Computer Science and Application 计算机科学与应用, 2023, 13(10), 1948-1964
Published Online October 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.1310193

Hans汉斯

基于LWR问题的无证书全同态加密方案

李明祥

河北金融学院金融研究所，河北 保定

收稿日期：2023年9月20日；录用日期：2023年10月18日；发布日期：2023年10月25日

摘 要

无证书全同态加密(CLFHE)把全同态加密和无证书加密两者的优势结合了起来，它吸引了人们关注的目光。目前人们基于带误差学习(LWE)问题提出了几个CLFHE方案。带舍入学习(LWR)问题是LWE问题的变形。它免除了LWE问题中计算代价高昂的高斯噪声抽样。迄今为止人们尚未提出基于LWR问题的CLFHE方案。本文利用Gentry、Sahai和Waters提出的近似特征向量技术，基于LWR问题设计了一个CLFHE方案，并在随机预言机模型下证明了它满足INDr-CPA安全性。与已有的基于LWE问题的CLFHE方案相比，所设计的方案免除了耗时的高斯噪声抽样而具有更高的计算效率。

关键词

全同态加密，无证书，LWE问题，LWR问题，随机预言机模型

Certificateless Fully Homomorphic Encryption Scheme Based on the LWR Problem

Mingxiang Li

Institute of Financial Research, Hebei Finance University, Baoding Hebei

Received: Sep. 20th, 2023; accepted: Oct. 18th, 2023; published: Oct. 25th, 2023

Abstract

Certificateless fully homomorphic encryption (CLFHE) combines the advantages of fully homomorphic encryption and certificateless encryption. Itcatches the attention of researchers. Several CLFHE schemes have been proposed based on the learning with errors (LWE) problem. The learning with rounding (LWR) problem is a variant of the LWE problem. It dispenses withthe costly Gaussian noise sampling required in the LWE problem. So far, no CLFHE scheme based on the LWR problem has been proposed. This paper designs a CLFHE scheme based on the LWR problem using

文章引用: 李明祥. 基于 LWR 问题的无证书全同态加密方案[J]. 计算机科学与应用, 2023, 13(10): 1948-1964.
DOI: 10.12677/csa.2023.1310193

Gentry, Sahai, and Waters's approximate eigenvector technique and proves that the designed scheme satisfies INDr-CPA securityin the random oracle model. Compared with existing CLFHE schemes based on the LWE problem, the proposedschemedispenses with the costly Gaussian noise sampling and enjoys higher computational efficiency.

Keywords

Fully Homomorphic Encryption, Certificateless, LWE Problem, LWR Problem, Random Oracle Model

1. 引言

全同态加密(Fully Homomorphic Encryption, FHE)是一种具有特殊性质的公钥加密体制。它能在不解密的情形下对密文数据进行任意计算，即 $\mathrm{Dec}\left(f\left(\mathrm{Enc}\left(\mu_1\right),\cdots,\mathrm{Enc}\left(\mu_\ell\right)\right)\right)=f\left(\mu_1,\cdots,\mu_\ell\right)$，其中 f 为任意函数。2009 年 Gentry [1]基于理想格提出了第一个全同态加密方案。Genry 开拓性的工作迅速掀起了全同态加密研究的浪潮。2013 年 Gentry、Sahai 和 Waters [2]提出了一种构造全同态加密方案的新技术，他们称之为近似特征向量技术。Gentry、Sahai 和 Waters [2]利用近似特征向量技术，基于带误差学习(Learning with Errors, LWE)问题[3]构造了一个层次型全同态加密(leveledFHE)方案。在层次型全同态加密方案中，方案的参数取决于方案所能计算的电路深度。利用 Gentry [1]提出的自举技术可以把层次型全同态加密方案转换为全同态加密方案。本文的工作专注于层次型全同态加密方案，故在下文的叙述中经常省去“层次型”一词。

无证书加密(Certificateless Encryption, CLE) [4]是一种新型公钥加密体制。它消除了基于身份的加密(Identity-Based Encryption, IBE) [5]固有的密钥托管问题，同时，它也避免了传统公钥加密系统中的公钥证书管理问题。无证书全同态加密(Certificateless Fully Homomorphic Encryption, CLFHE)结合了全同态加密和无证书加密两者的优势，它引起了人们的研究兴趣。2017 年 Chen 等人[6]利用近似特征向量技术，基于 LWE 问题提出了一个无证书全同态加密方案，并在随机预言机模型下证明了它满足 IND-CPA 安全性。最近，Li [7]利用近似特征向量技术，基于 LWE 问题又提出了一个在随机预言模型下可证明安全的无证书全同态加密方案和一个在标准模型下可证明安全的无证书全同态加密方案。

带舍入学习(Learning with Rounding, LWR)问题[8]是 LWE 问题[3]的变形。LWE 问题需要进行高斯噪声抽样。高斯噪声抽样的计算开销非常大，严重制约了基于 LWE 问题的全同态加密方案的计算性能。LWR 问题不需要进行高斯噪声抽样。近几年来，人们基于 LWR 问题构造了几个全同态加密方案[9] [10]。与 Gentry、Sahai 和 Waters [2]提出的基于 LWE 问题的全同态加密方案相比，这些全同态加密方案[9] [10]由于舍弃了计算代价高昂的高斯噪声抽样其计算效率有了很大提高。截至目前，人们尚未提出基于 LWR 问题的无证书全同态加密方案。

鉴于无证书全同态加密的研究现状，本文致力于基于 LWR 问题的无证书全同态加密方案的设计与分析。首先，利用 Gentry、Sahai 和 Waters [2]提出的近似特征向量技术，基于 LWR 问题设计了一个无证书全同态加密方案。其次，在随机预言机模型下证明了所设计的方案满足 INDr-CPA 安全性。INDr-CPA 比 IND-CPA 的安全性更强，它包括 IND-CPA 安全性和接收方匿名性。最后，本文具体给出了所设计的

方案的系统参数设置。相比于现有的基于 LWE 问题的无证书全同态加密方案[6] [7]，本文所设计的方案省掉了耗时的高斯噪声抽样，其计算效率更高。

2. 预备知识

2.1. 符号约定

下面介绍本文的符号约定，如表 1 所示。

Table 1. Notations and descriptions
表 1. 符号及其描述

符号	描述
$\mathbb{N}$	自然数集
$\mathbb{Z}$	整数集
$\mathbb{R}$	实数集
$\mathbb{Z}_q$	商环，并且为 $(-q/2, q/2]\cap\mathbb{Z}$，其中 $q\in\mathbb{Z}$，且 $q\geq 2$
$\log(\cdot)$	对数，且底为 2
$\lceil\cdot\rceil$	向上取整
$[\![\cdot]\!]$	四舍五入
$\boldsymbol{a}$	向量，且为列向量形式
$\boldsymbol{a}^{\mathrm{T}}$	向量 $\boldsymbol{a}$ 的转置
$\boldsymbol{A}$	矩阵，$\boldsymbol{A}$ 亦可看作其列向量的有序集合 $\{\mathbf{a}_1, \mathbf{a}_2, \ldots\}$
$\boldsymbol{A}^{\mathrm{T}}$	矩阵 $\boldsymbol{A}$ 的转置
$\otimes$	张量积
$\|\boldsymbol{a}\|$	向量 $\boldsymbol{a}$ 的 Euclidean 范数，定义为 $\|\boldsymbol{a}\|=\left(\sum_i \|a_i\|^2\right)^{\frac{1}{2}}$，其中 a_i 是向量 $\boldsymbol{a}$ 的分量
$\|\boldsymbol{A}\|$	矩阵 $\boldsymbol{A}$ 的 Euclidean 范数，定义为 $\|\boldsymbol{A}\|=\max_j \|\boldsymbol{a}_j\|$，其中 $\boldsymbol{a}_j$ 是矩阵 $\boldsymbol{A}$ 的列向量
$\|\boldsymbol{a}\|_\infty$	向量 $\boldsymbol{a}$ 的 ∞ 范数，定义为 $\|\boldsymbol{a}\|_\infty=\max_i \|a_i\|$，其中 a_i 是向量 $\boldsymbol{a}$ 的分量
$\|\boldsymbol{A}\|_\infty$	矩阵 $\boldsymbol{A}$ 的 ∞ 范数，定义为 $\|\boldsymbol{A}\|_\infty=\max_{i,j} \|a_{i,j}\|$，其中 $a_{i,j}$ 是矩阵 $\boldsymbol{A}$ 的元素
$\tilde{\boldsymbol{T}}$	向量集合 $\boldsymbol{T}$ 的 Gram-Schmidt 正交化
O, o, Ω, ω	算法渐近符号
$\mathrm{poly}(n)$	$f(n)$，且对某一常数 c，使得 $f(n)=O(n^c)$
$\mathrm{negl}(n)$	$f(n)$，且对每一固定常数 c，都使得 $f(n)=o(n^{-c})$

2.2. 格

下面简单介绍一下格理论，详细内容可参阅[11]。

定义 1 设 $\boldsymbol{B}=\{\boldsymbol{b}_1,\cdots,\boldsymbol{b}_m\}\subset\mathbb{R}^n$ 是一组线性无关向量，格 Λ 定义为

$$\Lambda=\left\{\boldsymbol{x}\in\mathbb{R}^n:\exists\boldsymbol{c}\in\mathbb{Z}^m,\boldsymbol{x}=\boldsymbol{B}\boldsymbol{c}=\sum_{i=1}^m c_i\boldsymbol{b}_i\right\},$$

其中 $\boldsymbol{B}$ 称为 Λ 的一组基。这里，n 为 Λ 的维数，m 为 Λ 的秩，且 $m\le n$。在 $m=n$ 时，Λ 称为满秩格。

定义 2 对正整数 q、矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，定义 m 维满秩整数格：

$$\Lambda^{\perp}(\boldsymbol{A})=\left\{\boldsymbol{e}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{e}=\boldsymbol{0}\bmod q\right\}$$

$$\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})=\left\{\boldsymbol{e}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{e}=\boldsymbol{u}\bmod q\right\}.$$

可以看出，如果 $\boldsymbol{t}\in\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})$，则 $\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})=\Lambda^{\perp}(\boldsymbol{A})+\boldsymbol{t}$。即 $\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})$ 是 $\Lambda^{\perp}(\boldsymbol{A})$ 的陪集。

定义 3 对任意的向量 $\boldsymbol{c}\in\mathbb{R}^n$ 和实数 $\sigma>0$，$\mathbb{R}^n$ 上高斯函数定义为

$$\forall\boldsymbol{x}\in\mathbb{R}^n,\ \rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/\sigma^2\right),$$

它以 $\boldsymbol{c}$ 为中心，以 σ 为参数。

对任意的向量 $\boldsymbol{c}\in\mathbb{R}^n$、实数 $\sigma>0$ 以及 n 维格 Λ，Λ 上的离散高斯分布定义为

$$\forall\boldsymbol{x}\in\Lambda,\ D_{\Lambda,\sigma,\boldsymbol{c}}=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\sum_{\boldsymbol{x}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}.$$

当下标 σ 和 $\boldsymbol{c}$ 的值分别为 1 和 $\boldsymbol{0}$ 时，可省去不写。

2.3. 格上的算法

引理 1 ([12]) 令 $\delta>0$ 为任意固定常数。存在概率多项式时间算法 $\mathrm{TrapGen}(n,q)$，它输入正整数 n、$q\ge2$ 和 $m\ge(5+3\delta)\cdot n\log q$，输出 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}\in\mathbb{Z}^{m\times m}$，并满足以下条件：① $\boldsymbol{A}$ 的分布统计接近 $\mathbb{Z}_q^{n\times m}$ 上的均匀分布，② $\boldsymbol{T}$ 为 $\Lambda^{\perp}(\boldsymbol{A})$ 的一组基，③ $\|\tilde{\boldsymbol{T}}\|\le O\left(\sqrt{n\log q}\right)$。

引理 2 ([13]) 存在概率多项式时间算法 $\mathrm{SamplePre}(\boldsymbol{A},\boldsymbol{T}_A,\boldsymbol{u},\sigma)$，它输入矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$、$\Lambda^{\perp}(\boldsymbol{A})$ 的一组基 $\boldsymbol{T}_A$、向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$ 和参数 $\sigma\ge\|\tilde{\boldsymbol{T}}_A\|\cdot\omega\left(\sqrt{\log m}\right)$，其中 $q\ge2$，$m>n$，输出向量 $\boldsymbol{e}\in\mathbb{Z}^m$，并且 $\boldsymbol{e}$ 的分布统计接近分布 $D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}),\sigma}$。

引理 3 ([13]) 令 n 和 q 为正整数，且 q 为素数，令 $m\ge2n\log q$。则对几乎所有的 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 以及任意的 $\sigma\ge\omega\left(\sqrt{\log m}\right)$，$\boldsymbol{u}=\boldsymbol{A}\cdot\boldsymbol{e}\bmod q$ 的分布统计接近 $\mathbb{Z}_q^n$ 上的均匀分布，其中 $\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,\sigma}$。

引理 4 ([14]) 对任意 n 维格 Λ、向量 $\boldsymbol{c}\in\mathbb{R}^n$ 以及实数 $0<\varepsilon<1$ 和 $\sigma\ge\eta_{\varepsilon}(\Lambda)$，有

$$\Pr_{\boldsymbol{x}\leftarrow D_{\Lambda,\sigma,\boldsymbol{c}}}\left[\|\boldsymbol{x}-\boldsymbol{c}\|>\sigma\sqrt{n}\right]\le\frac{1+\varepsilon}{1-\varepsilon}\cdot2^{-n},$$

其中 $\eta_{\varepsilon}(\Lambda)$ 是光滑参数。对 Λ 的任意一组基 $\boldsymbol{B}$，有 $\eta_{\varepsilon}(\Lambda)\le\|\tilde{\boldsymbol{B}}\|\cdot\omega\left(\sqrt{\log n}\right)$。

2.4. 困难问题

定义 4 令 λ 为安全参数，令 $n=n(\lambda)$ 和 $q=q(\lambda)$ 为整数，令 $\chi=\chi(\lambda)$ 为 $\mathbb{Z}$ 上的概率分布。$\mathrm{LWE}_{n,q,\chi}$ 问题可叙述为：对任意 $m=\mathrm{poly}(n)$，令 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$，$\boldsymbol{s}\leftarrow\mathbb{Z}_q^n$，$\boldsymbol{e}\leftarrow\chi^m$，$\boldsymbol{u}\leftarrow\mathbb{Z}_q^m$，$\left(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{s}+\boldsymbol{e}\right)$ 和 $(\boldsymbol{A},\boldsymbol{u})$ 是计算不可区分的。

定义 5 对整数上的分布系集$\{\chi_n\}_{n\in\mathbb{N}}$，如果$\Pr_{e\leftarrow\chi_n}\left[|e|>B\right]=\mathrm{negl}(n)$，则称分布系集$\{\chi_n\}_{n\in\mathbb{N}}$是$B$有界的。

引理 5 ([3] [15]) 对任意$\varepsilon>0$，存在$q=q(n)\le 2^n$、$\chi=\chi(n)$和$B=B(n)$，且χ是B有界的，$q/B\ge 2^{n^\varepsilon}$，使得$\mathrm{LWE}_{n,q,\chi}$至少和GapSVP_γ的经典困难性以及SIVP_γ的量子困难性一样困难，其中$\gamma=2^{\Omega\left(n^\varepsilon\right)}$。

定义 6 对整数q和p，且$q\ge p\ge 2$，取整函数$[\![\cdot]\!]_p$定义为$[\![\cdot]\!]_p:\mathbb{Z}_q\to\mathbb{Z}_p:x\mapsto\left[\!\left[\frac{p}{q}\cdot x\right]\!\right]$。通过逐项处理，可把$[\![\cdot]\!]_p$扩展到$\mathbb{Z}_q$上的向量或矩阵。

定义 7 令λ为安全参数，令$n=n(\lambda)$、$q=q(\lambda)$和$p=p(\lambda)$为整数，且$q\ge p\ge 2$，$\mathrm{LWR}_{n,q,p}$问题可叙述为：对任意$m=\mathrm{poly}(n)$，令$\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$，$\boldsymbol{s}\leftarrow\mathbb{Z}_q^n$，$\boldsymbol{u}\leftarrow\mathbb{Z}_p^m$，$\left(\boldsymbol{A},[\![\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{s}]\!]_p\right)$和$(\boldsymbol{A},\boldsymbol{u})$是计算不可区分的。

引理 6 ([8]) 令χ是$\mathbb{Z}$上可有效抽样的B有界分布，令$q\ge p\cdot B\cdot n^{\omega(1)}$，则求解任一分布上$\mathbf{s}\in\mathbb{Z}_q^n$的$\mathrm{LWR}_{n,q,p}$问题，至少与求解同一分布上$\mathbf{s}\in\mathbb{Z}_q^n$的$\mathrm{LWE}_{n,q,\chi}$问题的一样困难。

3. CLFHE 的定义及安全模型

3.1. 定义

CLFHE 由系统参数生成 Setup、部分私钥抽取 Extract、公私钥生成 KeyGen、加密 Encrypt、解密 Decrypt 和密文计算 Eval 六个多项式时间算法组成。其中 Setup 和 Extract 算法由密钥生成中心(Key Generation Center, KGC)执行。

$\mathrm{Setup}\left(1^\lambda,1^L\right)$：输入安全参数$\lambda$和电路深度$L$，输出系统主公钥$mpk$和主私钥$msk$。

$\mathrm{Extract}\left(mpk,msk,id\right)$：输入主公钥$mpk$、主私钥$msk$和身份$id\in\{0,1\}^*$，输出身份$id$的部分私钥$d_{id}$。

$\mathrm{KeyGen}\left(mpk,id,d_{id}\right)$：输入主公钥$mpk$、身份$id$和部分私钥$d_{id}$，输出用户的公钥$pk_{id}$和私钥$sk_{id}$。

$\mathrm{Encrypt}\left(mpk,id,pk_{id},\mu\right)$：输入主公钥$mpk$、接收方身份$id$、接收方公钥$pk_{id}$以及消息$\mu\in\mathcal{M}$，这里$\mathcal{M}$为消息空间，输出密文$c\in\mathcal{C}$或错误标识$\perp$，这里$\mathcal{C}$为密文空间。

$\mathrm{Decrypt}\left(mpk,sk_{id},c\right)$：输入主公钥$mpk$、接收方私钥$sk_{id}$以及密文$c\in\mathcal{C}$，输出消息$\mu\in\mathcal{M}$或错误标识$\perp$。

$\mathrm{Eval}\left(mpk,id,f,c_1,\cdots,c_\ell\right)$：输入主公钥$mpk$、身份$id$、电路$f:\mathcal{M}^\ell\to\mathcal{M}$和身份$id$下的一组密文$\{c_1,\cdots,c_\ell\}$，输出密文$c_f\in\mathcal{C}$。

CLFHE 应满足正确性约束。即

假定$\left(mpk,msk\right)\leftarrow\mathrm{Setup}\left(1^\lambda,1^L\right)$，$d_{id}\leftarrow\mathrm{Extract}\left(mpk,msk,id\right)$，$\left(pk_{id},sk_{id}\right)\leftarrow\mathrm{KeyGen}\left(mpk,id,d_{id}\right)$，则对全部$c_f\leftarrow\mathrm{Eval}\left(mpk,id,f,c_1,\cdots,c_\ell\right)$，其中$f:\mathcal{M}^\ell\to\mathcal{M}$，$\left\{c_i\leftarrow\mathrm{Encrypt}\left(mpk,id,pk_{id},\mu_i\right)\right\}_{i\in\{1,\cdots,\ell\}}$，都有$\mathrm{Decrypt}\left(mpk,sk_{id},c_f\right)=f\left(\mu_1,\cdots,\mu_\ell\right)$。

3.2. 安全模型

我们这里给出INDr-CPA的安全定义。INDr-CPA比IND-CPA的安全性更强。INDr-CPA包括IND-CPA安全性和接收方匿名性。CLFHE 的攻击者分为两类，即第 1 类攻击者$\mathcal{A}_\mathrm{I}$和第 2 类攻击者$\mathcal{A}_\mathrm{II}$。$\mathcal{A}_\mathrm{I}$模拟外部攻击者，允许它替换用户的公钥。$\mathcal{A}_\mathrm{II}$模拟诚实但好奇的 KGC，不允许它替换用户的公钥。

攻击者$\mathcal{A}_\mathrm{I}$的 INDr-CPA 安全游戏如下：

初始化：挑战者产生$\left(mpk,msk\right)\leftarrow\mathrm{Setup}\left(1^\lambda,1^L\right)$。并把主公钥$mpk$发送给$\mathcal{A}_\mathrm{I}$。

阶段 1：$\mathcal{A}_\mathrm{I}$可查询公钥询问(request public key)、公钥替换(replace public key)和部分私钥抽取(extract

partial private key)预言机。

公钥询问预言机：输入身份 id，它利用 KeyGen 和 Extract 产生公钥 pk_{id}，并返回 pk_{id}。同时它把身份 id 和它的 pk_{id} 记载下来。

公钥替换预言机：输入身份 id 和公钥 pk'_{id}，它修改身份 id 的有关记载，这以后 id 关联的公钥为 pk'_{id}。

部分私钥抽取预言机：输入身份 id，它产生部分私钥 $d_{id} \leftarrow \text{Extract}(mpk, msk, id)$，并返回 d_{id}。

$\mathcal{A}_{\text{I}}$ 结束查询输出目标身份 id^* 和消息 μ。

挑战：挑战者随机选择 $b \leftarrow \{0,1\}$ 和密文 $c \leftarrow \mathcal{C}$。若 $b=0$，设置挑战密文 $c^* = \text{Encrypt}(mpk, id^*, pk'_{id^*}, \mu)$，其中 pk'_{id^*} 是 id^* 当前关联的公钥；若 $b=1$，设置挑战密文 $c^* = c$。挑战者把 c^* 发送给 $\mathcal{A}_{\text{I}}$。

阶段 2：$\mathcal{A}_{\text{I}}$ 继续查询公钥询问、公钥替换和部分私钥抽取预言机。在结束查询时 $\mathcal{A}_{\text{I}}$ 输出猜测 $b' \in \{0,1\}$。

如果 $b=b'$，并且 $\mathcal{A}_{\text{I}}$ 在阶段 1 没有替换 id^* 的公钥或在两个查询阶段都没有询问 id^* 的部分私钥，则 $\mathcal{A}_{\text{I}}$ 赢得游戏。

$\mathcal{A}_{\text{I}}$ 的优势定义为 $\text{Adv}_{\mathcal{A}_{\text{I}}}(\lambda) = \left|\Pr[b=b'] - \frac{1}{2}\right|$。如果 $\text{Adv}_{\mathcal{A}_{\text{I}}}(\lambda)$ 是可忽略的，则称这个 CLFHE 方案在 $\mathcal{A}_{\text{I}}$ 攻击下是 INDr-CPA 安全的。

攻击者 $\mathcal{A}_{\text{II}}$ 的 INDr-CPA 安全游戏如下：

初始化：挑战者产生 $(mpk, msk) \leftarrow \text{Setup}(1^{\lambda}, 1^{L})$。并把主公钥 mpk 和主私钥 msk 发送给 $\mathcal{A}_{\text{II}}$。

阶段 1：$\mathcal{A}_{\text{II}}$ 可查询公钥询问(request public key)预言机。

公钥询问预言机：输入身份 id 和部分私钥 d_{id}，它计算公钥 $(pk_{id}, sk_{id}) \leftarrow \text{KeyGen}(mpk, id, d_{id})$，并返回 pk_{id}。

$\mathcal{A}_{\text{II}}$ 结束查询输出目标身份 id^* 和消息 μ。

挑战：挑战者随机选择 $b \leftarrow \{0,1\}$ 和密文 $c \leftarrow \mathcal{C}$。若 $b=0$，设置挑战密文 $c^* = \text{Encrypt}(mpk, id^*, pk_{id^*}, \mu)$，其中 pk_{id^*} 是 id^* 关联的公钥；若 $b=1$，设置挑战密文 $c^* = c$。

阶段 2：$\mathcal{A}_{\text{II}}$ 继续查询公钥询问预言机。在结束查询时 $\mathcal{A}_{\text{II}}$ 输出猜测 $b' \in \{0,1\}$。

如果 $b=b'$，则 $\mathcal{A}_{\text{II}}$ 赢得游戏。

$\mathcal{A}_{\text{II}}$ 的优势定义为 $\text{Adv}_{\mathcal{A}_{\text{II}}}(\lambda) = \left|\Pr[b=b'] - \frac{1}{2}\right|$。如果 $\text{Adv}_{\mathcal{A}_{\text{II}}}(\lambda)$ 是可忽略的，则称这个 CLFHE 方案在 $\mathcal{A}_{\text{II}}$ 攻击下是 INDr-CPA 安全的。

4. 基于 LWR 问题 CLFHE

4.1. 方案描述

我们令向量 $\boldsymbol{g} = \left(1, \cdots, 2^{\lceil \log p \rceil - 1}\right)^{\text{T}} \in \mathbb{Z}_p^{\lceil \log p \rceil}$。令矩阵 $\boldsymbol{G} = \boldsymbol{I}_{2m+1} \otimes \boldsymbol{g}^{\text{T}} \in \mathbb{Z}_p^{(2m+1)\times N}$，其中 $N = (2m+1)\cdot\lceil \log p \rceil$。定义反函数 $\boldsymbol{G}^{-1}: \mathbb{Z}_p^{(2m+1)\times N} \to \{0,1\}^{N\times N}$，它把输入矩阵的每个元素 $a \in \mathbb{Z}_p$ 扩展为比特向量 $\left(a_0, \cdots, a_{\lceil \log p \rceil - 1}\right)^{\text{T}} \in \{0,1\}^{\lceil \log p \rceil}$，且满足 $a = \sum_{i=0}^{\lceil \log p \rceil - 1} 2^i \cdot a_i$。对任意矩阵 $\boldsymbol{C} \in \mathbb{Z}_p^{(2m+1)\times N}$，有 $\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{C}) = \boldsymbol{C}$。

下面给出基于 LWR 问题的 CLFHE 方案，它的消息空间为 $\mathcal{M} = \{0,1\}$，密文空间为 $\mathcal{C} = \mathbb{Z}_p^{(2m+1)\times N}$。

$\text{Setup}(1^{\lambda}, 1^{L})$：KGC 设置参数 $n = n(\lambda, L)$、$q = q(\lambda, L)$、$p = p(\lambda, L)$、$m = m(\lambda, L)$、$\sigma_1 = \sigma_1(\lambda, L)$ 和 $\sigma_2 = \sigma_2(\lambda, L)$。这些参数具体见 4.3 节。调用 $\text{TrapGen}(n, q)$ 产生矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ 和 $\Lambda^{\perp}(\boldsymbol{A})$ 的一组基 $\boldsymbol{T}_A \in \mathbb{Z}^{m\times m}$，且 $\left\|\tilde{\boldsymbol{T}}_A\right\| \le O\left(\sqrt{n \log q}\right)$。随机选择矩阵 $\overline{\boldsymbol{A}} \leftarrow \mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{B} \leftarrow \mathbb{Z}_q^{n\times m}$。选择哈希函数 $H: \{0,1\}^{*} \to \mathbb{Z}_q^{n}$。输出主公钥 $mpk = \left(n, q, p, m, \sigma_1, \sigma_2, \boldsymbol{A}, \overline{\boldsymbol{A}}, \boldsymbol{B}, H\right)$ 和主私钥 $msk = \boldsymbol{T}_A$。

$\text{Extract}(mpk, msk, id)$：对身份 $id \in \{0,1\}^{*}$，KGC 计算 $\boldsymbol{u} = H(id) \in \mathbb{Z}_q^{n}$。调用 $\text{SamplePre}(\boldsymbol{A}, \boldsymbol{T}_A, \boldsymbol{u}, \sigma_1)$ 产

生向量 $\boldsymbol{d}\in\mathbb{Z}^m$。输出部分私钥 $d_{id}=\boldsymbol{d}$。这里有 $\boldsymbol{A}\cdot\boldsymbol{d}=\boldsymbol{u}\bmod q$。

KeyGen$\left(mpk,id,d_{id}\right)$：用户选择 $\boldsymbol{x}\leftarrow D_{\mathbb{Z}^m,\sigma_2}$，令 $\boldsymbol{v}=\boldsymbol{B}\cdot\boldsymbol{x}\bmod q$。此外令 $\overline{\boldsymbol{u}}=\overline{\boldsymbol{A}}\cdot\boldsymbol{d}\bmod q$。令 $\boldsymbol{r}=\begin{pmatrix}-\boldsymbol{d}\\-\boldsymbol{x}\\1\end{pmatrix}\in\mathbb{Z}^{2m+1}$。输出公钥 $pk_{id}=\left(\boldsymbol{v},\overline{\boldsymbol{u}}\right)$ 和私钥 $sk_{id}=\boldsymbol{r}$。

Encrypt$\left(mpk,id,pk_{id},\mu\right)$：对消息 $\mu\in\{0,1\}$，计算 $\boldsymbol{u}=H\left(id\right)\in\mathbb{Z}_q^n$。随机选择矩阵 $\boldsymbol{S}_1\leftarrow\mathbb{Z}_q^{n\times N}$、$\overline{\boldsymbol{S}}\leftarrow\mathbb{Z}_q^{n\times N}$ 和 $\boldsymbol{S}_2\leftarrow\mathbb{Z}_q^{n\times N}$，输出密文

$$\boldsymbol{C}=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{A}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p\\\left[\!\left[\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\\\left[\!\left[\boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{u}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p+\left[\!\left[\boldsymbol{v}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

Decrypt$\left(mpk,sk_{id},c\right)$：给定密文 $\boldsymbol{C}\in\mathbb{Z}_p^{(2m+1)\times N}$，已知 $sk_{id}=\boldsymbol{r}$。输出消息 $\mu'=\left[\!\left[\dfrac{\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{c}}{2^{\lceil\log p\rceil-2}}\right]\!\right]$，其中 $\boldsymbol{c}$ 为密文 $\boldsymbol{C}$ 的倒数第 2 列。

给定同一身份 id 下的两个密文 $\boldsymbol{C}_1\in\mathbb{Z}_p^{(2m+1)\times N}$ 和 $\boldsymbol{C}_2\in\mathbb{Z}_p^{(2m+1)\times N}$，密文同态加法和乘法如下：

Add$\left(\boldsymbol{C}_1,\boldsymbol{C}_2\right)$：输出 $\boldsymbol{C}_{\text{add}}=\boldsymbol{C}_1+\boldsymbol{C}_2\in\mathbb{Z}_p^{(2m+1)\times N}$。

Mult$\left(\boldsymbol{C}_1,\boldsymbol{C}_2\right)$：输出 $\boldsymbol{C}_{\text{mult}}=\boldsymbol{C}_1\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)\in\mathbb{Z}_p^{(2m+1)\times N}$。

4.2. 方案分析

4.2.1. 正确性

对于 Encrypt 输出的密文 $\boldsymbol{C}\in\mathbb{Z}_p^{(2m+1)\times N}$，有

$$\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{C}=\begin{pmatrix}-\boldsymbol{d}\\-\boldsymbol{x}\\1\end{pmatrix}^{\mathrm{T}}\cdot\begin{pmatrix}\left[\!\left[\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{A}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p\\\left[\!\left[\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\\\left[\!\left[\boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{u}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p+\left[\!\left[\boldsymbol{v}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\end{pmatrix}+\mu\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}$$

$$=\left[\!\left[\boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{u}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p+\left[\!\left[\boldsymbol{v}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p-\boldsymbol{d}^{\mathrm{T}}\cdot\left(\left[\!\left[\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{A}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p\right)-\boldsymbol{x}^{\mathrm{T}}\cdot\left[\!\left[\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p+\mu\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}$$

$$=\left(\left[\!\left[\boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p-\boldsymbol{d}^{\mathrm{T}}\cdot\left[\!\left[\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p\right)+\left(\left[\!\left[\overline{\boldsymbol{u}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p-\boldsymbol{d}^{\mathrm{T}}\cdot\left[\!\left[\overline{\boldsymbol{A}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p\right)+\left(\left[\!\left[\boldsymbol{v}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p-\boldsymbol{x}^{\mathrm{T}}\cdot\left[\!\left[\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\right)+\mu\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}$$

$$=\frac{p}{q}\left(\boldsymbol{u}^{\mathrm{T}}-\boldsymbol{d}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}\right)\boldsymbol{S}_1+\boldsymbol{e}_1^{\mathrm{T}}-\boldsymbol{d}^{\mathrm{T}}\boldsymbol{E}_1+\frac{p}{q}\left(\overline{\boldsymbol{u}}^{\mathrm{T}}-\boldsymbol{d}^{\mathrm{T}}\overline{\boldsymbol{A}}^{\mathrm{T}}\right)\overline{\boldsymbol{S}}+\overline{\boldsymbol{e}}^{\mathrm{T}}-\boldsymbol{d}^{\mathrm{T}}\overline{\boldsymbol{E}}+\frac{p}{q}\left(\boldsymbol{v}^{\mathrm{T}}-\boldsymbol{x}^{\mathrm{T}}\boldsymbol{B}^{\mathrm{T}}\right)\boldsymbol{S}_2+\boldsymbol{e}_2^{\mathrm{T}}-\boldsymbol{x}^{\mathrm{T}}\boldsymbol{E}_2+\mu\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}$$

$$=\boldsymbol{e}_1^{\mathrm{T}}+\overline{\boldsymbol{e}}^{\mathrm{T}}+\boldsymbol{e}_2^{\mathrm{T}}-\left(\boldsymbol{d}^{\mathrm{T}}\boldsymbol{E}_1+\boldsymbol{d}^{\mathrm{T}}\overline{\boldsymbol{E}}+\boldsymbol{x}^{\mathrm{T}}\boldsymbol{E}_2\right)+\mu\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}$$

其中

$$\boldsymbol{e}_1^{\mathrm{T}}=\left[\!\left[\boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p-\frac{p}{q}\cdot\boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_1\in\left[-\frac{1}{2},\frac{1}{2}\right]^{1\times N}$$

$$\boldsymbol{E}_1=\left[\!\left[\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p-\frac{p}{q}\cdot\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\in\left[-\frac{1}{2},\frac{1}{2}\right]^{m\times N}$$

$$\overline{\boldsymbol{e}}^{\mathrm{T}}=\left[\!\left[\overline{\boldsymbol{u}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p-\frac{p}{q}\cdot\overline{\boldsymbol{u}}^{\mathrm{T}}\cdot\overline{\boldsymbol{S}}\in\left[-\frac{1}{2},\frac{1}{2}\right]^{1\times N}$$

$$\bar{\boldsymbol{E}}=\left[\!\left[\bar{\boldsymbol{A}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p-\frac{p}{q}\cdot\bar{\boldsymbol{A}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\in\left[-\frac{1}{2},\frac{1}{2}\right]^{m\times N}$$

$$\boldsymbol{e}_2^{\mathrm{T}}=\left[\!\left[\boldsymbol{v}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p-\frac{p}{q}\cdot\boldsymbol{v}^{\mathrm{T}}\cdot\boldsymbol{S}_2\in\left[-\frac{1}{2},\frac{1}{2}\right]^{1\times N}$$

$$\boldsymbol{E}_2=\left[\!\left[\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p-\frac{p}{q}\cdot\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_2\in\left[-\frac{1}{2},\frac{1}{2}\right]^{m\times N}.$$

令 $\boldsymbol{w}^{\mathrm{T}}=\boldsymbol{e}_1^{\mathrm{T}}+\bar{\boldsymbol{e}}^{\mathrm{T}}+\boldsymbol{e}_2^{\mathrm{T}}-\left(\boldsymbol{d}^{\mathrm{T}}\boldsymbol{E}_1+\boldsymbol{d}^{\mathrm{T}}\bar{\boldsymbol{E}}+\boldsymbol{x}^{\mathrm{T}}\boldsymbol{E}_2\right)$，则 $\boldsymbol{C}$ 的误差

$$\begin{aligned}\left\|\boldsymbol{w}^{\mathrm{T}}\right\|_\infty&=\left\|\boldsymbol{e}_1^{\mathrm{T}}+\bar{\boldsymbol{e}}^{\mathrm{T}}+\boldsymbol{e}_2^{\mathrm{T}}-\left(\boldsymbol{d}^{\mathrm{T}}\boldsymbol{E}_1+\boldsymbol{d}^{\mathrm{T}}\bar{\boldsymbol{E}}+\boldsymbol{x}^{\mathrm{T}}\boldsymbol{E}_2\right)\right\|_\infty\\&\le\left\|\boldsymbol{e}_1^{\mathrm{T}}+\bar{\boldsymbol{e}}^{\mathrm{T}}+\boldsymbol{e}_2^{\mathrm{T}}\right\|_\infty+\left\|\boldsymbol{d}^{\mathrm{T}}\boldsymbol{E}_1+\boldsymbol{d}^{\mathrm{T}}\bar{\boldsymbol{E}}+\boldsymbol{x}^{\mathrm{T}}\boldsymbol{E}_2\right\|_\infty\\&\le\frac{3}{2}+m\cdot\left\|\boldsymbol{d}\right\|_\infty\cdot\left\|\boldsymbol{E}_1\right\|_\infty+m\cdot\left\|\boldsymbol{d}\right\|_\infty\cdot\left\|\bar{\boldsymbol{E}}\right\|_\infty+m\cdot\left\|\boldsymbol{x}\right\|_\infty\cdot\left\|\boldsymbol{E}_2\right\|_\infty\\&\le\frac{3}{2}+m\cdot\left\|\boldsymbol{d}\right\|_\infty+\frac{1}{2}\cdot m\cdot\left\|\boldsymbol{x}\right\|_\infty\\&\le\frac{3}{2}+m\cdot\left\|\boldsymbol{d}\right\|+\frac{1}{2}\cdot m\cdot\left\|\boldsymbol{x}\right\|\\&\le\frac{3}{2}+m\sqrt{m}\cdot\left(\sigma_1+\frac{1}{2}\cdot\sigma_2\right)\end{aligned}$$

其中 $\left\|\boldsymbol{d}\right\|\le\sigma_1\cdot\sqrt{m}$，$\left\|\boldsymbol{x}\right\|\le\sigma_2\cdot\sqrt{m}$。我们记 $\left\|\boldsymbol{w}^{\mathrm{T}}\right\|_\infty\le\Delta=\frac{3}{2}+m\sqrt{m}\cdot\left(\sigma_1+\frac{1}{2}\cdot\sigma_2\right)$。

对 $\mathrm{Add}\left(\boldsymbol{C}_1,\boldsymbol{C}_2\right)$ 输出的密文 $\boldsymbol{C}_{\mathrm{add}}$，有

$$\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{C}_{\mathrm{add}}=\boldsymbol{r}^{\mathrm{T}}\cdot\left(\boldsymbol{C}_1+\boldsymbol{C}_2\right)=\boldsymbol{w}_1^{\mathrm{T}}+\boldsymbol{w}_2^{\mathrm{T}}+\left(\mu_1+\mu_2\right)\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}.$$

令 $\boldsymbol{w}_{\mathrm{add}}^{\mathrm{T}}=\boldsymbol{w}_1^{\mathrm{T}}+\boldsymbol{w}_2^{\mathrm{T}}$，则 $\boldsymbol{C}_{\mathrm{add}}$ 的误差 $\left\|\boldsymbol{w}_{\mathrm{add}}^{\mathrm{T}}\right\|_\infty=\left\|\boldsymbol{w}_1^{\mathrm{T}}+\boldsymbol{w}_2^{\mathrm{T}}\right\|_\infty\le\left\|\boldsymbol{w}_1^{\mathrm{T}}\right\|_\infty+\left\|\boldsymbol{w}_2^{\mathrm{T}}\right\|_\infty\le2\Delta$。

对 $\mathrm{Mult}\left(\boldsymbol{C}_1,\boldsymbol{C}_2\right)$ 输出的密文 $\boldsymbol{C}_{\mathrm{mult}}$，有

$$\begin{aligned}\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{C}_{\mathrm{mult}}&=\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{C}_1\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)\\&=\left(\boldsymbol{w}_1^{\mathrm{T}}+\mu_1\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}\right)\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)\\&=\boldsymbol{w}_1^{\mathrm{T}}\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)+\mu_1\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)\\&=\boldsymbol{w}_1^{\mathrm{T}}\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)+\mu_1\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{C}_2\\&=\boldsymbol{w}_1^{\mathrm{T}}\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)+\mu_1\cdot\left(\boldsymbol{w}_2^{\mathrm{T}}+\mu_2\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}\right)\\&=\boldsymbol{w}_1^{\mathrm{T}}\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)+\mu_1\cdot\boldsymbol{w}_2^{\mathrm{T}}+\mu_1\mu_2\cdot\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{G}\end{aligned}$$

令 $\boldsymbol{w}_{\mathrm{mult}}=\boldsymbol{w}_1^{\mathrm{T}}\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)+\mu_1\cdot\boldsymbol{w}_2^{\mathrm{T}}$，则 $\boldsymbol{C}_{\mathrm{mult}}$ 的误差

$$\begin{aligned}\left\|\boldsymbol{w}_{\mathrm{mult}}\right\|_\infty&=\left\|\boldsymbol{w}_1^{\mathrm{T}}\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)+\mu_1\cdot\boldsymbol{w}_2^{\mathrm{T}}\right\|_\infty\\&\le\left\|\boldsymbol{w}_1^{\mathrm{T}}\cdot\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)\right\|_\infty+\left\|\mu_1\cdot\boldsymbol{w}_2^{\mathrm{T}}\right\|_\infty\\&\le N\cdot\left\|\boldsymbol{w}_1\right\|_\infty\cdot\left\|\boldsymbol{G}^{-1}\left(\boldsymbol{C}_2\right)\right\|_\infty+\Delta\\&\le N\Delta+\Delta=\left(N+1\right)\Delta\end{aligned}$$

通过迭代调用 $\mathrm{Add}(\boldsymbol{C}_1,\boldsymbol{C}_2)$ 和 $\mathrm{Mult}(\boldsymbol{C}_1,\boldsymbol{C}_2)$，密文计算 $\mathrm{Eval}(f,\boldsymbol{C}_1,\cdots,\boldsymbol{C}_\ell)$ 可输出密文 $\boldsymbol{C}_f\in\mathbb{Z}_p^{(2m+1)\times N}$。因为 $f:\mathcal{M}^\ell\to\mathcal{M}$ 的电路深度 $\mathrm{depth}(f)\le L$。又知道有 $\|\boldsymbol{w}_{\mathrm{add}}^{\mathrm{T}}\|_\infty\le 2\Delta$，$\|\boldsymbol{w}_{\mathrm{mult}}\|_\infty\le(N+1)\Delta$，即 $\|\boldsymbol{w}_{\mathrm{add}}^{\mathrm{T}}\|_\infty\ll\|\boldsymbol{w}_{\mathrm{mult}}\|_\infty$。故 $\boldsymbol{C}_f\in\mathbb{Z}_p^{(2m+1)\times N}$ 的误差 $\|\boldsymbol{w}_f\|_\infty\le(N+1)^L\Delta$。于是对 $\boldsymbol{C}_f\in\mathbb{Z}_p^{(2m+1)\times N}$ 的倒数第 2 列 $\boldsymbol{c}_f\in\mathbb{Z}_p^{2m+1}$，有 $\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{c}_f\le\|\boldsymbol{w}_f^{\mathrm{T}}\|_\infty+\mu_f\cdot 2^{\lceil\log p\rceil-2}$。因为 $2^{\lceil\log p\rceil-2}\in[p/4,p/2)$，故如果 $\|\boldsymbol{w}_f^{\mathrm{T}}\|_\infty\le(N+1)^L\Delta<p/8$，$\mathrm{Eval}(f,\boldsymbol{C}_1,\cdots,\boldsymbol{C}_\ell)$ 输出的密文 $\boldsymbol{C}_f\in\mathbb{Z}_p^{(2m+1)\times N}$ 可正确解密得到消息 $\mu_f=f(\mu_1,\cdots,\mu_\ell)$。

4.2.2. 安全性

所提出的 CLFHE 在 $\mathcal{A}_{\mathrm{I}}$ 攻击下是 INDr-CPA 安全的。即：

定理 1 令哈希函数 H 为随机预言机。若攻击者 $\mathcal{A}_{\mathrm{I}}$ 在 INDr-CPA 安全游戏中以优势 $\mathrm{Adv}_{\mathcal{A}_{\mathrm{I}}}(\lambda)$ 攻破所提出的 CLFHE 方案，且 H 预言、公钥询问次数为 q_{H}、q_{rpk}。则存在以优势 $\mathrm{Adv}_{\mathcal{B}}(\lambda)$ 解决 $\mathrm{LWR}_{n,q,p}$ 问题的算法 $\mathcal{B}$。其中

$$\mathrm{Adv}_{\mathcal{A}_{\mathrm{I}}}(\lambda)\le 2(q_{\mathrm{rpk}}+q_{\mathrm{H}})\cdot\mathrm{Adv}_{\mathcal{B}}(\lambda).$$

证明：我们基于游戏序列进行证明。并定义 Y_i 为攻击者 $\mathcal{A}_{\mathrm{I}}$ 在 Game i 中赢得游戏这一事件。

Game 0 它是攻击所提出的方案的 $\mathcal{A}_{\mathrm{I}}$ 和挑战者之间的原始 INDr-CPA 游戏。在这个游戏中，$\mathcal{A}_{\mathrm{I}}$ 的优势 $\mathrm{Adv}_{\mathcal{A}_{\mathrm{I}}}^{\mathrm{CLFHE}}(\lambda)=\left|\Pr[Y_0]-\frac{1}{2}\right|$。

Game 1 这个游戏相比 Game 0 的变化是以下四个方面：

① 始化：挑战者随机选择 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$。

② H 预言机：当 $\mathcal{A}_{\mathrm{I}}$ 询问身份 id 的 H 预言时，挑战者选择 $\boldsymbol{d}\leftarrow D_{\mathbb{Z}^m,\sigma_1}$，令 $\boldsymbol{u}=\boldsymbol{A}\cdot\boldsymbol{d}\bmod q$ 和 $\bar{\boldsymbol{u}}=\bar{\boldsymbol{A}}\cdot\boldsymbol{d}\bmod q$，把元组 $(id,\boldsymbol{u},\bar{\boldsymbol{u}},\boldsymbol{d})$ 存储起来，并返回 $\boldsymbol{u}$ 给 $\mathcal{A}_{\mathrm{I}}$。

③ 公钥询问预言机：当 $\mathcal{A}_{\mathrm{I}}$ 询问身份 id 的公钥时，挑战者选择 $\boldsymbol{x}\leftarrow D_{\mathbb{Z}^m,\sigma_2}$，令 $\boldsymbol{v}=\boldsymbol{B}\cdot\boldsymbol{x}\bmod q$。从 H 记载里找到元组 $(id,\boldsymbol{u},\bar{\boldsymbol{u}},\boldsymbol{d})$。令公钥 $pk_{id}=(\boldsymbol{v},\bar{\boldsymbol{u}})$，把元组 $(id,pk_{id},*)$ 存储起来，并返回 pk_{id} 给 $\mathcal{A}_{\mathrm{I}}$。其中 $*$ 表示该元素空缺，它用于存储替换公钥 pk'_{id}。

④ 部分私钥抽取预言机：当 $\mathcal{A}_{\mathrm{I}}$ 询问身份 id 的部分私钥时，挑战者从 H 记载里找到元组 $(id,\boldsymbol{u},\bar{\boldsymbol{u}},\boldsymbol{d})$，把 $\boldsymbol{d}$ 返回给 $\mathcal{A}_{\mathrm{I}}$。

由引理 3 等可知，Game 0 和 Game 1 是统计不可区分的。故 $\left|\Pr[Y_0]-\Pr[Y_1]\right|=\mathrm{negl}(\lambda)$。

Game 2 这个游戏相比 Game 1 调整了以下两个地方：

① 始化：挑战者随机产生猜测 $\eta\leftarrow\{0,1\}$。$\eta=0$ 表示 $\mathcal{A}_{\mathrm{I}}$ 会询问目标身份的部分私钥，$\eta=1$ 表示 $\mathcal{A}_{\mathrm{I}}$ 不会询问目标身份的部分私钥。

② 获胜条件：令 Extract 表示 $\mathcal{A}_{\mathrm{I}}$ 询问了目标身份的部分私钥。则

如果 $\eta=0$，并且 Extract 发生了，则在 $b=b'$ 时 $\mathcal{A}_{\mathrm{I}}$ 获胜；

如果 $\eta=1$，并且 Extract 发生了，则 $\mathcal{A}_{\mathrm{I}}$ 以概率 $\frac{1}{2}$ 获胜；

如果 $\eta=0$，并且 Extract 没有发生，则 $\mathcal{A}_{\mathrm{I}}$ 以概率 $\frac{1}{2}$ 获胜；

如果 $\eta=1$，并且 Extract 没有发生，则在 $b=b'$ 时 $\mathcal{A}_{\mathrm{I}}$ 获胜。

经简单计算可知 $\left|\Pr[Y_2]-\frac{1}{2}\right|=\frac{1}{2}\left|\Pr[Y_1]-\frac{1}{2}\right|$。又

$$\left|\Pr\left[Y_2\right]-\frac{1}{2}\right|=\left|\frac{1}{2}\Pr\left[Y_2\left|\eta=0\right.\right]+\frac{1}{2}\Pr\left[Y_2\left|\eta=1\right.\right]-\frac{1}{2}\right|$$
$$\le\frac{1}{2}\left|\Pr\left[Y_2\left|\eta=0\right.\right]-\frac{1}{2}\right|+\frac{1}{2}\left|\Pr\left[Y_2\left|\eta=1\right.\right]-\frac{1}{2}\right|$$

于是接下来我们依据猜测 $\eta\in\{0,1\}$ 的值把游戏分为两条不同的链。即猜测 $\eta=0$ 下的链 $\left\{\text{Game } i_{\eta=0}\right\}$ 和猜测 $\eta=1$ 下的链 $\left\{\text{Game } i_{\eta=1}\right\}$。因为猜测 $\eta\in\{0,1\}$ 只能为 0 或 1，所以在 Game 2 之后只可能选择其中的一条链执行。

Game $3_{\eta=0}$ 这个游戏相比 Game 2 的变化是以下三点：

① 初始化：挑战者选择 $i\leftarrow\{1,\cdots,q_{\text{rpk}}\}$。

② 公钥询问预言机：如果身份 id 是第 i 次公钥询问，挑战者随机选择 $\boldsymbol{v}_i\leftarrow\mathbb{Z}_q^n$。从 H 记载里找到元组 $(id,\boldsymbol{u},\bar{\boldsymbol{u}},\boldsymbol{d})$。令公钥 $pk_{id}=(\boldsymbol{v}_i,\bar{\boldsymbol{u}})$，把元组 $(id,pk_{id},*)$ 存储起来，并返回 pk_{id} 给 $\mathcal{A}_{\text{I}}$。否则，挑战者选择 $\boldsymbol{x}\leftarrow D_{\mathbb{Z}^m,\sigma_2}$，令 $\boldsymbol{v}=\boldsymbol{B}\cdot\boldsymbol{x}\bmod q$。从 H 记载里找到元组 $(id,\boldsymbol{u},\bar{\boldsymbol{u}},\boldsymbol{d})$。令公钥 $pk_{id}=(\boldsymbol{v},\bar{\boldsymbol{u}})$，把元组 $(id,pk_{id},*)$ 存储起来，并返回 pk_{id} 给 $\mathcal{A}_{\text{I}}$。

③ 挑战：如果目标身份 id^* 不是第 i 次询问的公钥预言机，则挑战者中止并输出 $\perp$。否则挑战者选择 $\boldsymbol{S}_1\leftarrow\mathbb{Z}_q^{n\times N}$、$\bar{\boldsymbol{S}}\leftarrow\mathbb{Z}_q^{n\times N}$ 和 $\boldsymbol{S}_2\leftarrow\mathbb{Z}_q^{n\times N}$，设定挑战密文

$$\boldsymbol{C}^*=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^{\text{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\bar{\boldsymbol{A}}^{\text{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p\\ \left[\!\left[\boldsymbol{B}^{\text{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\\ \left[\!\left[\boldsymbol{u}^{\text{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\bar{\boldsymbol{u}}^{\text{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p+\left[\!\left[\boldsymbol{v}_i^{\text{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

在这个游戏中，$\mathcal{A}_{\text{I}}$ 若没有询问目标身份 id^* 的部分私钥，挑战者输出一个随机比特，否则输出 $\mathcal{A}_{\text{I}}$ 的猜测 b'。

Game $3_{\eta=0}$ 不中止输出 $\perp$ 的概率为 $\Pr[\neg\text{abort}]=\frac{1}{q_{\text{rpk}}}$。故 $\left|\Pr\left[Y_3\left|\eta=0\right.\right]-\frac{1}{2}\right|=\frac{1}{q_{\text{rpk}}}\cdot\left|\Pr\left[Y_2\left|\eta=0\right.\right]-\frac{1}{2}\right|$。

Game $3_{\eta=1}$ 这个游戏相比 Game 2 的变化是以下四点：

① 初始化：挑战者选择 $j\leftarrow\{1,\cdots,q_{\text{H}}\}$。

② H 预言机：如果 id 是第 j 次 H 询问，挑战者随机选择 $\boldsymbol{u}_j\leftarrow\mathbb{Z}_q^n$ 和 $\bar{\boldsymbol{u}}\leftarrow\mathbb{Z}_q^n$，把元组 $(id,\boldsymbol{u}_j,\bar{\boldsymbol{u}},\perp)$ 存储起来，并把 $\boldsymbol{u}_j$ 返回给 $\mathcal{A}_{\text{I}}$。否则，挑战者选择 $\boldsymbol{d}\leftarrow D_{\mathbb{Z}^m,\sigma_1}$，令 $\boldsymbol{u}=\boldsymbol{A}\cdot\boldsymbol{d}\bmod q$ 和 $\bar{\boldsymbol{u}}=\bar{\boldsymbol{A}}\cdot\boldsymbol{d}\bmod q$，把元组 $(id,\boldsymbol{u},\bar{\boldsymbol{u}},\boldsymbol{d})$ 存储起来，并返回 $\boldsymbol{u}$ 给 $\mathcal{A}_{\text{I}}$。

③ 部分私钥抽取预言机：当 $\mathcal{A}_{\text{I}}$ 提交身份 id 询问其部分私钥时，挑战者从 H 记载里找到元组 $(id,\boldsymbol{u},\bar{\boldsymbol{u}},\boldsymbol{d})$，如果 $\boldsymbol{d}=\perp$，挑战者中止并输出一个随机比特。否则把 $\boldsymbol{d}$ 返回给 $\mathcal{A}_{\text{I}}$。

④ 挑战：如果目标身份 id^* 不是第 j 次询问的 H 预言机，则挑战者中止并输出 $\perp$。否则挑战者选择 $\boldsymbol{S}_1\leftarrow\mathbb{Z}_q^{n\times N}$、$\bar{\boldsymbol{S}}\leftarrow\mathbb{Z}_q^{n\times N}$ 和 $\boldsymbol{S}_2\leftarrow\mathbb{Z}_q^{n\times N}$，设定挑战密文

$$\boldsymbol{C}^*=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^{\text{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\bar{\boldsymbol{A}}^{\text{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p\\ \left[\!\left[\boldsymbol{B}^{\text{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\\ \left[\!\left[\boldsymbol{u}_j^{\text{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\bar{\boldsymbol{u}}'^{\text{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p+\left[\!\left[\boldsymbol{v}'^{\text{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N},$$

其中 $pk'_{id^*}=(\boldsymbol{v}',\bar{\boldsymbol{u}}')$ 是目标身份 id^* 当前关联的公钥。

Game $3_{\eta=1}$ 不中止输出 $\perp$ 的概率为 $\Pr[\neg\text{abort}]=\frac{1}{q_{\mathrm{H}}}$。故 $\left|\Pr\left[Y_3\middle|\eta=1\right]-\frac{1}{2}\right|=\frac{1}{q_{\mathrm{H}}}\cdot\left|\Pr\left[Y_2\middle|\eta=1\right]-\frac{1}{2}\right|$。

Game $4_{\eta=0}$ 这个游戏只对 Game $3_{\eta=0}$ 进行了一处修改。即

挑战：挑战者随机选择 $\tilde{\boldsymbol{B}}\leftarrow\mathbb{Z}_p^{m\times N}$ 和 $\tilde{\boldsymbol{b}}\leftarrow\mathbb{Z}_p^{N}$，令挑战密文

$$\boldsymbol{C}^*=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\bar{\boldsymbol{A}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p\\ \tilde{\boldsymbol{B}}\\ \left[\!\left[\boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\bar{\boldsymbol{u}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p+\tilde{\boldsymbol{b}}^{\mathrm{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

假设 $\mathcal{A}_{\mathrm{I}}$ 以不可忽略的优势区分 Game $3_{\eta=0}$ 和 Game $4_{\eta=0}$，则利用 $\mathcal{A}_{\mathrm{I}}$ 可构造解决 $\mathrm{LWR}_{n,q,p}$ 问题的算法 $\mathcal{B}$。$\mathcal{B}$ 的输入是一个 $\mathrm{LWR}_{n,q,p}$ 问题实例 $\left(\left(\boldsymbol{F}\middle|\boldsymbol{f}\right),\begin{pmatrix}\boldsymbol{Z}\\ \boldsymbol{z}^{\mathrm{T}}\end{pmatrix}\right)\in\mathbb{Z}_q^{n\times(m+1)}\times\mathbb{Z}_p^{(m+1)\times N}$。$\mathcal{B}$ 模拟挑战者与 $\mathcal{A}_{\mathrm{I}}$ 交互如下：

初始化：$\mathcal{B}$ 令 $\boldsymbol{B}=\boldsymbol{F}$。并选择 $i\leftarrow\{1,\cdots,q_{\mathrm{rpk}}\}$。

公钥询问预言机：如果 *id* 是第 *i* 次公钥询问，$\mathcal{B}$ 令 $\boldsymbol{v}_i=\boldsymbol{f}$。从 *H* 记载里找到元组 $(id,\boldsymbol{u},\bar{\boldsymbol{u}},\boldsymbol{d})$。令公钥 $pk_{id}=(\boldsymbol{f},\bar{\boldsymbol{u}})$，把元组 $(id,pk_{id},*)$ 存储起来，并返回 pk_{id} 给 $\mathcal{A}_{\mathrm{I}}$。

挑战：$\mathcal{B}$ 选择 $\boldsymbol{S}_1\leftarrow\mathbb{Z}_q^{n\times N}$ 和 $\bar{\boldsymbol{S}}\leftarrow\mathbb{Z}_q^{n\times N}$，设定挑战密文

$$\boldsymbol{C}^*=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\bar{\boldsymbol{A}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p\\ \boldsymbol{Z}\\ \left[\!\left[\boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\bar{\boldsymbol{u}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p+\boldsymbol{z}^{\mathrm{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

其余的内容 $\mathcal{B}$ 都与 Game $3_{\eta=0}$ 一样进行处置。

若 $\begin{pmatrix}\boldsymbol{Z}\\ \boldsymbol{z}^{\mathrm{T}}\end{pmatrix}\in\mathbb{Z}_p^{(m+1)\times N}$ 是通过密钥 $\boldsymbol{S}\in\mathbb{Z}_q^{n\times N}$ 产生的，$\boldsymbol{C}^*$ 的分布和 Game $3_{\eta=0}$ 中一样。若 $\begin{pmatrix}\boldsymbol{Z}\\ \boldsymbol{z}^{\mathrm{T}}\end{pmatrix}\in\mathbb{Z}_p^{(m+1)\times N}$ 是随机选择的，$\boldsymbol{C}^*$ 的分布和 Game $4_{\eta=0}$ 中一样。故 $\left|\Pr\left[Y_3\middle|\eta=0\right]-\Pr\left[Y_4\middle|\eta=0\right]\right|=\mathrm{Adv}_{\mathcal{B}}(\lambda)$。

Game $4_{\eta=1}$ 这个游戏只对 Game $3_{\eta=1}$ 进行了一处修改。即

挑战：挑战者随机选择 $\tilde{\boldsymbol{A}}\leftarrow\mathbb{Z}_p^{m\times N}$ 和 $\tilde{\boldsymbol{a}}\leftarrow\mathbb{Z}_p^{N}$，令挑战密文

$$\boldsymbol{C}^*=\begin{pmatrix}\tilde{\boldsymbol{A}}+\left[\!\left[\bar{\boldsymbol{A}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p\\ \left[\!\left[\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\\ \tilde{\boldsymbol{a}}^{\mathrm{T}}+\left[\!\left[\bar{\boldsymbol{u}}'^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right]\!\right]_p+\left[\!\left[\boldsymbol{v}'^{\mathrm{T}}\cdot\boldsymbol{S}_2\right]\!\right]_p\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

假设 $\mathcal{A}_{\mathrm{I}}$ 以不可忽略的优势区分 Game $3_{\eta=1}$ 和 Game $4_{\eta=1}$，则利用 $\mathcal{A}_{\mathrm{I}}$ 可构造解决 $\mathrm{LWR}_{n,q,p}$ 问题的算法 $\mathcal{B}$。$\mathcal{B}$ 的输入是一个 $\mathrm{LWR}_{n,q,p}$ 问题实例 $\left(\left(\boldsymbol{F}\middle|\boldsymbol{f}\right),\begin{pmatrix}\boldsymbol{Z}\\ \boldsymbol{z}^{\mathrm{T}}\end{pmatrix}\right)\in\mathbb{Z}_q^{n\times(m+1)}\times\mathbb{Z}_p^{(m+1)\times N}$。$\mathcal{B}$ 模拟挑战者与 $\mathcal{A}_{\mathrm{I}}$ 交互如下：

初始化：$\mathcal{B}$ 令 $\boldsymbol{A}=\boldsymbol{F}$。并选择 $j\leftarrow\{1,\cdots,q_{\mathrm{H}}\}$。

H 预言机：如果 *id* 是第 *j* 次 *H* 询问，$\mathcal{B}$ 令 $\boldsymbol{u}_j=\boldsymbol{f}$。$\mathcal{B}$ 随机选择 $\bar{\boldsymbol{u}}\leftarrow\mathbb{Z}_q^{n}$。把元组 $(id,\boldsymbol{f},\bar{\boldsymbol{u}},\perp)$ 存储起来，并把 $\boldsymbol{f}$ 返回给 $\mathcal{A}_{\mathrm{I}}$。

挑战：$\mathcal{B}$ 选择 $\bar{\boldsymbol{S}}\leftarrow\mathbb{Z}_q^{n\times N}$ 和 $\boldsymbol{S}_2\leftarrow\mathbb{Z}_q^{n\times N}$，设定挑战密文

$$\boldsymbol{C}^{*}=\begin{pmatrix}\boldsymbol{Z}+\left\lfloor \bar{\boldsymbol{A}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right\rceil_{p}\\ \left\lfloor \boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_{2}\right\rceil_{p}\\ \boldsymbol{z}^{\mathrm{T}}+\left\lfloor \bar{\boldsymbol{u}}'^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right\rceil_{p}+\left\lfloor \boldsymbol{v}'^{\mathrm{T}}\cdot\boldsymbol{S}_{2}\right\rceil_{p}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_{p}^{(2m+1)\times N}.$$

其余的内容 $\mathcal{B}$ 都与 Game $3_{\eta=1}$ 一样进行处置。

若 $\begin{pmatrix}\boldsymbol{Z}\\ \boldsymbol{z}^{\mathrm{T}}\end{pmatrix}\in\mathbb{Z}_{p}^{(m+1)\times N}$ 是由密钥 $\boldsymbol{S}\in\mathbb{Z}_{q}^{n\times N}$ 产生的，$\boldsymbol{C}^{*}$ 的分布和 Game $3_{\eta=1}$ 中一样。若 $\begin{pmatrix}\boldsymbol{Z}\\ \boldsymbol{z}^{\mathrm{T}}\end{pmatrix}\in\mathbb{Z}_{p}^{(m+1)\times N}$ 是随机选择的，$\boldsymbol{C}^{*}$ 的分布和 Game $4_{\eta=1}$ 中一样。故 $\left|\Pr\left[Y_{3}\middle|\eta=1\right]-\Pr\left[Y_{4}\middle|\eta=1\right]\right|=\mathrm{Adv}_{\mathcal{B}}(\lambda)$。

Game $5_{\eta=0}$ 它只对 Game $4_{\eta=0}$ 进行了一处修改。即

挑战：挑战者随机选择 $\hat{\boldsymbol{b}}\leftarrow\mathbb{Z}_{p}^{N}$，令挑战密文为

$$\boldsymbol{C}^{*}=\begin{pmatrix}\left\lfloor \boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_{1}\right\rceil_{p}+\left\lfloor \bar{\boldsymbol{A}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right\rceil_{p}\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\mathrm{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_{p}^{(2m+1)\times N}.$$

在 Game $4_{\eta=0}$ 中，$\tilde{\boldsymbol{b}}\leftarrow\mathbb{Z}_{p}^{N}$ 是均匀随机的，故 $\left\lfloor \boldsymbol{u}^{\mathrm{T}}\cdot\boldsymbol{S}_{1}\right\rceil_{p}+\left\lfloor \bar{\boldsymbol{u}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right\rceil_{p}+\tilde{\boldsymbol{b}}^{\mathrm{T}}$ 亦是均匀随机的。故 $\left|\Pr\left[Y_{4}\middle|\eta=0\right]-\Pr\left[Y_{5}\middle|\eta=0\right]\right|=\mathrm{negl}(\lambda)$。

Game $5_{\eta=1}$ 它只对 Game $4_{\eta=1}$ 进行了一处修改。即

挑战：挑战者随机选择 $\hat{\boldsymbol{A}}\leftarrow\mathbb{Z}_{p}^{m\times N}$ 和 $\hat{\boldsymbol{a}}\leftarrow\mathbb{Z}_{p}^{N}$，令挑战密文为

$$\boldsymbol{C}^{*}=\begin{pmatrix}\hat{\boldsymbol{A}}\\ \left\lfloor \boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{S}_{2}\right\rceil_{p}\\ \hat{\boldsymbol{a}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_{p}^{(2m+1)\times N}.$$

在 Game $4_{\eta=1}$ 中，$\tilde{\boldsymbol{A}}\leftarrow\mathbb{Z}_{p}^{m\times N}$ 和 $\tilde{\boldsymbol{a}}\leftarrow\mathbb{Z}_{p}^{N}$ 是均匀随机的，故 $\tilde{\boldsymbol{A}}+\left\lfloor \bar{\boldsymbol{A}}^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right\rceil_{p}$ 和 $\tilde{\boldsymbol{a}}^{\mathrm{T}}+\left\lfloor \bar{\boldsymbol{u}}'^{\mathrm{T}}\cdot\bar{\boldsymbol{S}}\right\rceil_{p}+\left\lfloor \boldsymbol{v}'^{\mathrm{T}}\cdot\boldsymbol{S}_{2}\right\rceil_{p}$ 亦是均匀随机的。故 $\left|\Pr\left[Y_{4}\middle|\eta=1\right]-\Pr\left[Y_{5}\middle|\eta=1\right]\right|=\mathrm{negl}(\lambda)$。

Game $6_{\eta=0}$ 相比 Game $5_{\eta=0}$ 只进行了一处修改。即

挑战：挑战者随机选择 $\boldsymbol{A}'\leftarrow\mathbb{Z}_{p}^{m\times N}$，令挑战密文为

$$\boldsymbol{C}^{*}=\begin{pmatrix}\left\lfloor \boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_{1}\right\rceil_{p}+\boldsymbol{A}'\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\mathrm{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_{p}^{(2m+1)\times N}.$$

假设 $\mathcal{A}_{1}$ 以不可忽略的优势区分 Game $5_{\eta=0}$ 和 Game $6_{\eta=0}$，则利用 $\mathcal{A}_{1}$ 可构造解决 $\mathrm{LWR}_{n,q,p}$ 问题的算法 $\mathcal{B}$。$\mathcal{B}$ 的输入是一个 $\mathrm{LWR}_{n,q,p}$ 问题实例 $(\boldsymbol{F},\boldsymbol{Z})\in\mathbb{Z}_{q}^{n\times m}\times\mathbb{Z}_{p}^{m\times N}$。$\mathcal{B}$ 模拟挑战者与 $\mathcal{A}_{1}$ 交互如下：

初始化：$\mathcal{B}$ 令 $\bar{\boldsymbol{A}}=\boldsymbol{F}$。

挑战：$\mathcal{B}$ 选择 $\boldsymbol{S}_{1}\leftarrow\mathbb{Z}_{q}^{n\times N}$，令挑战密文为

$$\boldsymbol{C}^{*}=\begin{pmatrix}\left\lfloor \boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_{1}\right\rceil_{p}+\boldsymbol{Z}\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\mathrm{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_{p}^{(2m+1)\times N}.$$

其余的内容 $\mathcal{B}$ 都与 Game $5_{\eta=0}$ 一样进行处置。

若 $\boldsymbol{Z}\in\mathbb{Z}_p^{m\times N}$ 是通过密钥 $\boldsymbol{S}\in\mathbb{Z}_q^{n\times N}$ 产生的，$\boldsymbol{C}^*$ 的分布和 Game $5_{\eta=0}$ 中一样。若 $\boldsymbol{Z}\in\mathbb{Z}_p^{m\times N}$ 是随机选择的，$\boldsymbol{C}^*$ 的分布和 Game $6_{\eta=0}$ 中一样。故 $\left|\Pr\left[Y_5\middle|\eta=0\right]-\Pr\left[Y_6\middle|\eta=0\right]\right|=\mathrm{Adv}_{\mathcal{B}}(\lambda)$。

Game $6_{\eta=1}$ 相比 Game $5_{\eta=1}$ 只进行了一处修改。即

挑战：挑战者随机选择 $\boldsymbol{B}'\leftarrow\mathbb{Z}_p^{m\times N}$，令挑战密文为

$$\boldsymbol{C}^*=\begin{pmatrix}\hat{\boldsymbol{A}}\\ \boldsymbol{B}'\\ \hat{\boldsymbol{a}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

假设 $\mathcal{A}_1$ 以不可忽略的优势区分 Game $5_{\eta=1}$ 和 Game $6_{\eta=1}$，则利用 $\mathcal{A}_1$ 可构造解决 $\mathrm{LWR}_{n,q,p}$ 问题的算法 $\mathcal{B}$。$\mathcal{B}$ 的输入是一个 $\mathrm{LWR}_{n,q,p}$ 问题实例 $(\boldsymbol{F},\boldsymbol{Z})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_p^{m\times N}$。$\mathcal{B}$ 模拟挑战者与 $\mathcal{A}_1$ 交互如下：

初始化：$\mathcal{B}$ 令 $\boldsymbol{B}=\boldsymbol{F}$。

挑战：$\mathcal{B}$ 令挑战密文为 $\boldsymbol{C}^*=\begin{pmatrix}\hat{\boldsymbol{A}}\\ \boldsymbol{Z}\\ \hat{\boldsymbol{a}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}$。

其余的内容 $\mathcal{B}$ 都与 Game $5_{\eta=1}$ 一样进行处置。

若 $\boldsymbol{Z}\in\mathbb{Z}_p^{m\times N}$ 是由密钥 $\boldsymbol{S}\in\mathbb{Z}_q^{n\times N}$ 产生的，$\boldsymbol{C}^*$ 的分布和 Game $5_{\eta=1}$ 中一样。若 $\boldsymbol{Z}\in\mathbb{Z}_p^{m\times N}$ 是随机选择的，$\boldsymbol{C}^*$ 的分布和 Game $6_{\eta=1}$ 中一样。故 $\left|\Pr\left[Y_5\middle|\eta=1\right]-\Pr\left[Y_6\middle|\eta=1\right]\right|=\mathrm{Adv}_{\mathcal{B}}(\lambda)$。

Game $7_{\eta=0}$ 相比 Game $6_{\eta=0}$ 只有一处修改。即

挑战：挑战者随机选择 $\boldsymbol{A}''\leftarrow\mathbb{Z}_p^{m\times N}$，令挑战密文为

$$\boldsymbol{C}^*=\begin{pmatrix}\boldsymbol{A}''\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\mathrm{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

在 Game $6_{\eta=0}$ 中，$\boldsymbol{A}'\leftarrow\mathbb{Z}_p^{m\times N}$ 是均匀随机的，故 $\left\lfloor\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{S}_1\right\rceil_p+\boldsymbol{A}'$ 亦是均匀随机的。故 $\left|\Pr\left[Y_6\middle|\eta=0\right]-\Pr\left[Y_7\middle|\eta=0\right]\right|=\mathrm{negl}(\lambda)$。

Game $7_{\eta=1}$ 相比 Game $6_{\eta=1}$ 只有一处修改。即

挑战：挑战者随机选择 $\boldsymbol{C}^*\leftarrow\mathbb{Z}_p^{(2m+1)\times N}$。

在 Game $6_{\eta=1}$ 中 $\begin{pmatrix}\hat{\boldsymbol{A}}\\ \boldsymbol{B}'\\ \hat{\boldsymbol{a}}\end{pmatrix}\in\mathbb{Z}_p^{(2m+1)\times N}$ 是均匀随机的，故 $\begin{pmatrix}\hat{\boldsymbol{A}}\\ \boldsymbol{B}'\\ \hat{\boldsymbol{a}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}$ 亦是均匀随机的。故 $\left|\Pr\left[Y_6\middle|\eta=1\right]-\Pr\left[Y_7\middle|\eta=1\right]\right|=\mathrm{negl}(\lambda)$。

在 Game $7_{\eta=1}$ 中，挑战密文 $\boldsymbol{C}^*\leftarrow\mathbb{Z}_p^{(2m+1)\times N}$ 是均匀随机的，故 $\left|\Pr\left[Y_7\middle|\eta=1\right]-\frac{1}{2}\right|=0$。

Game $8_{\eta=0}$ 只对 Game $7_{\eta=0}$ 进行了一处修改。即

挑战：挑战者随机选择 $\boldsymbol{C}^*\leftarrow\mathbb{Z}_p^{(2m+1)\times N}$。

在 Game $7_{\eta=0}$ 中 $\begin{pmatrix}\boldsymbol{A}''\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\mathrm{T}}\end{pmatrix}\in\mathbb{Z}_p^{(2m+1)\times N}$ 是均匀随机的，故 $\begin{pmatrix}\boldsymbol{A}''\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\mathrm{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}$ 亦是均匀随机的。故 $\left|\Pr\left[Y_7\middle|\eta=0\right]-\Pr\left[Y_8\middle|\eta=0\right]\right|=\mathrm{negl}(\lambda)$。

在 $\text{Game}\,8_{\eta=0}$ 中，挑战密文 $\boldsymbol{C}^* \leftarrow \mathbb{Z}_p^{(2m+1)\times N}$ 是均匀随机的，故 $\left|\Pr\left[Y_8 \middle| \eta=0\right]-\frac{1}{2}\right|=0$。

综上，我们有

$$\begin{aligned}\text{Adv}_{\mathcal{A}_\text{I}}(\lambda)&=\left|\Pr\left[Y_0\right]-\frac{1}{2}\right|=2\left|\Pr\left[Y_2\right]-\frac{1}{2}\right|\\&\le\left|\Pr\left[Y_2\middle|\eta=0\right]-\frac{1}{2}\right|+\left|\Pr\left[Y_2\middle|\eta=1\right]-\frac{1}{2}\right|\\&=q_{\text{rpk}}\cdot\left|\Pr\left[Y_3\middle|\eta=0\right]-\frac{1}{2}\right|+q_{\text{H}}\cdot\left|\Pr\left[Y_3\middle|\eta=1\right]-\frac{1}{2}\right|\\&=2q_{\text{rpk}}\cdot\text{Adv}_{\mathcal{B}}(\lambda)+2q_{\text{eppk}}\cdot\text{Adv}_{\mathcal{B}}(\lambda)\\&=2\left(q_{\text{rpk}}+q_{\text{eppk}}\right)\cdot\text{Adv}_{\mathcal{B}}(\lambda)\end{aligned}$$

□

所提出的 CLFHE 在 $\mathcal{A}_\text{II}$ 攻击下是 INDr-CPA 安全的。即：

定理 2 若攻击者 $\mathcal{A}_\text{II}$ 在 INDr-CPA 安全游戏中以优势 $\text{Adv}_{\mathcal{A}_\text{II}}(\lambda)$ 攻破所提出的 CLFHE 方案，且公钥询问次数为 q_{rpk}。则存在以优势 $\text{Adv}_{\mathcal{B}}(\lambda)$ 解决 $\text{LWR}_{n,q,p}$ 问题的算法 $\mathcal{B}$。其中

$$\text{Adv}_{\mathcal{A}_\text{II}}(\lambda)\le 2q_{\text{rpk}}\cdot\text{Adv}_{\mathcal{B}}(\lambda)+\text{negl}(\lambda).$$

证明：我们基于游戏序列进行证明。并定义 Y_i 为攻击者 $\mathcal{A}_\text{II}$ 在 Game i 中赢得游戏这一事件。

Game 0 它是攻击所提出的方案的 $\mathcal{A}_\text{II}$ 和挑战者之间的原始 INDr-CPA 游戏。在这个游戏中，$\mathcal{A}_\text{II}$ 的优势 $\text{Adv}_{\mathcal{A}_\text{II}}(\lambda)=\left|\Pr\left[Y_0\right]-\frac{1}{2}\right|$。

Game 1 这个游戏相比 Game 0 修改了以下三点：

① 初始化：挑战者选择 $i\leftarrow\left\{1,\cdots,q_{\text{rpk}}\right\}$。

② 公钥询问预言机：如果 id 是第 i 次公钥询问，挑战者随机选择 $\boldsymbol{v}_i\leftarrow\mathbb{Z}_q^n$，令 $\overline{\boldsymbol{u}}=\overline{\boldsymbol{A}}\cdot\boldsymbol{d}\bmod q$，并返回 $pk_{id}=\left(\boldsymbol{v}_i,\overline{\boldsymbol{u}}\right)$ 给 $\mathcal{A}_\text{II}$。否则，挑战者计算 $\left(pk_{id},sk_{id}\right)\leftarrow\text{KeyGen}\left(mpk,id,d_{id}\right)$，并返回 pk_{id} 给 $\mathcal{A}_\text{II}$。

③ 挑战：如果 id^* 不是第 i 次询问的公钥预言机，则挑战者中止并输出 $\perp$。否则挑战者选择 $\boldsymbol{S}_1\leftarrow\mathbb{Z}_q^{n\times N}$、$\overline{\boldsymbol{S}}\leftarrow\mathbb{Z}_q^{n\times N}$ 和 $\boldsymbol{S}_2\leftarrow\mathbb{Z}_q^{n\times N}$，令挑战密文

$$\boldsymbol{C}^*=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^\text{T}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{A}}^\text{T}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p\\\left[\!\left[\boldsymbol{B}^\text{T}\cdot\boldsymbol{S}_2\right]\!\right]_p\\\left[\!\left[\boldsymbol{u}^\text{T}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{u}}^\text{T}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p+\left[\!\left[\boldsymbol{v}_i^\text{T}\cdot\boldsymbol{S}_2\right]\!\right]_p\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

Game 1 不中止输出 $\perp$ 的概率为 $\Pr\left[\neg\text{abort}\right]=\frac{1}{q_{\text{rpk}}}$。故 $\left|\Pr\left[Y_1\right]-\frac{1}{2}\right|=\frac{1}{q_{\text{rpk}}}\cdot\left|\Pr\left[Y_0\right]-\frac{1}{2}\right|$。

Game 2 这个游戏相比 Game 1 只修改了一处。即

挑战：挑战者随机选择 $\tilde{\boldsymbol{B}}\leftarrow\mathbb{Z}_p^{m\times N}$ 和 $\tilde{\boldsymbol{b}}\leftarrow\mathbb{Z}_p^N$，令挑战密文

$$\boldsymbol{C}^*=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^\text{T}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{A}}^\text{T}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p\\\tilde{\boldsymbol{B}}\\\left[\!\left[\boldsymbol{u}^\text{T}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{u}}^\text{T}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p+\tilde{\boldsymbol{b}}^\text{T}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

假设 $\mathcal{A}_{\text{II}}$ 以不可忽略的优势区分 Game 1 和 Game 2，则利用 $\mathcal{A}_{\text{II}}$ 可解决一个 $\text{LWR}_{n,q,p}$ 问题实例 $\left(\left(\boldsymbol{F}\,|\,\boldsymbol{f}\right),\begin{pmatrix}\boldsymbol{Z}\\ \boldsymbol{z}^{\text{T}}\end{pmatrix}\right)\in\mathbb{Z}_q^{n\times(m+1)}\times\mathbb{Z}_p^{(m+1)\times N}$。于是，有 $\left|\Pr[Y_1]-\Pr[Y_2]\right|=\text{Adv}_{\mathcal{B}}(\lambda)$。

Game 3 相比 Game 2 只修改了一个地方。即

挑战：挑战者随机选择 $\hat{\boldsymbol{b}}\leftarrow\mathbb{Z}_p^N$，令挑战密文为

$$\boldsymbol{C}^*=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^{\text{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\left[\!\left[\overline{\boldsymbol{A}}^{\text{T}}\cdot\overline{\boldsymbol{S}}\right]\!\right]_p\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\text{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

这里有 $\left|\Pr[Y_2]-\Pr[Y_3]\right|=\text{negl}(\lambda)$。

Game 4 相比 Game 3 只修改了一个地方。即

挑战：挑战者随机选择 $\boldsymbol{A}'\leftarrow\mathbb{Z}_p^{m\times N}$，令挑战密文为

$$\boldsymbol{C}^*=\begin{pmatrix}\left[\!\left[\boldsymbol{A}^{\text{T}}\cdot\boldsymbol{S}_1\right]\!\right]_p+\boldsymbol{A}'\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\text{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

假设 $\mathcal{A}_{\text{II}}$ 以不可忽略的优势区分 Game 3 和 Game 4，则利用 $\mathcal{A}_{\text{II}}$ 可解决一个 $\text{LWR}_{n,q,p}$ 问题实例 $(\boldsymbol{F},\boldsymbol{Z})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_p^{m\times N}$。于是，有 $\left|\Pr[Y_3]-\Pr[Y_4]\right|=\text{Adv}_{\mathcal{B}}(\lambda)$。

Game 5 相比 Game 4 只进行了一处修改。即

挑战：挑战者随机选择 $\boldsymbol{A}''\leftarrow\mathbb{Z}_p^{m\times N}$，令挑战密文为

$$\boldsymbol{C}^*=\begin{pmatrix}\boldsymbol{A}''\\ \tilde{\boldsymbol{B}}\\ \hat{\boldsymbol{b}}^{\text{T}}\end{pmatrix}+\mu\cdot\boldsymbol{G}\in\mathbb{Z}_p^{(2m+1)\times N}.$$

这里有 $\left|\Pr[Y_4]-\Pr[Y_5]\right|=\text{negl}(\lambda)$。

Game 6 只对 Game 5 进行了一处修改。即

挑战：挑战者随机选择 $\boldsymbol{C}^*\leftarrow\mathbb{Z}_p^{(2m+1)\times N}$。

这里，有 $\left|\Pr[Y_5]-\Pr[Y_6]\right|=\text{negl}(\lambda)$，且有 $\left|\Pr[Y_6]-\frac{1}{2}\right|=0$。

综上，我们有

$$\begin{aligned}\text{Adv}_{\mathcal{A}_{\text{II}}}^{\text{CLFHE}}(\lambda)&=\left|\Pr[Y_0]-\frac{1}{2}\right|=q_{\text{rpk}}\cdot\left|\Pr[Y_1]-\frac{1}{2}\right|\\ &\le q_{\text{rpk}}\cdot\left|\Pr[Y_2]+\text{Adv}_{\mathcal{B}}(\lambda)-\frac{1}{2}\right|+\text{negl}(\lambda)\\ &\le q_{\text{rpk}}\cdot\left|\Pr[Y_4]+2\text{Adv}_{\mathcal{B}}(\lambda)-\frac{1}{2}\right|+\text{negl}(\lambda)\\ &\le q_{\text{rpk}}\cdot\left|\Pr[Y_6]+2\text{Adv}_{\mathcal{B}}(\lambda)-\frac{1}{2}\right|+\text{negl}(\lambda)\\ &\le 2q_{\text{rpk}}\cdot\text{Adv}_{\mathcal{B}}(\lambda)+\text{negl}(\lambda)\end{aligned}$$

4.3. 参数设置

所提出的 CLFHE 方案应满足以下条件：

$$m \geq 6n\log q$$

$\sigma_1 \geq \left\|\tilde{\mathbf{T}}\right\| \cdot \omega\left(\sqrt{\log m}\right)$，其中 $\left\|\tilde{\mathbf{T}}\right\| \leq O\left(\sqrt{n\log q}\right)$

$$\sigma_2 \geq \omega\left(\sqrt{\log m}\right)$$

$p > 8(N+1)^L \Delta$，其中 $\Delta = \frac{3}{2} + m\sqrt{m} \cdot \left(\sigma_1 + \frac{1}{2} \cdot \sigma_2\right)$

$$q \geq p \cdot B \cdot n^{\omega(1)}$$

$q \leq 2^n$，$q/B \geq 2^{n^\varepsilon}$，其中 $\varepsilon > 0$。

于是，所提出的 CLFHE 方案的系统参数可设置如下：

$$n = n(\lambda, L)$$

$$m = 6n^{1+\xi} = O(n \cdot L \cdot \log n)$$

$$\sigma_1 = \sqrt{m} \cdot \omega\left(\sqrt{\log n}\right)$$

$$\sigma_2 = \omega\left(\sqrt{\log n}\right)$$

$$p = 2^{O(L \cdot \log n)}$$

$$q = B \cdot 2^{O(L \cdot \log n)},$$

其中 ξ 使得 $n^\xi > \lceil \log q \rceil = O(L \cdot \log n)$。

5. 结束语

本文提出了第一个基于 LWR 问题的 CLFHE 方案，并在随机预言机模型下证明了它是 INDr-CPA 安全的。LWR 问题是 LWE 问题的变形。它省掉了 LWE 问题中的高斯噪声抽样。高斯噪声抽样计算开销非常大。因此本文所提出的 CLFHE 方案比现有基于 LWE 问题的 CLFHE 方案[6] [7]具有更高的计算效率。我们接下来会致力于基于所提出的 CLFHE 方案构造相关安全协议解决物联网、云计算和区块链等面临的安全问题。

参考文献

[1] Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. *Proceedings of the* 41*st Annual ACM Symposium on Theory of Computing*, Bethesda, 31 May 2009-2 June 2009, 169-178. https://doi.org/10.1145/1536414.1536440

[2] Gentry, C., Sahai, A. and Waters, B. (2013) Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. In: Canetti, R., Garay, J.A., Eds., *Advances in Cryptology—CRYPTO* 2013, *Lecture Notes in Computer Science*, Vol. 8042, Springer, Berlin, 75-92. https://doi.org/10.1007/978-3-642-40041-4_5

[3] Regev, O. (2009) On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, **56**, 1-40. https://doi.org/10.1145/1568318.1568324

[4] Al-Riyami, S.S. and Paterson, K.G. (2003) Certificateless Public Key Cryptography. In: Laih, C.S., Ed., *Advances in Cryptology—ASIACRYPT* 2003, *Lecture Notes in Computer Science*, Vol. 2894, Springer, Berlin, 452-473. https://doi.org/10.1007/978-3-540-40061-5_29

[5] Boneh, D. and Franklin, M. (2001) Identity-Based Encryption from the Weil Pairing. In: Kilian, J., Ed., *Advances in*

Cryptology—CRYPTO 2001, *Lecture Notes in Computer Science*, Vol. 2139, Springer, Berlin, 213-229. https://doi.org/10.1007/3-540-44647-8_13

[6] Chen, H., Hu, Y. and Lian, Z. (2017) Leveled Homomorphic Encryption in Certificateless Cryptosystem. *Chinese Journal of Electronics*, **26**, 1213-1220.https://doi.org/10.1049/cje.2017.07.008

[7] Li, M. (2020) Leveled Certificateless Fully Homomorphic Encryption Schemes from Learning with Errors. *IEEE Access*, **8**, 26749-26763. https://doi.org/10.1109/ACCESS.2020.2971342

[8] Banerjee, A., Peikert, C. and Rosen, A. (2012) Pseudorandom Functions and Lattices. In: Pointcheval, D., Johansson, T., Eds., *Advances in Cryptology—EUROCRYPT* 2012, *Lecture Notes in Computer Science*, Vol. 7237, Springer, Berlin, 719-737. https://doi.org/10.1007/978-3-642-29011-4_42

[9] 李明祥, 刘照, 张明艳. 无高斯噪声的全同态加密方案[J]. 计算机应用, 2017, 37(12): 3430-3434.

[10] Luo, F., Wang, F., Wang K., *et al*. (2018) LWR-Based Fully Homomorphic Encryption, Revisited. *Security and Communication Networks*, **2018**, Article ID: 5967635. https://doi.org/10.1155/2018/5967635

[11] Peikert, C. (2014) A Decade of Lattice Cryptography. *Foundations and Trends in Theoretical Computer Science*, **10**, 283-424. http://dx.doi.org/10.1561/0400000074

[12] Alwen, J. and Peikert, C. (2011) Generating Shorter Bases for Hard Random Lattices. *Theory of Computing Systems*, **48**, 535-553. https://doi.org/10.1007/s00224-010-9278-3

[13] Gentry, C., Peikert, C. and Vaikuntanathan, V. (2008) Trapdoors for Hard Lattices and New Cryptographic Constructions. *Proceedings of the* 40*th Annual ACM Symposium on Theory of Computing*, Victoria, 17-20 May 2008, 197-206. https://doi.org/10.1145/1374376.1374407

[14] Micciancio, D. and Regev, O. (2007) Worst-Case to Average-Case Reductions Based on Gaussian Measures. *SIAM Journal on Computing*, **37**, 267-302. https://doi.org/10.1137/S00975397054473

[15] Micciancio, D. and Peikert, C. (2012) Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In: Pointcheval, D., Johansson, T., Eds., *Advances in Cryptology—EUROCRYPT* 2012, *Lecture Notes in Computer Science*, Vol. 7237, Springer, Berlin, 700-718. https://doi.org/10.1007/978-3-642-29011-4_41