z}_q^{m\times N}$ and $\widehat{\mathbf{u}}_j \leftarrow \mathbb{Z}_q^N$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \widehat{\mathbf{A}} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \widehat{\mathbf{u}}_j^{\mathrm{T}} + \mathbf{v}_j^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}_j^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

Suppose $\mathcal{A}_I$ has a non-negligible advantage in distinguishing Game $2'$ from Game $3'$. We use $\mathcal{A}_I$ to construct an algorithm $\mathcal{B}_3$ to solve a $\mathsf{DLWE}_{n,q,\chi}$ problem instance $\left((\mathbf{F}, \mathbf{f}), \begin{pmatrix} \mathbf{P} \\ \mathbf{p}^{\mathrm{T}} \end{pmatrix}\right) \in \mathbb{Z}_q^{n\times(m+1)} \times \mathbb{Z}_q^{(m+1)\times N}$. $\mathcal{B}_3$ simulates the challenger for $\mathcal{A}_I$ as follows:

- In the setup phase, $\mathcal{B}_3$ sets $\mathbf{A} = \mathbf{F}$.
- On $\mathcal{A}_I$'s kth distinct hash query id_k to H, $\mathcal{B}_3$ does the following: If $k = j$, it lets $\mathbf{u}_j = \mathbf{f}$, chooses $\mathbf{w}_j \leftarrow \mathbb{Z}_q^n$ at random, locally stores the tuple $\left(id_j, \mathbf{f}, \mathbf{w}_j, \perp\right)$, and returns $\mathbf{f}$ to $\mathcal{A}_I$. Otherwise, it samples $\mathbf{d}_k \leftarrow D_{\mathbb{Z}^m,\sigma_1}$, lets $\mathbf{u}_k = \mathbf{A} \cdot \mathbf{d}_k \mod q$ and $\mathbf{w}_k = \mathbf{W} \cdot \mathbf{d}_k \mod q$, locally stores the tuple $(id_k, \mathbf{u}_k, \mathbf{w}_k, \mathbf{d}_k)$, and returns $\mathbf{u}_k$ to $\mathcal{A}_I$.
- When $\mathcal{A}_I$ produces a target identity id^* and a message μ, $\mathcal{B}_3$ does the following: If $id^* \neq id_j$, it aborts and outputs the symbol $\perp$. Otherwise, it sends the challenge ciphertext $\mathbf{C}_b^*$ to $\mathcal{A}_I$, where

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{P} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \mathbf{p}^{\mathrm{T}} + \mathbf{v}_j^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}_j^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

- $\mathcal{B}_3$ is otherwise the same as the Game $2'$ challenger.
- Finally, $\mathcal{A}_I$ guesses whether the challenger it is interacting with is the Game $2'$ challenger or the Game $3'$ challenger. $\mathcal{B}_3$ outputs $\mathcal{A}_I$'s guess as the answer to the given DLWE instance.

It can be seen that the advantage of $\mathcal{B}_3$ in solving the given DLWE instance is the same as that of $\mathcal{A}_I$ in distinguishing Game $2'$ from Game $3'$. Therefore,

$$\left|\Pr\left[Y_2'\right] - \Pr\left[Y_3'\right]\right| \leq \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_3}(\lambda).$$

Game $4'$. In this game, we change the way in which the challenge ciphertext $\mathbf{C}_0^*$ is created. The challenger chooses $\overset{\triangle}{\mathbf{A}} \leftarrow \mathbb{Z}_q^{m\times N}$ and $\overset{\triangle}{\mathbf{u}}_j \leftarrow \mathbb{Z}_q^N$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \overset{\triangle}{\mathbf{A}} \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \overset{\triangle}{\mathbf{u}}{}_j^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

In Game $3'$, $\widehat{\mathbf{A}}$ and $\widehat{\mathbf{u}}_j^{\mathrm{T}}$ are uniformly random in $\mathbb{Z}_q^{m\times N}$ and $\mathbb{Z}_q^{1\times N}$, respectively. Therefore, $\widehat{\mathbf{A}} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3$ and $\widehat{\mathbf{u}}_j^{\mathrm{T}} + \mathbf{v}_j^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}_j^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}}$ are also uniformly random in $\mathbb{Z}_q^{m\times N}$ and $\mathbb{Z}_q^{1\times N}$, respectively. Thus,

$$\left|\Pr\left[Y_3'\right] - \Pr\left[Y_4'\right]\right| = \mathrm{negl}(\lambda).$$

Game $5'$. In this game, we change the way in which the challenge ciphertext $\mathbf{C}_0^*$ is created. The challenger chooses $\widehat{\mathbf{V}} \leftarrow \mathbb{Z}_q^{m\times N}$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \overset{\triangle}{\mathbf{A}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{u}}{}_j^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

Suppose $\mathcal{A}_I$ has a non-negligible advantage in distinguishing Game $4'$ from Game $5'$. We use $\mathcal{A}_I$ to construct an algorithm $\mathcal{B}_4$ to solve a $\mathsf{DLWE}_{n,q,\chi}$ problem instance $(\mathbf{F}, \mathbf{P}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times N}$. $\mathcal{B}_4$ simulates the challenger for $\mathcal{A}_I$ as follows:

- In the setup phase, $\mathcal{B}_4$ sets $\mathbf{V} = \mathbf{F}$.
- When $\mathcal{A}_I$ produces a target identity id^* and a message μ, $\mathcal{B}_4$ does the following: If $id^* \neq id_j$, it aborts and outputs the symbol $\perp$. Otherwise, it sends the challenge ciphertext $\mathbf{C}_b^*$ to $\mathcal{A}_I$, where

$$\mathbf{C}_0^* = \begin{pmatrix} \overset{\triangle}{\mathbf{A}} \\ \mathbf{P} \\ \overset{\triangle}{\mathbf{u}}{}_j^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G} \in \mathbb{Z}_q^{(2m+1)\times N}.$$

- $\mathcal{B}_4$ is otherwise the same as the Game $4'$ challenger.
- Finally, $\mathcal{A}_I$ guesses whether the challenger it is interacting with is the Game $4'$ challenger or the Game $5'$ challenger. $\mathcal{B}_4$ outputs $\mathcal{A}_I$'s guess as the answer to the given DLWE instance.

It can be seen that the advantage of $\mathcal{B}_4$ in solving the given DLWE instance is the same as that of $\mathcal{A}_I$ in distinguishing Game $4'$ from Game $5'$. Therefore,

$$\left|\Pr\left[Y_4'\right] - \Pr\left[Y_5'\right]\right| \leq \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_4}(\lambda).$$

Game $6'$. In this game, we change the way in which the challenge ciphertext $\mathbf{C}_0^*$ is created. The challenger chooses the challenge ciphertext $\mathbf{C}_0^* \leftarrow \mathbb{Z}_q^{(2m+1)\times N}$ at random.

In Game 5′, $\begin{pmatrix} \overset{\triangle}{\mathbf{A}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{u}}_j^{\mathrm{T}} \end{pmatrix}$ is a random element in $\mathbb{Z}_q^{(2m+1)\times N}$; thus $\begin{pmatrix} \overset{\triangle}{\mathbf{A}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{u}}_j^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}$ is also a random element in $\mathbb{Z}_q^{(2m+1)\times N}$. Therefore,

$$\left|\Pr\left[Y_5'\right] - \Pr\left[Y_6'\right]\right| = \mathrm{negl}(\lambda).$$

In Game 6′, the challenge ciphertext $\mathbf{C}_0^*$ is chosen at random from $\mathbb{Z}_q^{(2m+1)\times N}$. Thus,

$$\left|\Pr\left[Y_6'\right] - \frac{1}{2}\right| = 0.$$

In summary, we obtain that

$$\begin{aligned}
\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_I}^{\mathrm{INDr-ID-CPA}}(\lambda) &= \left|\Pr\left[Y_0\right] - \frac{1}{2}\right| \\
&= 2 \cdot \left|\Pr\left[Y_1\right] - \frac{1}{2}\right| \\
&\leq \left|\Pr\left[Y_1 | h = 0\right] - \frac{1}{2}\right| + \left|\Pr\left[Y_1 | h = 1\right] - \frac{1}{2}\right| \\
&= Q_{\mathrm{r}} \cdot \left|\Pr\left[Y_2\right] - \frac{1}{2}\right| + Q_{\mathrm{h}} \cdot \left|\Pr\left[Y_2'\right] - \frac{1}{2}\right| \\
&\leq Q_{\mathrm{r}} \cdot \left(\mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_1}(\lambda) + \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_2}(\lambda)\right) \\
&\quad + Q_{\mathrm{h}} \cdot \left(\mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_3}(\lambda) + \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_4}(\lambda)\right) + \mathrm{negl}(\lambda) \\
&\leq 2\left(Q_{\mathrm{r}} + Q_{\mathrm{h}}\right) \cdot \mathrm{Adv}_{\mathsf{DLWE}}(\lambda) + \mathrm{negl}(\lambda),
\end{aligned}$$

where $\mathrm{Adv}_{\mathsf{DLWE}}(\lambda) = \max\left\{\mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_i}(\lambda)\right\}_{i\in[4]}$.

□

Theorem 2: Suppose the hash function H is a random oracle. Then, the CLFHE scheme in Section IV-A is INDr-ID-CPA secure against Type II attacks assuming that the $\mathsf{DLWE}_{n,q,\chi}$ assumption holds. In particular, suppose there exists an attacker $\mathcal{A}_{II}$ that wins the INDr-ID-CPA game defined in Section III-B with advantage $\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_{II}}^{\mathrm{INDr-ID-CPA}}(\lambda)$, making at most Q_{r} public key request queries, then there exists an algorithm that solves the $\mathsf{DLWE}_{n,q,\chi}$ problem with advantage $\mathrm{Adv}_{\mathsf{DLWE}}(\lambda)$, such that

$$\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_{II}}^{\mathrm{INDr-ID-CPA}}(\lambda)) \leq 2Q_{\mathrm{r}} \cdot \mathrm{Adv}_{\mathsf{DLWE}}(\lambda) + \mathrm{negl}(\lambda).$$

The proof of Theorem 2 is similar to that of Theorem 1 under the guess $h = 0$. As a result, we omit a detailed proof of Theorem 2 here.

V. A LEVELED CLFHE SCHEME IN THE STANDARD MODEL

A. CONSTRUCTION

The proposed leveled CLFHE scheme in the standard model is described as follows.

Setup$(1^\lambda, 1^L)$: On input a security parameter λ and a circuit depth L, do:

1) Set the parameters $n = n(\lambda, L)$, $m = m(\lambda, L)$, $\alpha = \alpha(\lambda, L)$, $q = q(\lambda, L)$, $\sigma_1 = \sigma_1(\lambda, L)$, and $\sigma_2 = \sigma_2(\lambda, L)$ as specified in Section V-B below.
2) Define the gadget matrix $\mathbf{G} = \mathbf{I}_{3m+1} \otimes \mathbf{g}^{\mathrm{T}} \in \mathbb{Z}_q^{(3m+1)\times N}$, where $\mathbf{g} = \left(1, \ldots, 2^{\lceil \log q \rceil - 1}\right)^{\mathrm{T}} \in \mathbb{Z}_q^{\lceil \log q \rceil}$, $N = (3m+1) \cdot \lceil \log q \rceil$. Define the inverse function $\mathbf{G}^{-1} : \mathbb{Z}_q^{(3m+1)\times N} \to \{0, 1\}^{N\times N}$ that expands each entry $a \in \mathbb{Z}_q$ of the input matrix into a vector $\left(a_0, \ldots, a_{\lceil \log q \rceil - 1}\right)^{\mathrm{T}}$, where a_i is the ith bit in a's binary representation. For any matrix $\mathbf{X} \in \mathbb{Z}_q^{(3m+1)\times N}$, it is clear that $\mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{X}) = \mathbf{X}$. The definitions of $\mathbf{G}$ and $\mathbf{G}^{-1}$ can also be found in [31], [32].
3) Invoke the algorithm $\mathsf{GenBasis}\,(1^n, 1^m, q)$ to generate a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a basis $\mathbf{T_A}$ for $\Lambda^\perp(\mathbf{A})$ such that $\|\widetilde{\mathbf{T_A}}\| \leq O(\sqrt{n \log q})$.
4) Select three matrices $\mathbf{A}_1, \mathbf{B}, \mathbf{V} \leftarrow \mathbb{Z}_q^{n\times m}$ at random, select a matrix $\mathbf{W} \leftarrow \mathbb{Z}_q^{n\times 2m}$ at random, and select a vector $\mathbf{u} \leftarrow \mathbb{Z}_q^n$ at random.
5) Choose a function $H : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$ which is an encoding with full-rank differences as defined in [22].
6) Output a master public key and a master private key: $mpk = \left(\mathbf{A}, \mathbf{A}_1, \mathbf{B}, \mathbf{V}, \mathbf{W}, \mathbf{u}, H\right)$ and $msk = \mathbf{T_A}$.

Extract(mpk, msk, id): On input a master private key msk and an identity $id \in \mathbb{Z}_q^n$, do:

1) Invoke the algorithm $\mathsf{SampleLeft}(\mathbf{A}, \mathbf{A}_1 + H(id) \cdot \mathbf{B}, \mathbf{T_A}, \mathbf{u}, \sigma_1)$ to sample a vector $\mathbf{d} \in \mathbb{Z}^{2m}$. Let $\mathbf{A}_{id} = (\mathbf{A}|\mathbf{A}_1 + H(id) \cdot \mathbf{B}) \in \mathbb{Z}_q^{n\times 2m}$, then $\mathbf{A}_{id} \cdot \mathbf{d} = \mathbf{u} \mod q$ and $\mathbf{d}$ is distributed as $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}_{id}),\sigma_1}$ by Proposition 4.
2) Output a partial private key $psk_{id} = \mathbf{d}$.

KeyGen(mpk, id, psk_{id}): On input an identity $id \in \mathbb{Z}_q^n$ and a partial private key $psk_{id} = \mathbf{d}$, do:

1) Sample a vector $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,\sigma_2}$.
2) Let $\mathbf{v} = \mathbf{V} \cdot \mathbf{x} \mod q$.
3) Let $\mathbf{w} = \mathbf{W} \cdot \mathbf{d} \mod q$.
4) Let $\mathbf{z} = \begin{pmatrix} -\mathbf{d} \\ -\mathbf{x} \\ 1 \end{pmatrix} \in \mathbb{Z}^{3m+1}$.
5) Output a public key $pk_{id} = (\mathbf{v}, \mathbf{w})$ and a private key $sk_{id} = \mathbf{z}$.

Encrypt(mpk, id, pk_{id}, μ): On input an identity $id \in \mathbb{Z}_q^n$, a public key pk_{id}, and a message $\mu \in \{0, 1\}$, do:

1) Set $\mathbf{A}_{id} = (\mathbf{A}|\mathbf{A}_1 + H(id) \cdot \mathbf{B}) \in \mathbb{Z}_q^{n\times 2m}$.
2) Pick three matrices $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3 \leftarrow \mathbb{Z}_q^{n\times N}$ at random.
3) Sample a matrix $\mathbf{R} \leftarrow D_{\mathbb{Z},\omega(\sqrt{\log m})}^{m\times m}$.
4) Sample a noise matrix $\mathbf{E}_1 \leftarrow D_{\mathbb{Z},\alpha q}^{m\times N}$ and set $\mathbf{E}_{id} = \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{R}^{\mathrm{T}} \cdot \mathbf{E}_1 \end{pmatrix} \in \mathbb{Z}^{2m\times N}$, sample two noise matrices $\mathbf{E}_2 \leftarrow D_{\mathbb{Z},\alpha q}^{m\times N}$ and $\mathbf{E}_3 \leftarrow D_{\mathbb{Z},\alpha q}^{2m\times N}$, and sample three noise vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \leftarrow D_{\mathbb{Z},\alpha q}^N$.
5) Output a ciphertext $\mathbf{C}$ given by

$$\mathbf{C} = \begin{pmatrix} \mathbf{A}_{id}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_{id} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \mathbf{u}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \mathbf{v}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G} \in \mathbb{Z}_q^{(3m+1)\times N}.$$

Decrypt$(mpk, sk_{id}, \mathbf{C})$: On input a private key $sk_{id} = \mathbf{z}$ and a ciphertext $\mathbf{C}$, do:

1) Let $\mathbf{c}$ be the penultimate column of $\mathbf{C}$.

2) Output a message

$$\mu = \left\lfloor \frac{\mathbf{z}^{\mathrm{T}} \cdot \mathbf{c}}{2^{\lceil \log q \rceil - 2}} \right\rceil.$$

Add$(mpk, id, \mathbf{C}_1, \mathbf{C}_2)$: On input two ciphertexts $\mathbf{C}_1$, $\mathbf{C}_2$ under the same identity id, output $\mathbf{C}_{\mathrm{Add}} = \mathbf{C}_1 + \mathbf{C}_2 \in \mathbb{Z}_q^{(3m+1)\times N}$.

Mult$(mpk, id, \mathbf{C}_1, \mathbf{C}_2)$: On input two ciphertexts $\mathbf{C}_1$, $\mathbf{C}_2$ under the same identity id, output $\mathbf{C}_{\mathrm{Mult}} = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \in \mathbb{Z}_q^{(3m+1)\times N}$.

B. CORRECTNESS AND PARAMETER SELECTION

For a ciphertext $\mathbf{C} \leftarrow$ Encrypt(mpk, id, pk_{id}, μ), we have

$$\begin{aligned}
\mathbf{z}^{\mathrm{T}}\mathbf{C} &= \mathbf{z}^{\mathrm{T}} \begin{pmatrix} \mathbf{A}_{id}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_{id} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \mathbf{u}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \mathbf{v}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} \\
&\quad + \mu \cdot \mathbf{z}^{\mathrm{T}}\mathbf{G} \\
&= \underbrace{\mathbf{e}_1^{\mathrm{T}} + \mathbf{e}_2^{\mathrm{T}} + \mathbf{e}_3^{\mathrm{T}} - \mathbf{d}^{\mathrm{T}}\mathbf{E}_{id} - \mathbf{x}^{\mathrm{T}}\mathbf{E}_2 - \mathbf{d}^{\mathrm{T}}\mathbf{E}_3}_{\text{error term}} \\
&\quad + \mu \cdot \mathbf{z}^{\mathrm{T}}\mathbf{G},
\end{aligned}$$

We write $\mathbf{r}^{\mathrm{T}} = \mathbf{e}_1^{\mathrm{T}} + \mathbf{e}_2^{\mathrm{T}} + \mathbf{e}_3^{\mathrm{T}} - \mathbf{d}^{\mathrm{T}}\mathbf{E}_{id} - \mathbf{x}^{\mathrm{T}}\mathbf{E}_2 - \mathbf{d}^{\mathrm{T}}\mathbf{E}_3$. The error term is bounded by

$$\begin{aligned}
\|\mathbf{r}^{\mathrm{T}}\| &= \|\mathbf{e}_1^{\mathrm{T}} + \mathbf{e}_2^{\mathrm{T}} + \mathbf{e}_3^{\mathrm{T}} - \mathbf{d}^{\mathrm{T}}\mathbf{E}_{id} - \mathbf{x}^{\mathrm{T}}\mathbf{E}_2 - \mathbf{d}^{\mathrm{T}}\mathbf{E}_3\| \\
&\le \|\mathbf{e}_1^{\mathrm{T}} + \mathbf{e}_2^{\mathrm{T}} + \mathbf{e}_3^{\mathrm{T}}\| + \|\mathbf{d}^{\mathrm{T}}\mathbf{E}_{id} + \mathbf{x}^{\mathrm{T}}\mathbf{E}_2 + \mathbf{d}^{\mathrm{T}}\mathbf{E}_3\| \\
&\le 3\alpha q + \|\mathbf{d}^{\mathrm{T}}\mathbf{E}_{id}\| + \|\mathbf{x}^{\mathrm{T}}\mathbf{E}_2\| + \|\mathbf{d}^{\mathrm{T}}\mathbf{E}_3\| \\
&\le 3\alpha q + \|\mathbf{d}\| \cdot \|\mathbf{E}_{id}\| + \|\mathbf{x}\| \cdot \|\mathbf{E}_2\| + \|\mathbf{d}\| \cdot \|\mathbf{E}_3\| \\
&\le 3\alpha q + \|\mathbf{d}\| \cdot \left(\|\mathbf{E}_1\| + \sqrt{m} \cdot \|\mathbf{R}\| \cdot \|\mathbf{E}_1\|\right) \\
&\quad + \sigma_2\sqrt{m} \cdot \alpha q\sqrt{m} + \sigma_1\sqrt{2m} \cdot \alpha q \sqrt{2m} \\
&\le 3\alpha q + \sigma_1\sqrt{2m}\left(\alpha q\sqrt{m} + \sqrt{m} \cdot \omega(\sqrt{\log m})\sqrt{m}\alpha q\sqrt{m}\right) \\
&\quad + \sigma_2\, m\alpha q + 2\sigma_1\, m\alpha q \\
&= \left(\sqrt{2}\sigma_1\, m^2\omega(\sqrt{\log m}) + (2+\sqrt{2})\sigma_1\, m + \sigma_2\, m + 3\right)\alpha q,
\end{aligned}$$

where $\|\mathbf{d}\| \le \sigma_1\sqrt{2m}$, $\|\mathbf{x}\| \le \sigma_2\sqrt{m}$. In addition, we write $B = \left(\sqrt{2}\sigma_1\, m^2\omega(\sqrt{\log m}) + (2+\sqrt{2})\sigma_1\, m + \sigma_2\, m + 3\right)\alpha q$.

For two fresh ciphertexts $\mathbf{C}_1$ and $\mathbf{C}_2$ under the same identity id, the error term of $\mathbf{C}_{\mathrm{Add}}$ and $\mathbf{C}_{\mathrm{Mult}}$ is bounded by $\|\mathbf{r}_{\mathrm{Add}}^{\mathrm{T}}\| \le 2B$ and $\|\mathbf{r}_{\mathrm{Mult}}^{\mathrm{T}}\| \le (N+1)B$, respectively. Hence, for an evaluated ciphertext $\mathbf{C}_f \leftarrow$ Eval $(mpk, id, f, \mathbf{C}_1, \ldots, \mathbf{C}_\ell)$, the error term of $\mathbf{C}_f$ is bounded by $\|\mathbf{r}_f^{\mathrm{T}}\| \le (N+1)^L B$, where f is a circuit of depth $\le L$. Since $2^{\lceil \log q \rceil - 2} \in [q/4, q/2)$, Decrypt$(mpk, sk_{id}, \mathbf{C}_f)$ will output the value $f(\mu_1, \ldots, \mu_\ell)$ on the condition that $(N+1)^L B < q/8$.

To work correctly, the scheme requires that:

- $m \ge 6n \log q$;
- $\sigma_1 \ge \|\widetilde{\mathbf{T}_\mathbf{A}}\| \cdot \omega(\sqrt{\log m})$ and $\sigma_1 \ge \|\widetilde{\mathbf{T}_\mathbf{B}}\| \cdot m \cdot \omega(\sqrt{\log m})^2$, where $\|\mathbf{T}_\mathbf{A}\|, \|\mathbf{T}_\mathbf{B}\| \le O(\sqrt{n \log q})$;
- $\sigma_2 \ge \omega(\sqrt{\log m})$;
- $(N+1)^L B < q/8$, where $B = \left(\sqrt{2}\sigma_1\, m^2\omega(\sqrt{\log m}) + (2+\sqrt{2})\sigma_1\, m + \sigma_2\, m + 3\right)\alpha q$;
- $\alpha \in (0,1)$ and $\alpha \ge 2\sqrt{n}/q$.

To satisfy the requirements, we set the parameters $(n, m, \alpha, q, \sigma_1, \sigma_2)$ as follows:

$$\begin{aligned}
n &= n(\lambda, L), \\
m &= 6n^{1+\delta}, \\
\alpha &= \left(2^{O(L \log n)} \cdot O(m^{7/2}) \cdot \omega(\sqrt{\log n})^3\right)^{-1}, \\
q &= 2^{O(L \log n)} \cdot O(m^4) \cdot \omega(\sqrt{\log n})^3, \\
\sigma_1 &= m^{3/2} \cdot \omega(\sqrt{\log n})^2, \\
\sigma_2 &= \omega(\sqrt{\log n}).
\end{aligned}$$

Here we assume that δ is such that $n^\delta > \lceil \log q \rceil = O(L \log n)$.

In addition, we observe that the evaluated ciphertext $\mathbf{C}_f \in \mathbb{Z}_q^{(3m+1)\times N}$. Hence,

$$\begin{aligned}
\left|\mathbf{C}_f\right| &\le (3m+1) \cdot N \cdot \lceil \log q \rceil \\
&= (3m+1) \cdot (3m+1) \cdot \lceil \log q \rceil \cdot \lceil \log q \rceil \\
&= (3m+1)^2 \cdot \lceil \log q \rceil^2,
\end{aligned}$$

where $N = (3m+1) \cdot \lceil \log q \rceil$. Consequently, the proposed scheme satisfies the compactness requirement.

C. SECURITY PROOF

Theorem 3: The CLFHE scheme in Section V-A is INDr-sID-CPA secure against Type I attacks if the DLWE$_{n,q,\chi}$ assumption holds. Specifically, suppose there exists an attacker $\mathcal{A}_I$ that wins the INDr-sID-CPA game defined in Section III-C with an advantage $\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_I}^{\mathrm{INDr-sID-CPA}}(\lambda)$, then there exists an algorithm that solves the DLWE$_{n,q,\chi}$ problem with an advantage $\mathrm{Adv}_{\mathsf{DLWE}}(\lambda)$ such that

$$\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_I}^{\mathrm{INDr-sID-CPA}}(\lambda) \le 4 \cdot \mathrm{Adv}_{\mathsf{DLWE}}(\lambda) + \mathrm{negl}(\lambda).$$

Proof: We prove this theorem via a series of indistinguishable games. In Game i, we let Y_i denote the event that the attacker wins the game, i.e., the event $b = b'$.

Game 0. This game is the original INDr-sID-CPA game between an attacker $\mathcal{A}_I$ in attacking our CLFHE scheme and a challenger. By definition,

$$\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_I}^{\mathrm{INDr-sID-CPA}}(\lambda) = \left|\Pr[Y_0] - \frac{1}{2}\right|.$$

Game 1. Similar to the proof of Theorem 1, In Game 1 we also introduce a guess $h \leftarrow \{0,1\}$ and change the conditions in which $\mathcal{A}_I$ wins the game. Thus, we obtain

$$\begin{aligned}
\left|\Pr[Y_0] - \frac{1}{2}\right| &= 2 \cdot \left|\Pr[Y_1] - \frac{1}{2}\right|, \\
\left|\Pr[Y_1] - \frac{1}{2}\right| &\le \frac{1}{2} \cdot \left|\Pr[Y_1 | h = 0] - \frac{1}{2}\right| \\
&\quad + \frac{1}{2} \cdot \left|\Pr[Y_1 | h = 1] - \frac{1}{2}\right|.
\end{aligned}$$

The games in the case of the guess $h = 0$ are as follows.

Game 2. In this game, the challenger changes the way to answer the public key request queries. When $\mathcal{A}_I$ asks for a public key for the identity id, assume that $\mathcal{A}_I$ has not queried the partial private key on id. If $id = id^*$, the challenger chooses $\mathbf{v}_{id^*} \leftarrow \mathbb{Z}_q^n$ at random, extracts $\mathbf{d}^* \leftarrow \mathsf{Extract}(mpk, msk, id^*)$ and lets $\mathbf{w}_{id^*} = \mathbf{W} \cdot \mathbf{d}^* \bmod q$, and returns $pk_{id^*} = (\mathbf{v}_{id^*}, \mathbf{w}_{id^*})$ to $\mathcal{A}_I$. Otherwise, the challenger extracts $\mathbf{d} \leftarrow \mathsf{Extract}(mpk, msk, id)$, generates $(pk_{id}, sk_{id}) \leftarrow \mathsf{KeyGen}(mpk, id, \mathbf{d})$, and returns pk_{id} to $\mathcal{A}_I$. By Corollary 5.4 in [21], Game 2 is statistically indistinguishable from Game 1. Hence,

$$\left|\Pr\left[Y_1 | h = 0\right] - \Pr\left[Y_2\right]\right| = \mathrm{negl}(\lambda).$$

Game 3. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects $\widehat{\mathbf{V}} \leftarrow \mathbb{Z}_q^{m \times N}$ and $\widehat{\mathbf{v}}_{id^*} \leftarrow \mathbb{Z}_q^N$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}_{id^*}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_{id^*} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \widehat{\mathbf{V}} \\ \mathbf{u}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \widehat{\mathbf{v}}_{id^*}^{\mathrm{T}} + \mathbf{w}_{id^*}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

Suppose $\mathcal{A}_I$ has a non-negligible advantage in distinguishing Game 2 from Game 3. We use $\mathcal{A}_I$ to construct an algorithm $\mathcal{B}_1$ to solve a $\mathsf{DLWE}_{n,q,\chi}$ problem instance $\left((\mathbf{F}, \mathbf{f}), \begin{pmatrix} \mathbf{P} \\ \mathbf{p}^{\mathrm{T}} \end{pmatrix}\right) \in \mathbb{Z}_q^{n \times (m+1)} \times \mathbb{Z}_q^{(m+1) \times N}$. $\mathcal{B}_1$ simulates the challenger for $\mathcal{A}_I$ using the following way: $\mathcal{B}_1$ sets $\mathbf{V} = \mathbf{F}$, sets $\mathbf{v}_{id^*} = \mathbf{f}$, and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}_{id^*}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_{id^*} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{P} \\ \mathbf{u}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \mathbf{p}^{\mathrm{T}} + \mathbf{w}_{id^*}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

It can be seen that the advantage of $\mathcal{B}_1$ in solving the given DLWE problem instance is the same as that of $\mathcal{A}_I$ in distinguishing Game 2 from Game 3. Therefore,

$$\left|\Pr\left[Y_2\right] - \Pr\left[Y_3\right]\right| \leq \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_1}(\lambda).$$

Game 4. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects $\overset{\triangle}{\mathbf{v}}_{id^*} \leftarrow \mathbb{Z}_q^N$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}_{id^*}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_{id^*} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_{id^*}{}^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

In Game 3, $\widehat{\mathbf{v}}_{id^*}^{\mathrm{T}}$ is uniformly random in $\mathbb{Z}_q^{1 \times N}$; thus, $\mathbf{u}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{e}_1^{\mathrm{T}} + \widehat{\mathbf{v}}_{id^*}^{\mathrm{T}} + \mathbf{w}_{id^*}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}}$ is also uniformly random in $\mathbb{Z}_q^{1 \times N}$. Therefore,

$$\left|\Pr\left[Y_3\right] - \Pr\left[Y_4\right]\right| = \mathrm{negl}(\lambda).$$

Game 5. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects $\widehat{\mathbf{W}} \leftarrow \mathbb{Z}_q^{2m \times N}$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}_{id^*}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_{id^*} + \widehat{\mathbf{W}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_{id^*}^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

Suppose $\mathcal{A}_I$ has a non-negligible advantage in distinguishing Game 4 from Game 5. We use $\mathcal{A}_I$ to construct an algorithm $\mathcal{B}_2$ to solve a $\mathsf{DLWE}_{n,q,\chi}$ problem instance $(\mathbf{F}, \mathbf{P}) \in \mathbb{Z}_q^{n \times 2m} \times \mathbb{Z}_q^{2m \times N}$. $\mathcal{B}_2$ simulates the challenger for $\mathcal{A}_I$ in the following way: $\mathcal{B}_2$ sets $\mathbf{W} = \mathbf{F}$ and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{A}_{id^*}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_{id^*} + \mathbf{P} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_{id^*}^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

It can be seen that the advantage of $\mathcal{B}_2$ in solving the given DLWE problem instance is the same as that of $\mathcal{A}_I$ in distinguishing Game 4 from Game 5. Therefore,

$$\left|\Pr\left[Y_4\right] - \Pr\left[Y_5\right]\right| \leq \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_2}(\lambda).$$

Game 6. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects $\widehat{\mathbf{W}} \leftarrow \mathbb{Z}_q^{2m \times N}$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \overset{\triangle}{\mathbf{W}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_{id^*}^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

In Game 5, $\widehat{\mathbf{W}}$ is uniformly random in $\mathbb{Z}_q^{2m \times N}$; thus, $\mathbf{A}_{id^*}^{\mathrm{T}}\mathbf{S}_1 + \mathbf{E}_{id^*} + \widehat{\mathbf{W}}$ is also uniformly random in $\mathbb{Z}_q^{2m \times N}$. Therefore,

$$\left|\Pr\left[Y_5\right] - \Pr\left[Y_6\right]\right| = \mathrm{negl}(\lambda).$$

Game 7. In this game, the challenger changes the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects the challenge ciphertext $\mathbf{C}_0^* \leftarrow \mathbb{Z}_q^{(3m+1) \times N}$ at random. In Game 6, $\begin{pmatrix} \overset{\triangle}{\mathbf{W}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_{id^*}^{\mathrm{T}} \end{pmatrix}$ is a random element in $\mathbb{Z}_q^{(3m+1) \times N}$; hence $\begin{pmatrix} \overset{\triangle}{\mathbf{W}} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{v}}_{id^*}^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}$ is also a random element in $\mathbb{Z}_q^{(3m+1) \times N}$. Therefore,

$$\left|\Pr\left[Y_6\right] - \Pr\left[Y_7\right]\right| = \mathrm{negl}(\lambda).$$

In Game 7,

$$\left|\Pr\left[Y_7\right] - \frac{1}{2}\right| = 0.$$

The games in the case of the guess $h = 1$ are as follows.

Game 2′. Compared with Game 1, Game 2′ makes two changes:

1) At the setup phase, the challenger samples $\mathbf{R} \leftarrow D_{\mathbb{Z},\omega(\sqrt{\log m})}^{m \times m}$. Notice that the challenger will use $\mathbf{R}$ to generate the challenge ciphertext $\mathbf{C}_0^*$ in the challenge phase.
2) At the setup phase, the challenger constructs $\mathbf{A}_1$ as $\mathbf{A}_1 = \mathbf{A}\mathbf{R} - H(id^*) \cdot \mathbf{B}$. In this way, we obtain

$$\mathbf{A}_{id^*} = \left(\mathbf{A} | \mathbf{A}_1 + H(id^*) \cdot \mathbf{B}\right) = \left(\mathbf{A} | \mathbf{A}\mathbf{R}\right).$$

By the leftover hash lemma [33], [34], we obtain

$$\left|\Pr\left[Y_1|h=1\right]-\Pr\left[Y_2'\right]\right| = \mathrm{negl}(\lambda).$$

Game 3′. Compared with Game 2′, Game 3′ makes four changes:

1) At the setup phase, the challenger generates $\mathbf{A}$ as a random matrix in $\mathbb{Z}_q^{n\times m}$.
2) At the setup phase, the challenger generates $\mathbf{B}$ by invoking the algorithm $\mathsf{GenBasis}\,(1^n, 1^m, q)$ so that $\mathbf{B}$ is a random matrix in $\mathbb{Z}_q^{n\times m}$, but the challenger gets a trapdoor $\mathbf{T_B}$ for $\Lambda^{\perp}(\mathbf{B})$ such that $\|\widetilde{\mathbf{T_B}}\| \le O(\sqrt{n\log q})$.
3) When $\mathcal{A}_I$ asks for a partial private key for the identity id, the challenger does the following: If $id = id^*$, it aborts and outputs a random bit, i.e., $\mathcal{A}_I$ wins the game with a probability of $1/2$. Otherwise for $id \neq id^*$, we have that

$$\begin{aligned}\mathbf{A}_{id} &= (\mathbf{A}|\mathbf{A}_1 + H(id)\cdot\mathbf{B})\\ &= \left(\mathbf{A}|\mathbf{A}\mathbf{R} + \left(H(id) - H(id^*)\right)\cdot\mathbf{B}\right).\end{aligned}$$

Since $H(id) - H(id^*) \neq \mathbf{0} \in \mathbb{Z}_q^{n\times n}$, $\mathbf{T_B}$ is also a trapdoor for $\Lambda_q^{\perp}\left((H(id) - H(id^*))\cdot\mathbf{B}\right)$. It samples

$$\mathbf{d} \leftarrow \mathsf{SampleRight}\left(\mathbf{A}, \mathbf{B}', \mathbf{R}, \mathbf{T_B}, \mathbf{u}, \sigma_1\right) \in \mathbb{Z}^{2m},$$

where $\mathbf{B}' = (H(id) - H(id^*))\cdot\mathbf{B}$, and returns $\mathbf{d}$ to $\mathcal{A}_I$. Note that $\mathbf{A}_{id}\cdot\mathbf{d} = \mathbf{u} \mod q$ and $\mathbf{d}$ is distributed as $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}_{id}),\sigma_1}$ by Proposition 5.
4) When $\mathcal{A}_I$ asks for a public key for the identity id, the challenger does the following: If $id = id^*$, it samples $\mathbf{x}^* \leftarrow D_{\mathbb{Z}^m,\sigma_2}$ and lets $\mathbf{v}_{id^*} = \mathbf{V}\cdot\mathbf{x}^* \mod q$, chooses $\mathbf{w}_{id^*} \leftarrow \mathbb{Z}_q^n$ at random, and returns $pk_{id^*} = (\mathbf{v}_{id^*}, \mathbf{w}_{id^*})$ to $\mathcal{A}_I$. Otherwise for $id \neq id^*$, assume that $\mathcal{A}_I$ has not queried the partial private key on id. It samples $\mathbf{d} \leftarrow \mathsf{SampleRight}\left(\mathbf{A}, \mathbf{B}', \mathbf{R}, \mathbf{T_B}, \mathbf{u}, \sigma_1\right)$ where $\mathbf{B}' = (H(id) - H(id^*))\cdot\mathbf{B}$, generates $(pk_{id}, sk_{id}) \leftarrow \mathsf{KeyGen}(mpk, id, \mathbf{d})$, and returns pk_{id} to $\mathcal{A}_I$.

Since σ_1 used in the scheme is sufficiently large, Game 3′ is statistically indistinguishable from Game 2′. Therefore,

$$\left|\Pr\left[Y_2'\right]-\Pr\left[Y_3'\right]\right| = \mathrm{negl}(\lambda).$$

Game 4′. In this game, we change the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects $\widehat{\mathbf{A}}_{id^*} \leftarrow \mathbb{Z}_q^{2m\times N}$ and $\widehat{\mathbf{u}} \leftarrow \mathbb{Z}_q^N$ at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \widehat{\mathbf{A}}_{id^*} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \widehat{\mathbf{u}}^{\mathrm{T}} + \mathbf{v}_{id^*}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}_{id^*}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu\cdot\mathbf{G}.$$

Suppose $\mathcal{A}_I$ has a non-negligible advantage in distinguishing Game 3′ from Game 4′. We use $\mathcal{A}_I$ to construct an algorithm $\mathcal{B}_3$ to solve a $\mathsf{DLWE}_{n,q,\chi}$ problem instance $\left((\mathbf{F}, \mathbf{f}), \begin{pmatrix}\mathbf{P}\\ \mathbf{p}^{\mathrm{T}}\end{pmatrix}\right) \in \mathbb{Z}_q^{n\times(m+1)} \times \mathbb{Z}_q^{(m+1)\times N}$. $\mathcal{B}_3$ simulates the challenger for $\mathcal{A}_I$ as follows: $\mathcal{B}_3$ sets $\mathbf{A} = \mathbf{F}$ and $\mathbf{u} = \mathbf{f}$, sets $\mathbf{P}_{id^*} = \begin{pmatrix}\mathbf{P}\\ \mathbf{R}^{\mathrm{T}}\cdot\mathbf{P}\end{pmatrix}$, and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \mathbf{P}_{id^*} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3 \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \mathbf{p}^{\mathrm{T}} + \mathbf{v}_{id^*}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}_{id^*}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}} \end{pmatrix} + \mu\cdot\mathbf{G}.$$

When $\left((\mathbf{F}, \mathbf{f}), \begin{pmatrix}\mathbf{P}\\ \mathbf{p}^{\mathrm{T}}\end{pmatrix}\right) \leftarrow A_{\mathbf{S},\chi}$ where the secret $\mathbf{S} \in \mathbb{Z}_q^{n\times N}$, it can be observed that

$$\begin{aligned}\mathbf{P}_{id^*} &= \begin{pmatrix}\mathbf{P}\\ \mathbf{R}^{\mathrm{T}}\cdot\mathbf{P}\end{pmatrix} = \begin{pmatrix}\mathbf{A}^{\mathrm{T}}\mathbf{S} + \mathbf{E}\\ \mathbf{R}^{\mathrm{T}}\cdot\mathbf{A}^{\mathrm{T}}\mathbf{S} + \mathbf{R}^{\mathrm{T}}\cdot\mathbf{E}\end{pmatrix}\\ &= (\mathbf{A}|\mathbf{A}\mathbf{R})^{\mathrm{T}}\,\mathbf{S} + \begin{pmatrix}\mathbf{E}\\ \mathbf{R}^{\mathrm{T}}\cdot\mathbf{E}\end{pmatrix} = \mathbf{A}_{id^*}^{\mathrm{T}}\mathbf{S} + \begin{pmatrix}\mathbf{E}\\ \mathbf{R}^{\mathrm{T}}\cdot\mathbf{E}\end{pmatrix},\\ \mathbf{p}^{\mathrm{T}} &= \mathbf{u}^{\mathrm{T}}\mathbf{S} + \mathbf{e}^{\mathrm{T}}.\end{aligned}$$

Thus, $\mathbf{C}_0^*$ is distributed exactly as in Game 3′. When $\left((\mathbf{F}, \mathbf{f}), \begin{pmatrix}\mathbf{P}\\ \mathbf{p}^{\mathrm{T}}\end{pmatrix}\right)$ is chosen from the uniform distribution over $\mathbb{Z}_q^{n\times(m+1)} \times \mathbb{Z}_q^{(m+1)\times N}$, we obtain that $\mathbf{P}_{id^*}$ is uniform in $\mathbb{Z}_q^{2m\times N}$ by the leftover hash lemma [33], [34], and that $\mathbf{p}$ is uniform in $\mathbb{Z}_q^N$. Consequently, $\mathbf{C}_0^*$ is distributed exactly as in Game 4′. Hence, the advantage of $\mathcal{B}_3$ in solving the given DLWE problem instance is the same as that of $\mathcal{A}_I$ in distinguishing Game 3′ from Game 4′. Therefore,

$$\left|\Pr\left[Y_3'\right]-\Pr\left[Y_4'\right]\right| \le \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_3}(\lambda).$$

Game 5′. In this game, we change the way in which the challenge ciphertext $\mathbf{C}_0^*$ is created. The challenger selects $\overset{\triangle}{\mathbf{A}}_{id^*} \leftarrow \mathbb{Z}_q^{2m\times N}$ and $\overset{\triangle}{\mathbf{u}} \leftarrow \mathbb{Z}_q^N$at random and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \overset{\triangle}{\mathbf{A}}_{id^*} \\ \mathbf{V}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{E}_2 \\ \overset{\triangle}{\mathbf{u}}^{\mathrm{T}} \end{pmatrix} + \mu\cdot\mathbf{G}.$$

In Game 4′, $\widehat{\mathbf{A}}_{id^*}$ and $\widehat{\mathbf{u}}^{\mathrm{T}}$ are uniformly random in $\mathbb{Z}_q^{2m\times N}$ and $\mathbb{Z}_q^{1\times N}$, respectively; hence, $\widehat{\mathbf{A}}_{id^*} + \mathbf{W}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{E}_3$ and $\widehat{\mathbf{u}}^{\mathrm{T}} + \mathbf{v}_{id^*}^{\mathrm{T}}\mathbf{S}_2 + \mathbf{e}_2^{\mathrm{T}} + \mathbf{w}_{id^*}^{\mathrm{T}}\mathbf{S}_3 + \mathbf{e}_3^{\mathrm{T}}$ are also uniformly random in $\mathbb{Z}_q^{2m\times N}$ and $\mathbb{Z}_q^{1\times N}$, respectively. Therefore,

$$\left|\Pr\left[Y_4'\right]-\Pr\left[Y_5'\right]\right| = \mathrm{negl}(\lambda).$$

Game 6′. In this game, we change the way in which the challenge ciphertext $\mathbf{C}_0^*$ is generated. The challenger selects $\widehat{\mathbf{V}} \leftarrow \mathbb{Z}_q^{m\times N}$ at random and sets the challenge ciphertex

$$\mathbf{C}_0^* = \begin{pmatrix} \overset{\triangle}{\mathbf{A}}_{id^*} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{u}}^{\mathrm{T}} \end{pmatrix} + \mu\cdot\mathbf{G}.$$

Suppose $\mathcal{A}_I$ has a non-negligible advantage in distinguishing Game 5′ from Game 6′. We use $\mathcal{A}_I$ to construct an algorithm $\mathcal{B}_4$ to solve a $\mathsf{DLWE}_{n,q,\chi}$ problem instance

$(\mathbf{F}, \mathbf{P}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times N}$. $\mathcal{B}_4$ simulates the challenger for $\mathcal{A}_I$ as follows: $\mathcal{B}_4$ sets $\widehat{\mathbf{V}} = \mathbf{F}$ and sets the challenge ciphertext

$$\mathbf{C}_0^* = \begin{pmatrix} \overset{\triangle}{\mathbf{A}}_{id^*} \\ \mathbf{P} \\ \overset{\triangle}{\mathbf{u}}^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}.$$

Clearly, the advantage of $\mathcal{B}_4$ in solving the given DLWE problem instance is the same as that of $\mathcal{A}_I$ in distinguishing Game 5′ from Game 6′. Therefore,

$$\left|\Pr[Y_5'] - \Pr[Y_6']\right| \leq \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_4}(\lambda).$$

Game 7′. In this game, we change the way in which the challenge ciphertext $\mathbf{C}_0^*$ is created. The challenger selects the challenge ciphertex $\mathbf{C}^* \leftarrow \mathbb{Z}_q^{(3m+1)\times N}$ at random. In Game 6′, $\begin{pmatrix} \overset{\triangle}{\mathbf{A}}_{id^*} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{u}}^{\mathrm{T}} \end{pmatrix}$ is a random element in $\mathbb{Z}_q^{(3m+1)\times N}$; thus, $\begin{pmatrix} \overset{\triangle}{\mathbf{A}}_{id^*} \\ \widehat{\mathbf{V}} \\ \overset{\triangle}{\mathbf{u}}^{\mathrm{T}} \end{pmatrix} + \mu \cdot \mathbf{G}$ is also a random element in $\mathbb{Z}_q^{(3m+1)\times N}$. Therefore,

$$\left|\Pr[Y_6'] - \Pr[Y_7']\right| = \mathrm{negl}(\lambda).$$

In Game 7′,

$$\left|\Pr[Y_7'] - \frac{1}{2}\right| = 0.$$

To sum up, we obtain that

$$\begin{aligned}
&\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_I}^{\mathrm{INDr-sID-CPA}}(\lambda) = \left|\Pr[Y_0] - \frac{1}{2}\right| \\
&= 2 \cdot \left|\Pr[Y_1] - \frac{1}{2}\right| \\
&\leq \left|\Pr[Y_1|h=0] - \frac{1}{2}\right| + \left|\Pr[Y_1|h=1] - \frac{1}{2}\right| \\
&= \left|\Pr[Y_2] - \frac{1}{2}\right| + \left|\Pr[Y_2'] - \frac{1}{2}\right| + \mathrm{negl}(\lambda) \\
&\leq \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_1}(\lambda) + \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_2}(\lambda) \\
&\quad + \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_3}(\lambda) + \mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_4}(\lambda) + \mathrm{negl}(\lambda) \\
&\leq 4 \cdot \mathrm{Adv}_{\mathsf{DLWE}}(\lambda) + \mathrm{negl}(\lambda),
\end{aligned}$$

where $\mathrm{Adv}_{\mathsf{DLWE}}(\lambda) = \max \left\{\mathrm{Adv}_{\mathsf{DLWE},\mathcal{B}_i}(\lambda)\right\}_{i\in[4]}$.

□

Theorem 4: The CLFHE scheme in Section V-A is INDr-sID-CPA secure against Type II attacks if the $\mathsf{DLWE}_{n,q,\chi}$ assumption holds. In particular, suppose there exists an attacker $\mathcal{A}_{II}$ that wins the INDr-sID-CPA game defined in Section III-C with an advantage $\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_{II}}^{\mathrm{INDr-sID-CPA}}(\lambda)$, then there exists an algorithm that solves the $\mathsf{DLWE}_{n,q,\chi}$ problem with an advantage $\mathrm{Adv}_{\mathsf{DLWE}}(\lambda)$ such that

$$\mathrm{Adv}_{\mathrm{CLFHE},\mathcal{A}_{II}}^{\mathrm{INDr-sID-CPA}}(\lambda) \leq 2 \cdot \mathrm{Adv}_{\mathsf{DLWE}}(\lambda) + \mathrm{negl}(\lambda).$$

The proof of Theorem 4 is similar to that of Theorem 3 in the case of the guess $h = 0$. Thus, we omit the detailed proof of Theorem 4 here.

VI. CONCLUSION AND FUTURE WORK

Based on the LWE problem, we constructed two leveled CLFHE schemes, one in the random oracle model and the other in the standard model. Our future work includes the following:

1) The ring-LWE problem [35] is an algebraic variant of the LWE problem. In general, CLFHE schemes based on the ring-LWE problem have much better performance than schemes based on the LWE problem. Thus, we will construct leveled CLFHE schemes based on the ring-LWE problem.
2) Several chosen-ciphertext secure FHE schemes [36]–[38] have been proposed. An otherwise secure CLFHE scheme may be defeated under a chosen-ciphertext attack. Therefore, we will construct chosen-ciphertext secure leveled CLFHE schemes based on the LWE problem.
3) Multi-key FHE [39] allows homomorphic computation on data encrypted under different keys. Multi-key FHE schemes [40]–[42] and multi-key identity-based FHE schemes [43], [44] have been proposed. We will design multi-key certificateless FHE schemes.
4) Proxy re-encryption (PRE) [45] is an extension of public-key encryption. Homomorphic proxy re-encryption (HPRE) schemes [46], [47] and identity-based HPRE schemes [48] have been proposed. We will design certificateless HPRE schemes.

REFERENCES

[1] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On data banks and privacy homomorphisms,” *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, 1978.

[2] C. Gentry, “Fully homomorphic eneryption using ideal lattices,” in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, Bethesda, MD, USA, May/Jun. 2009, pp. 169–178.

[3] C. Gentry, A. Sahai, and B. Waters, “Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based,” in *Proc. 33rd Annu. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 2013, pp. 75–92.

[4] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” in *Proc. 37th Annu. ACM Symp. Theory Comput. (STOC)*, Baltimore, MD, USA, May 2005, pp. 84–93.

[5] J. Alperin-Sheriff and C. Peikert, “Faster bootstrapping with polynomial error,” in *Proc. 34th Annu. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 2014, pp. 297–314.

[6] D. Micciancio and C. Peikert, “Trapdoors for lattices: Simpler, tighter, faster, smaller,” in *Proc. 31st Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*. Cambridge, U.K.: Springer, Apr. 2012, pp. 700–718.

[7] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” in *Proc. 9th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT)*, Taipei, Taiwan. Berlin, Germany: Springer, Nov./Dec. 2003, pp. 452–473.

[8] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Proc. 4th Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 1984, pp. 47–53.

[9] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in *Proc. 21st Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 2001, pp. 213–229.

[10] A. W. Dent, “A survey of certificateless encryption schemes and security models,” *Int. J. Inf. Secur.*, vol. 7, no. 5, pp. 349–377, 2008.

[11] A. W. Dent, “A brief introduction to certificateless encryption schemes and their infrastructures,” in *Proc. 6th Eur. Workshop Public Key Infrastruct., Services Appl. (EuroPKI)*, Pisa, Italy. Berlin, Germany: Springer, Sep. 2009, 2009, pp. 1–16.

[12] M. Jiang, Y. Hu, H. Lei, B. Wang, and Q. Lai, "Lattice-based certificateless encryption scheme," *Frontiers Comput. Sci.*, vol. 8, no. 5, pp. 828–836, 2014.

[13] R. Sepahi, R. Steinfeld, and J. Pieprzyk, "Lattice-based certificateless public-key encryption in the standard model," *Int. J. Inf. Secur.*, vol. 13, no. 4, pp. 315–333, Aug. 2014.

[14] Y. Guang, C.-X. Gu, Y.-F. Zhu, Y.-H. Zheng, and J.-L. Fei, "Certificateless fully homomorphic encryption based on LWE problem," (in Chinese), *J. Electron. Inf. Technol.*, vol. 35, no. 4, pp. 988–993, Feb. 2014.

[15] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in *Proc. 52nd Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Palm Springs, CA, USA, Oct. 2011, pp. 97–106.

[16] H. Chen, Y. Hu, and Z. Lian, "Leveled homomorphic encryption in certificateless cryptosystem," *Chin. J. Electron.*, vol. 26, no. 6, pp. 1213–1220, Nov. 2017.

[17] F. Wang, K. Wang, and B. Li, "An efficient leveled identity-based FHE," in *Proc. 9th Int. Conf. Netw. Syst. Secur. (NSS)*. New York, NY, USA: Springer, Nov. 2015, pp. 303–315.

[18] X. Sun, J. Yu, T. Wang, Z. Sun, and P. Zhang, "Efficient identity-based leveled fully homomorphic encryption from RLWE," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5155–5165, Dec. 2016.

[19] M. Hu, Q. Ye, and Y. Tang, "Efficient batch identity-based fully homomorphic encryption scheme in the standard model," *IET Inf. Secur.*, vol. 12, no. 6, pp. 475–483, Nov. 2018.

[20] F. Luo, K. Wang, and C. Lin, "Leveled hierarchical identity-based fully homomorphic encryption from learning with rounding," in *Proc. 14th Int. Conf. Inf. Secur. Pract. Exper. (ISPEC)*, Tokyo, Japan. Cham, Switzerland: Springer, Sep. 2018, pp. 101–115.

[21] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 40th Annu. ACM Symp. Theory Comput. (STOC)*, Victoria, BC, Canada, May 2008, pp. 197–206.

[22] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Proc. 29th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Monaco, France. Berlin, Germany: Springer, May/Jun. 2010, pp. 553–572.

[23] M. Ajtai, "Generating hard instances of the short basis problem," in *Proc. 26th Int. Colloq. Automata, Lang., Program. (ICALP)*, Prague, Czech Republic. Berlin, Germany: Springer, Jul. 1999, pp. 1–9.

[24] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," in *Proc. 26th Int. Symp. Theor. Aspects Comput. Sci. (STACS)*, Freiburg, Germany, Feb. 2009, pp. 75–86.

[25] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," in *Proc. 45th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Rome, Italy, Oct. 2004, pp. 372–381.

[26] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, Bethesda, MD, USA, May/Jun. 2009, pp. 333–342.

[27] D. Micciancio and P. Mol, "Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions," in *Proc. 31st Annu. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 2011, pp. 465–484.

[28] R. Hiromasa, M. Abe, and T. Okamoto, "Packing messages and optimizing bootstrapping in GSW-FHE," in *Proc. 18th Int. Conf. Pract. Theory Public-Key Cryptogr. (PKC)*, Gaithersburg, MD, USA. Berlin, Germany: Springer, Mar./Apr. 2015, pp. 699–715.

[29] J. Baek, R. Safavi-Naini, and W. Susilo, "Certificateless public key encryption without pairing," in *Proc. 8th Int. Conf. Inf. Secur. (ISC)*. Singapore: Springer, Sep. 2005, pp. 134–148.

[30] J. Lai and W. Kou, "Self-generated-certificate public key encryption without pairing," in *Proc. 10th Int. Conf. Pract. Theory Public-Key Cryptogr. (PKC)*, Beijing, China, Springer, Apr. 2007, pp. 476–489.

[31] Z. Brakerski, D. Cash, R. Tsabary, and H. Wee, "Targeted homomorphic attribute-based encryption," in *Proc. 14th Theory Cryptogr. Conf. (TCC-B)*. Beijing, China: Springer, Oct./Nov. 2016, pp. 330–360.

[32] Z. Li, C. Ma, and D. Wang, "Leakage resilient leveled FHE on multiple bit message," *IEEE Trans. Big Data*, to be published, doi: 10.1109/TBDATA.2017.2726554.

[33] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM J. Comput.*, vol. 28, no. 4, pp. 1364–1396, Jan. 1999.

[34] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008.

[35] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. 29th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Monaco, France. Berlin, Germany: Springer, May/Jun. 2010, pp. 1–23.

[36] J. Loftus, A. May, N. P. Smart, and F. Vercauteren, "On CCA-secure somewhat homomorphic encryption," in *Proc. 18th Int. Workshop Sel. Areas Cryptogr. (SAC)*, Toronto, ON, Canada. Berlin, Germany: Springer, Aug. 2011, pp. 55–72.

[37] R. Canetti, S. Raghuraman, S. Richelson, and V. Vaikuntanathan, "Chosen-ciphertext secure fully homomorphic encryption," in *Proc. 20th Int. Conf. Pract. Theory Public-Key Cryptogr. (PKC)*. Amsterdam, The Netherlands: Springer, Mar. 2017, pp. 213–240.

[38] S. Yasuda, F. Kitagawa, and K. Tanaka, "Constructions for the IND-CCA1 secure fully homomorphic encryption," in *Mathematical Modelling for Next-Generation Cryptography* (Mathematics for Industry) vol. 29. Singapore: Springer, 2018, pp. 331–347.

[39] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in *Proc. 44th Annu. ACM Symp. Theory Comput. Conf. (STOC)*, New York, NY, USA, May 2012, pp. 1219–1234.

[40] P. Mukherjee and D. Wichs, "Two round multiparty computation via multi-key FHE," in *Proc. 35th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*. Vienna, Austria: Springer, May 2016, pp. 735–763.

[41] C. Peikert and S. Shiehian, "Multi-key FHE from LWE, revisited," in *Proc. 14th Int. Conf. Theory Cryptogr. (TCC-B)*. Beijing, China: Springer, Oct./Nov. 2016, pp. 217–238.

[42] Z. Li, C. Ma, and H. Zhou, "Multi-key FHE for multi-bit messages," *Sci. China Inf. Sci.*, vol. 61, no. 2, pp. 029101:1–029101:3, 2018.

[43] M. Clear and C. McGoldrick, "Multi-identity and multi-key leveled FHE from learning with errors," in *Proc. 35th Annu. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 2015, pp. 630–656.

[44] T. Shen, F. Wang, K. Chen, K. Wang, and B. Li, "Efficient leveled (multi) identity-based fully homomorphic encryption schemes," *IEEE Access*, vol. 7, pp. 79299–79310, 2019, doi: 10.1109/ACCESS.2019.2922685.

[45] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. 17th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Espoo, Finland. Berlin, Germany: Springer, May/Jun. 1998, pp. 127–144.

[46] C. Ma, J. Li, and W. Ouyang, "A homomorphic proxy re-encryption from lattices," in *Proc. 10th Int. Conf. Provable Secur. (ProvSec)*, Nanjing, China. Cham, Switzerland: Springer, Nov. 2016, pp. 353–372.

[47] M. Zhang, L. Wu, X. A. Wang, and X. Yang, "Unidirectional IBPRE scheme from lattice for cloud computation," *Int. J. Netw. Secur.*, vol. 7, vol. 21, no. 4, pp. 592–600, 2019.

[48] Z. Li, C. Ma, and D. Wang, "Towards multi-hop homomorphic identity-based proxy re-encryption via branching program," *IEEE Access*, vol. 5, pp. 16214–16228, 2017, doi: 10.1109/ACCESS.2017.2740720.

MINGXIANG LI received the Ph.D. degree in computer application technology from the University of Science and Technology Beijing, Beijing, China, in 2009. He is currently an Associate Professor with the Institute of Financial Research, Hebei Finance University, China, and a Research Fellow with the Science and Technology Finance Key Laboratory of Hebei Province, China. His research interests include fully homomorphic encryption, lattice-based cryptography, and post-quantum cryptography.