Computer Science and Application 计算机科学与应用, **2023, 13(9), 1675-1690**
Published Online September 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.139166

Hans汉斯

基于身份的整数矩阵全同态加密方案

李明祥

河北金融学院，金融研究所，河北　保定

收稿日期：2023 年 8 月 3 日；录用日期：2023 年 9 月 7 日；发布日期：2023 年 9 月 14 日

摘　要

全同态加密允许人们在不知晓解密密钥的情形下对密文进行任意计算。它在云计算等领域具有重要的应用价值。本论文致力于基于身份的多比特全同态加密方案的设计与安全性分析。首先，基于带误差学习问题 (**learning with errors**, LWE) 设计了一个层次型基于身份的多比特全同态加密方案，该方案加密整数矩阵，支持整数矩阵加法和乘法同态运算；其次，在标准模型下证明了所设计方案满足 **INDr-sID-CPA** 安全性；最后，给出了所设计方案有关参数的具体设置。迄今为止，人们还没有提出支持整数矩阵同态运算的基于身份的多比特全同态加密方案。因此，所设计的方案不仅具有理论意义，而且在云计算等领域还具有应用前景。

关键词

全同态加密，基于身份，层次型，LWE 问题

Identity-Based Integer Matrix Fully Homomorphic Encryption Scheme

Mingxiang Li

Institute of Financial Research, Hebei Finance University, Baoding Hebei

Received: Aug. 3^{rd}, 2023; accepted: Sep. 7^{th}, 2023; published: Sep. 14^{th}, 2023

文章引用: 李明祥. 基于身份的整数矩阵全同态加密方案 [J]. 计算机科学与应用, 2023, 13(9): 1675-1690.
DOI: 10.12677/csa.2023.139166

Abstract

Fully homomorphic encryption allows us to perform arbitrary computation on encrypted data despite not having the secret decryption key. It has critical applications in fields such as cloud computing. This paper focuses on the design and security analysis of identity-based multi-bit fully homomorphic encryption schemes. Firstly, based on the learning with errors (LWE) problem, this paper designs a leveled identity-based multi-bit fully homomorphic encryption scheme which encrypts integer matrices and supports homomorphic integer matrix addition and multiplication. Then, this paper proves that the proposed scheme satisfies INDr-sID-CPA security in the standard model. Finally, this paper gives the specific parameter settings of the proposed scheme. To date, the identity-based multi-bit fully homomorphic encryption scheme for integer matrix messages has not been proposed. Hence, the proposed scheme in this paper not only has theoretical significance but also has application prospects in cloud computing and other fields.

Keywords

Fully Homomorphic Encryption, Identity-Based, Leveled, LWE Problem

1. 引言

全同态加密 (fully homomorphic encryption, FHE) 允许任何人对密文进行任意计算，解密结果与对明文进行同样计算的结果一样，即$\mathsf{Dec}_{sk}(f(\mathsf{Enc}_{pk}(\mu_1),\ldots,\mathsf{Enc}_{pk}(\mu_\kappa))) = f(\mu_1,\ldots,\mu_\kappa)$。利用全同态加密，我们可以把计算外包给远程服务器，而不必担心数据隐私泄露问题。2009 年 Gentry [1] 利用格技术构造了第一个全同态加密方案。Gentry 开创性的工作掀起了全同态加密的研究热潮。2013 年 Genry、Sahai 和 Waters [2] 利用近似特征向量技术，基于带误差学习 (learning with wrrors, LWE) 问题构造了一个层次型全同态加密方案。在层次型全同态加密方案中，方案的参数依赖于方案所能计算的电路深度。并且利用 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。Genry、Sahai 和 Waters [2] 提出的全同态加密方案是单比特全同态加密方案，其密文数量比较庞大。同态操作因为需要处理如此大量的密文，其计算效率比较低。为了提高同态操作的计算效率，Smart 和 Vercauteren [3] 提出了密文打包技术。即把多个消息放进一个密文中，并且可以应用单指令多数据 (single instruction multiple data, SIMD) 进行同态密文计算操作。人们提出了几个层次型多比特全同态加密方案 [4, 5]，它们加密比特矩阵，支持比特矩阵加法和乘法同态运算。近年来，人们又提出了几个层次型多比特全同态加密方案 [6]，它们加密整数矩阵，支持整数矩阵加法和乘法同态运算。

Shamir [7] 首先提出了基于身份的加密 (identity-based encryption, IBE) 的思想。在基于身份的加密方案中，用户的公钥由其身份信息计算出来，用户的私钥由被称为密钥生成中心 (key generation centre, KGC) 的可信第三方产生。基于身份的加密简化了用户公钥的管理，它可应用到资源受限的环境中。人们基于LWE 问题提出了一些基于身份的加密方案 [8, 9]。基于身份的全同态加密 (identity-based fully homomorphic encryption, IBFHE) 把全同态加密和基于身份的加密两者结合起来，它具有全同态加密和基于身份的加密两者的特点和优势。近年来，人们提出了一些层次型基于身份的全同态加密方案 [10, 11]。这些基于身份的全同态加密方案 [10, 11] 都是单比特全同态加密方案。最近，陈虹等人 [12] 构造了一个层次型基于身份的多比特全同态加密方案，它加密比特矩阵，支持比特矩阵加法和乘法同态运算。截至目前，人们还没有提出基于身份的多比特全同态加密方案，该方案加密整数矩阵，支持整数矩阵加法和乘法同态运算。

鉴于以上基于身份的全同态加密方案的研究现状，本论文利用近似特征向量技术，基于LWE 问题设计了一个层次型基于身份的多比特全同态加密方案，它加密整数矩阵，支持整数矩阵加法和乘法同态运算，并且证明了它在选择明文攻击下是安全的。此外，我们还给出了所设计方案的正确性分析和有关参数设置。

2. 预备知识

下面给出本论文需要的预备知识。

2.1. 符号定义

首先我们给出符号约定，具体如 表 1 所示。

2.2. 统计距离

对域 S 上的两个概率分布 X 和 Y（或具有这些分布的随机变量），它们的统计距离定义为

$$\Delta(X,Y)=\max_{A\subseteq S}\left|\Pr[X\in A]-\Pr[Y\in A]\right|.$$

如果两个系集$X=\{X_\lambda\}_{\lambda\in\mathbb{N}}$ 和$Y=\{Y_\lambda\}_{\lambda\in\mathbb{N}}$ 的统计距离不大于 $\epsilon(\lambda)$，则它们是 $\epsilon=\epsilon(\lambda)$ 接近的。如果$\epsilon(\lambda)=\mathsf{negl}(\lambda)$，则称它们是统计接近的。如果域$S$ 上系集$X=\{X_\lambda\}_{\lambda\in\mathbb{N}}$ 和 S 上均匀分布系集是 $\epsilon=\epsilon(\lambda)$ 接近的，则 X 在 S 上是 ϵ 均匀的（当S 显然时，我们有时会省略S）。

Table 1. Notations and descriptions

表 1. 符号及其描述

符号	描述
$\mathbb{Z}$	整数集
$\mathbb{R}$	实数集
$\mathbb{Z}_q$	模q 剩余类环，并且定义$\mathbb{Z}_q=(-q/2,q/2]\cap\mathbb{Z}$，其中$q$ 为正整数
$[k]$	集合$\{1,\ldots,k\}$，其中k 为正整数
log	底为 2 的对数
$\lfloor\cdot\rceil$	四舍五入取整
$\mathsf{poly}(\lambda)$	多项式函数，它是函数$f(\lambda)$，且使得对某一常数c，$f(\lambda)=O(\lambda^c)$
$\mathsf{negl}(\lambda)$	可忽略函数，它是函数$f(\lambda)$，且使得对任一固定常数c，$f(\lambda)=o(\lambda^{-c})$
$x\xleftarrow{\$}X$	表示x 是依据分布X 抽样的，其中X 为域S 上的概率分布
$x\xleftarrow{\$}S$	表示x 是依据分布$U(S)$ 抽样的，其中$U(S)$ 为集合S 上的均匀分布
$\boldsymbol{x}$	向量，默认为列向量形式
$\boldsymbol{X}$	矩阵，有时把矩阵看作其列向量的有序集合
$\boldsymbol{I}_n$	$n\times n$ 单位矩阵
$\boldsymbol{X}^{\mathsf{T}}$	矩阵$\boldsymbol{X}$ 的转置
$(\boldsymbol{X}\|\boldsymbol{Y})$	矩阵$\boldsymbol{X}$ 和$\boldsymbol{Y}$ 的水平连接
$\otimes$	张量积
$\|\boldsymbol{x}\|$	向量的2 范数，定义为$\|\boldsymbol{x}\|=\left(\sum_i\|x_i\|^2\right)^{1/2}$，其中$x_i$ 为向量$\boldsymbol{x}$ 的分量
$\|\boldsymbol{x}\|_\infty$	向量的∞ 范数，定义为$\|\boldsymbol{x}\|_\infty=\max_i\|x_i\|$，其中$x_i$ 为向量$\boldsymbol{x}$ 的分量
$\|\boldsymbol{X}\|$	矩阵的2 范数，定义为$\|\boldsymbol{X}\|=\max_j\|\boldsymbol{x}_j\|$，其中$\boldsymbol{x}_j$ 为矩阵$\boldsymbol{X}$ 的列向量
$\|\boldsymbol{X}\|_\infty$	矩阵的∞ 范数，定义为$\|\boldsymbol{X}\|_\infty=\max_{i,j}\|x_{i,j}\|$，其中$x_{i,j}$ 为矩阵$\boldsymbol{X}$ 的元素
$\widetilde{\boldsymbol{T}}$	线性无关向量集合$\boldsymbol{T}$ 的 Gram-Schmidt 正交化

2.3. 格

定义 1 (格)**.** 令$\boldsymbol{B}=(\boldsymbol{b}_1|\cdots|\boldsymbol{b}_m)\in\mathbb{R}^{m\times m}$ 为$m\times m$ 矩阵，其中$\boldsymbol{b}_1,\ldots,\boldsymbol{b}_m\in\mathbb{R}^m$ 是一组线性无关向量。由基$\boldsymbol{B}$ 生成的m 维格$\varLambda$ 定义为

$$\varLambda=\mathcal{L}(\boldsymbol{B})=\left\{\boldsymbol{B}\boldsymbol{c}=\sum\nolimits_{i\in[m]}c_i\cdot\boldsymbol{b}_i\ \text{ s.t. }\ \boldsymbol{c}\in\mathbb{Z}^m\right\}.$$

定义 2 (q 模格)**.** 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$m$ 维整数格

$$\varLambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{v}\in\mathbb{Z}^m\ \text{ s.t. }\ \boldsymbol{A}\boldsymbol{v}=\boldsymbol{0}\mod q\},$$
$$\varLambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})=\{\boldsymbol{v}\in\mathbb{Z}^m\ \text{ s.t. }\ \boldsymbol{A}\boldsymbol{v}=\boldsymbol{u}\mod q\}.$$

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

定义 3 (离散高斯分布)**.** 对任意$\boldsymbol{c}\in\mathbb{R}^m$、实数$\sigma>0$ 和m 维格$\varLambda$，$\varLambda$ 上的离散高斯分布定义为

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

其中$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/\sigma^2)$ 是$\mathbb{R}^m$ 上以$\boldsymbol{c}$ 为中心、σ 为参数的高斯函数。

引理 1 ([13, 14])**.** 存在概率多项式时间算法$\mathsf{TrapGen}(n,q)$，它输入正整数n、$q\geq2$ 和$m\geq6n\log q$，输出矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和$\varLambda^{\perp}(\boldsymbol{A})$ 的一组基$\boldsymbol{T}\in\mathbb{Z}^{m\times m}$，并且满足：$\boldsymbol{A}$ 统计接近于$\mathbb{Z}_q^{n\times m}$ 上的

均匀分布；$\|\widetilde{\boldsymbol{T}}\| \leq O(\sqrt{n\log q})$。

引理 2 ([8])．令n、$q \geq 2$ 和$m \geq 2n\log q$ 为正整数。则存在概率多项式时间算法SampleLeft$(\boldsymbol{A}, \boldsymbol{A}_1, \boldsymbol{T}_{\boldsymbol{A}}, \boldsymbol{u}, \sigma)$，它输入矩阵$\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$、矩阵$\boldsymbol{A}_1 \in \mathbb{Z}_q^{n\times m_1}$、$\Lambda^{\perp}(\boldsymbol{A})$ 的一组基$\boldsymbol{T}_{\boldsymbol{A}} \in \mathbb{Z}^{m\times m}$、向量$\boldsymbol{u} \in \mathbb{Z}_q^n$ 和高斯参数$\sigma \geq \|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\| \cdot \omega(\sqrt{\log(m+m_1)})$，而输出向量$\boldsymbol{v} \in \mathbb{Z}^{m+m_1}$，并且$\boldsymbol{v}$ 的分布统计接近于分布$D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{F}),\sigma}$，其中$\boldsymbol{F} = (\boldsymbol{A}|\boldsymbol{A}_1) \in \mathbb{Z}_q^{n\times(m+m_1)}$。

引理 3 ([8])．令n、$q \geq 2$ 和$m > n$ 为正整数。则存在概率多项式时间算法SampleRight$(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{R}, \boldsymbol{T}_{\boldsymbol{B}}, \boldsymbol{u}, \sigma)$，它输入矩阵$\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$、矩阵$\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}$、矩阵$\boldsymbol{R} \in \{-1,1\}^{m\times m}$、$\Lambda^{\perp}(\boldsymbol{B})$ 的一组基$\boldsymbol{T}_{\boldsymbol{B}} \in \mathbb{Z}^{m\times m}$、向量$\boldsymbol{u} \in \mathbb{Z}_q^n$ 和高斯参数$\sigma \geq \|\widetilde{\boldsymbol{T}_{\boldsymbol{B}}}\| \cdot m \cdot \omega(\sqrt{\log m})$，而输出向量$\boldsymbol{v} \in \mathbb{Z}^{2m}$，并且$\boldsymbol{v}$ 的分布统计接近于分布$D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{F}),\sigma}$，其中$\boldsymbol{F} = (\boldsymbol{A}|\boldsymbol{A}\boldsymbol{R}+\boldsymbol{B}) \in \mathbb{Z}_q^{n\times 2m}$。

这里我们介绍一种特殊的矩阵，它的陷门是公开的。

引理 4 ([15])．对任意$m = n\cdot(\lfloor\log q\rfloor+1)$，存在一个可计算矩阵$\boldsymbol{G} \in \mathbb{Z}_q^{n\times m}$ 和一个可计算的确定性函数$\boldsymbol{G}^{-1}(\cdot)$，它们满足：给定矩阵$\boldsymbol{A} \in \mathbb{Z}_q^{n\times m'}$，其中$m' \geq 1$，函数$\boldsymbol{G}^{-1}(\boldsymbol{A})$ 输出一个比特矩阵$\boldsymbol{G}^{-1}(\boldsymbol{A}) \in \{0,1\}^{m\times m'}$，并使得$\boldsymbol{G}\boldsymbol{G}^{-1}(\boldsymbol{A}) = \boldsymbol{A}$。

具体地，设置$\boldsymbol{G} = \boldsymbol{I}_n \otimes \boldsymbol{g}^{\mathsf{T}}$，其中$\boldsymbol{g} = (1,2,\ldots,2^{\lfloor\log q\rfloor})^{\mathsf{T}} \in \mathbb{Z}_q^{\lfloor\log q\rfloor+1}$。定义函数$\boldsymbol{G}^{-1}: \mathbb{Z}_q^{n\times m'} \to \{0,1\}^{m\times m'}$，它把输入矩阵的每一项$a \in \mathbb{Z}_q$ 都扩展为一个比特向量$(a_0,\ldots,a_{\lfloor\log q\rfloor})^{\mathsf{T}} \in \{0,1\}^{\lfloor\log q\rfloor+1}$，并且$a = \boldsymbol{g}^{\mathsf{T}}\cdot(a_0,\ldots,a_{\lfloor\log q\rfloor})^{\mathsf{T}}$。这样，对矩阵$\boldsymbol{A} \in \mathbb{Z}_q^{n\times m'}$，我们有$\boldsymbol{G}\boldsymbol{G}^{-1}(\boldsymbol{A}) = \boldsymbol{A}$成立。

2.4. LWE 问题

定义 4 (LWE 问题)．对于安全参数λ，令$n = n(\lambda)$ 和$q = q(\lambda) \geq 2$ 为正整数，令误差分布$\chi = \chi(\lambda)$ 为$\mathbb{Z}$ 上的分布。LWE$_{n,q,\chi}$ 问题是区分以下两种分布：在第一种分布中，随机均匀选择$\boldsymbol{v} \xleftarrow{\$} \mathbb{Z}_q^n$，然后通过随机均匀选择$\boldsymbol{a}_i \xleftarrow{\$} \mathbb{Z}_q^n$，选择误差$e_i \xleftarrow{\$} \chi$，设置$p_i = \boldsymbol{a}_i^{\mathsf{T}}\boldsymbol{v} + e_i \mod q$，而抽取样本$(\boldsymbol{a}_i, p_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$；在第二种分布中，样本$(\boldsymbol{a}_i, p_i)$ 是从$\mathbb{Z}_q^n \times \mathbb{Z}_q$ 中随机均匀抽取的。LWE$_{n,q,\chi}$ 假设认为LWE$_{n,q,\chi}$ 问题没有可行解。

在一定的参数条件下，我们可把格问题GapSVP 量子地或经典地归约到LWE 问题，如下面的引理所示。在这些归约中，误差分布χ 为离散高斯分布$D_{\mathbb{Z},\alpha q}$，其中αq 为高斯参数，且$\alpha \in (0,1)$。

引理 5 ([15–18])．令$q = q(n) \in \mathbb{N}$ 为素数的幂$q = p^r$ 或者为素数的积$q = \prod_i q_i$（$q_i = \mathrm{poly}(n)$ 且对$i \neq j$，$q_i \neq q_j$），并令$\alpha > 2\sqrt{n}/q$。如果存在解决平均情况LWE$_{n,q,D_{\mathbb{Z},\alpha q}}$ 问题的有效算法，那么：

- 存在解决任意n 维格上GapSVP$_{\widetilde{O}(n/\alpha)}$ 问题的有效量子算法；
- 如果$q \geq \widetilde{O}(2^{n/2})$，则存在解决任意$n$ 维格上GapSVP$_{\widetilde{O}(n/\alpha)}$ 问题的有效经典算法。

3. 基于身份全同态加密的定义和安全模型

下面给出基于身份的全同态加密方案的定义和安全模型。

3.1. 定义

基于身份的全同态加密方案包括五个多项式时间算法(Setup, KeyGen, Encrypt, Decrypt, Eval)。下面我们给出层次型基于身份的全同态加密方案的具体定义。

$(pp, msk) \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$：它输入安全参数$\lambda$ 和电路的最大深度L，输出系统参数pp 和主密钥msk。系统参数包括对身份空间$\mathcal{ID}$、消息空间$\mathcal{M}$ 和密文空间$\mathcal{C}$ 的描述。这个算法由密钥生成中心 KGC 执行。

$sk_{id} \leftarrow \mathsf{KeyGen}(pp, msk, id)$：它输入系统参数$pp$、主密钥$msk$ 和身份$id \in \mathcal{ID}$，输出私钥sk_{id}。这个算法由密钥生成中心 KGC 执行。

$C \leftarrow \mathsf{Encrypt}(pp, id, M)$：它输入系统参数$pp$、用户$id$ 的公钥pk_{id} 和消息$M \in \mathcal{M}$，输出密文$C \in \mathcal{C}$。

$M \leftarrow \mathsf{Decrypt}(pp, sk_{id}, C)$：它输入系统参数$pp$、私钥$sk_{id}$ 和密文$C \in \mathcal{C}$，输出消息$M \in \mathcal{M}$。

$C_f \leftarrow \mathsf{Eval}(pp, id, f, C_1, \ldots, C_\kappa)$：它输入系统参数$pp$、电路$f : \mathcal{M}^\kappa \to \mathcal{M}$ 且其深度$d \le L$ 以及同一身份id 下的密文$C_1, \ldots, C_\kappa$，输出密文$C_f \in \mathcal{C}$。

这些算法应当满足正确性要求。即对任意$(pp, msk) \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$、任意$id \in \mathcal{ID}$、任意$M_1, \ldots, M_\kappa \in \mathcal{M}$ 以及任意$f : \mathcal{M}^\kappa \to \mathcal{M}$，且$f$ 的电路深度$d \le L$，设置$\{C_i \leftarrow \mathsf{Encrypt}(pp, id, M_i)\}_{i\in[\kappa]}$ 和$C_f \leftarrow \mathsf{Eval}(pp, id, f, C_1, \ldots, C_\kappa)$，则$f(M_1, \ldots, M_\kappa) \leftarrow \mathsf{Decrypt}(pp, sk_{id}, C_f)$，其中$sk_{id} \leftarrow \mathsf{KeyGen}(pp, msk, id)$。

3.2. 安全模型

基于身份的全同态加密方案通常应当满足在选择性选择身份和适应性选择明文攻击下密文是不可区分的 (IND-sID-CPA)。本论文提出的基于身份的全同态加密方案满足比 IND-sID-CPA 更强的安全性，即满足在选择性选择身份和适应性选择明文攻击下密文与密文空间的随机元素是不可区分的 (INDr-sID-CPA)。下面我们通过一个在敌手$\mathcal{A}$ 和挑战者之间的游戏定义这种安全性。

初始： $\mathcal{A}$ 输出目标身份id^*，它想要在id^* 上接受挑战。

设置： 挑战者运行$(pp, msk) \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$，并把$pp$ 发送给$\mathcal{A}$。

阶段 1： $\mathcal{A}$ 适应性地发出私钥询问$id \in \mathcal{ID}$，其中$id \ne id^*$。挑战者运行$sk_{id} \leftarrow \mathsf{KeyGen}(pp, msk, id)$，并把$sk_{id}$ 发送给$\mathcal{A}$。

挑战： $\mathcal{A}$ 输出消息$M^* \in \mathcal{M}$，它想要在M^* 上接受挑战。挑战者随机选择$b \xleftarrow{\$} \{0,1\}$ 和$C \xleftarrow{\$} \mathcal{C}$。如果$b = 0$，它设置挑战密文$C^* = \mathsf{Encrypt}(pp, id^*, M^*)$；如果$b = 1$，它设置挑战密文$C^* = C$。挑战者把$C^*$ 作为挑战发送给$\mathcal{A}$。

阶段 2： $\mathcal{A}$ 继续发出私钥询问$id \in \mathcal{ID}$，其中$id \ne id^*$。

猜测： $\mathcal{A}$ 输出猜测$b' \in \{0,1\}$。如果$b = b'$，$\mathcal{A}$ 赢得游戏。

我们把这样的敌手$\mathcal{A}$ 称为 INDr-sID-CPA 敌手。敌手$\mathcal{A}$ 攻击基于身份的全同态加密方案$\mathcal{E}$ 的优势定义为

$$\mathsf{Adv}_{\mathcal{E},\mathcal{A}}^{\text{INDr-sID-CPA}}(\lambda) = \left|\Pr[b = b'] - 1/2\right|.$$

定义 5 (INDr-sID-CPA 安全性). 如果对任意多项式时间 INDr-sID-CPA 敌手$\mathcal{A}$，$\mathsf{Adv}_{\mathcal{E},\mathcal{A}}^{\text{INDr-sID-CPA}}(\lambda)$ 都是可忽略的，则我们称这个基于身份的全同态加密方案$\mathcal{E}$ 是 INDr-sID-CPA 安全的。

为了证明本论文提出的基于身份的全同态加密方案的安全性，我们引入一种循环安全性。这里，通过一个在敌手$\mathcal{A}$ 和挑战者之间的游戏定义这一安全概念。

设置: 挑战者令$h : \mathcal{K} \to \mathcal{C}$ 为从$\mathcal{K}$ 到$\mathcal{C}$ 的函数，其中$\mathcal{K}$ 为用户私钥空间，$\mathcal{C}$ 为密文空间，计算$(pp, msk) \leftarrow \mathsf{Setup}(1^\lambda, 1^L)$，并把$h$ 和pp 发送给$\mathcal{A}$。

阶段 1: $\mathcal{A}$ 适应性地发出私钥询问$id \in \mathcal{ID}$。挑战者运行$sk_{id} \leftarrow \mathsf{KeyGen}(pp, msk, id)$，并把$sk_{id}$ 发送给$\mathcal{A}$。

挑战: $\mathcal{A}$ 输出目标身份$id^* \in \mathcal{ID}$。这里要求$\mathcal{A}$ 在阶段 1 没有询问id^* 的私钥。挑战者随机选择$b \xleftarrow{\$} \{0,1\}$，计算$sk_{id^*} \leftarrow \mathsf{KeyGen}(pp, msk, id^*)$，计算挑战密文$C^*$ 如下：

$$C^* = \begin{cases} \mathsf{Eval}(pp, id^*, h_+, \mathsf{Encrypt}(pp, id^*, 0), h(sk_{id^*})), & \text{若 } b = 0 \\ \mathsf{Encrypt}(pp, id^*, 0), & \text{若 } b = 1. \end{cases}$$

其中函数$h_+ : \mathcal{M} \times \mathcal{M} \to \mathcal{M}$，且$h_+(M_1, M_2) = M_1 + M_2$。挑战者把$C^*$ 作为挑战发送给$\mathcal{A}$。

阶段 2: $\mathcal{A}$ 继续发出私钥询问$id \in \mathcal{ID}$，其中$id \neq id^*$。

猜测: $\mathcal{A}$ 输出猜测$b' \in \{0,1\}$。如果$b = b'$，$\mathcal{A}$ 赢得游戏。

关于函数h，$\mathcal{A}$ 攻击基于身份的全同态加密方案$\mathcal{E}$ 的优势定义为

$$\mathsf{Adv}_{h,\mathcal{E},\mathcal{A}}^{\text{CS}}(\lambda) = \left|\Pr[b = b'] - 1/2\right|.$$

定义 6 (循环安全性). 如果对任意多项式时间敌手$\mathcal{A}$，$\mathsf{Adv}_{g,\mathcal{E},\mathcal{A}}^{\text{CS}}(\lambda)$ 都是可忽略的，则我们称这个基于身份的全同态加密方案$\mathcal{E}$ 关于函数h 是循环安全的。

注意，我们可把$\mathsf{Eval}(pp, id^*, h, \mathsf{Encrypt}(pp, id^*, 0), g(sk_{id^*}))$ 看作是对$g(sk_{id^*})$ 加密产生的一种密文。正是由于这个缘故，我们把这个安全概念称为循环安全性。

4. 基于身份的整数矩阵全同态加密方案

下面给出基于身份的整数矩阵全同态加密方案以及它的安全性证明。

4.1. 方案描述

我们设计的层次型基于身份的整数矩阵全同态加密方案具体如下：

Setup$(1^\lambda, 1^L)$**:** 给定安全参数λ 和电路的最大深度L，执行：

(1) 设定参数n、m、r、σ、p、q 和α，且q 为2 的幂。令$\ell = \log q + 1$，$N = (2m + r) \cdot \ell$。

(2) 定义身份空间$\mathcal{ID}=\mathbb{Z}_q^n$、消息空间$\mathcal{M}=\mathbb{Z}_q^{r\times r}$ 和密文空间$\mathcal{C}=\mathbb{Z}_q^{(2m+r)\times N}$。

(3) 调用算法$\mathsf{TrapGen}(n,q)$ 产生一个矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和$\Lambda^{\perp}(\boldsymbol{A})$ 的一组基$\boldsymbol{T_A}\in\mathbb{Z}^{m\times m}$，且满足$\|\widetilde{\boldsymbol{T_A}}\|\leq O(\sqrt{n\log q})$。

(4) 随机选择矩阵$\boldsymbol{A}_1,\boldsymbol{B}\xleftarrow{\$}\mathbb{Z}_q^{n\times m}$，随机选择矩阵$\boldsymbol{U}\xleftarrow{\$}\mathbb{Z}_q^{n\times r}$。

(5) 输出系统参数$pp=\{\mathcal{ID},\mathcal{M},\mathcal{C},\boldsymbol{A},\boldsymbol{A}_1,\boldsymbol{B},\boldsymbol{U}\}$ 和主密钥$msk=\boldsymbol{T_A}$。

KeyGen(pp,msk,id)**:** 给定系统参数pp、主密钥msk 和身份$id\in\mathbb{Z}_q^n$，执行：

(1) KGC 调用算法$\mathsf{SampleLeft}(\boldsymbol{A},\boldsymbol{A}_1+H(id)\boldsymbol{B},\boldsymbol{T_A},\boldsymbol{U},\sigma)$ 产生$\boldsymbol{S}'_{id}\in\mathbb{Z}^{2m\times r}$。这里$H:\mathbb{Z}_q^n\to\mathbb{Z}_q^{n\times n}$ 为满秩差分映射，其定义参见 [8]。令$\boldsymbol{F}'_{id}=(\boldsymbol{A}|\boldsymbol{A}_1+H(id)\boldsymbol{B})\in\mathbb{Z}_q^{n\times 2m}$，则$\boldsymbol{F}'_{id}\cdot\boldsymbol{S}'_{id}=\boldsymbol{U}\mod q$。

(2) KGC 设定$\boldsymbol{S}_{id}=\begin{pmatrix}\boldsymbol{I}_r\\-\boldsymbol{S}'_{id}\end{pmatrix}\in\mathbb{Z}^{(2m+r)\times r}$，并把它作为私钥$sk_{id}$ 发送给用户id。

(3) 用户id 设置$\boldsymbol{F}_{id}=(\boldsymbol{U}|\boldsymbol{F}'_{id})=(\boldsymbol{U}|\boldsymbol{A}|\boldsymbol{A}_1+H(id)\boldsymbol{B})\in\mathbb{Z}_q^{n\times(2m+r)}$。

(4) 用户id 对每一$(i,j)\in[r]\times[r]$，设置矩阵$\boldsymbol{W}_{i,j}\in\{0,1\}^{r\times r}$，它只在第$i$ 行第j 列为1，在其他位置皆为0。对$\boldsymbol{W}_{i,j}\in\{0,1\}^{r\times r}(i,j\in[r])$，随机选择矩阵$\boldsymbol{V}_{i,j}\xleftarrow{\$}\mathbb{Z}_q^{n\times N}$，随机选择矩阵$\boldsymbol{R}_{i,j}\xleftarrow{\$}\{-1,1\}^{m\times m}$，选择误差矩阵$\boldsymbol{X}_{i,j}\xleftarrow{\$}D_{\mathbb{Z},\alpha q}^{r\times N}$ 和$\boldsymbol{Y}_{i,j}\xleftarrow{\$}D_{\mathbb{Z},\alpha q}^{m\times N}$，设置$\boldsymbol{Z}_{i,j}=\begin{pmatrix}\boldsymbol{X}_{i,j}\\\boldsymbol{Y}_{i,j}\\\boldsymbol{R}_{i,j}^{\mathsf{T}}\cdot\boldsymbol{Y}_{i,j}\end{pmatrix}\in\mathbb{Z}^{(2m+r)\times N}$，设置

$$\boldsymbol{P}_{i,j}=\boldsymbol{F}_{id}^{\mathsf{T}}\boldsymbol{V}_{i,j}+\boldsymbol{Z}_{i,j}+\begin{pmatrix}\boldsymbol{W}_{i,j}\boldsymbol{S}_{id}^{\mathsf{T}}\\\boldsymbol{0}\end{pmatrix}\boldsymbol{G}\in\mathbb{Z}_q^{(2m+r)\times N}.$$

这里$\boldsymbol{G}=\boldsymbol{I}_{2m+r}\otimes\boldsymbol{g}^{\mathsf{T}}\in\mathbb{Z}_q^{(2m+r)\times N}$，其中$\boldsymbol{g}=(1,\ldots,2^{\ell-2},2^{\ell-1})^{\mathsf{T}}\in\mathbb{Z}_q^{\ell}$。

(5) 用户id 设置公钥$pk_{id}=\{id,\{\boldsymbol{P}_{i,j}\}_{i,j\in[r]}\}$，它除身份$id$ 外还包括$\{\boldsymbol{P}_{i,j}\}_{i,j\in[r]}$。

Encrypt$(pp,id,\boldsymbol{M})$**:** 给定系统参数pp、用户id 的公钥pk_{id} 和消息$\boldsymbol{M}\in\mathbb{Z}_q^{r\times r}$，且$\|\boldsymbol{M}\|_{\infty}\leq p$，执行：

(1) 设置$\boldsymbol{F}_{id}=(\boldsymbol{U}|\boldsymbol{F}'_{id})=(\boldsymbol{U}|\boldsymbol{A}|\boldsymbol{A}_1+H(id)\boldsymbol{B})\in\mathbb{Z}_q^{n\times(2m+r)}$。

(2) 随机选择矩阵$\boldsymbol{V}\xleftarrow{\$}\mathbb{Z}_q^{n\times N}$，随机选择矩阵$\boldsymbol{R}\xleftarrow{\$}\{-1,1\}^{m\times m}$，选择误差矩阵$\boldsymbol{X}\xleftarrow{\$}D_{\mathbb{Z},\alpha q}^{r\times N}$ 和$\boldsymbol{Y}\xleftarrow{\$}D_{\mathbb{Z},\alpha q}^{m\times N}$，设置$\boldsymbol{Z}=\begin{pmatrix}\boldsymbol{X}\\\boldsymbol{Y}\\\boldsymbol{R}^{\mathsf{T}}\cdot\boldsymbol{Y}\end{pmatrix}\in\mathbb{Z}^{(2m+r)\times N}$，设置

$$\boldsymbol{C}=\boldsymbol{F}_{id}^{\mathsf{T}}\boldsymbol{V}+\boldsymbol{Z}+\sum\nolimits_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{P}_{i,j}\in\mathbb{Z}_q^{(2m+r)\times N},$$

其中$\mu_{i,j}\in\mathbb{Z}_q$ 为矩阵$\boldsymbol{M}\in\mathbb{Z}_q^{r\times r}$ 的第i 行第j 列元素。

(3) 输出密文$\boldsymbol{C}\in\mathbb{Z}_q^{(2m+r)\times N}$。

Decrypt$(pp,sk_{id},\boldsymbol{C})$**:** 给定系统参数$pp$、私钥$sk_{id}$ 和密文$\boldsymbol{C}\in\mathbb{Z}_q^{(2m+r)\times N}$，执行：

(1) 对$i,j=1,\ldots,r$，执行

(a) 令$\boldsymbol{s}_i$ 为私钥$\boldsymbol{S}_{id}=\begin{pmatrix}\boldsymbol{I}_r\\-\boldsymbol{S}'_{id}\end{pmatrix}\in\mathbb{Z}^{(2m+r)\times r}$ 的第i 列。对$k=1,\ldots,\ell-1$，令$\boldsymbol{c}_{j\ell-k}$ 为密

文$\boldsymbol{C} \in \mathbb{Z}_q^{(2m+r)\times N}$ 的第$j\ell - k$ 列。计算

$$\gamma_{i,j,k-1} = \begin{cases} \left\lfloor \frac{\boldsymbol{s}_i^{\mathsf{T}} \cdot \boldsymbol{c}_{j\ell-k} \mod q}{2^{\ell-2}} \right\rceil \in \{0,1\}, & k=1 \\ \left\lfloor \frac{\boldsymbol{s}_i^{\mathsf{T}} \cdot \boldsymbol{c}_{j\ell-k} - (\sum_{\phi\in[k-1]} \gamma_{i,j,\phi-1} \cdot 2^{\phi-1}) \cdot 2^{\ell-k-1} \mod q}{2^{\ell-2}} \right\rceil \in \{0,1\}, & k \geq 2. \end{cases}$$

(b) 令$\mu_{i,j} = \sum_{k=1}^{\ell-1} \gamma_{i,j,k-1} \cdot 2^{k-1} \in \mathbb{Z}_q$，其中$\gamma_{i,j,k-1} \in \{0,1\}$。

这里，注意$q = 2^{\ell-1}$。

(2) 输出消息矩阵$\boldsymbol{M} = (\mu_{i,j})_{i,j\in[r]} \in \mathbb{Z}_q^{r\times r}$。

Eval$(pp, id, +, \boldsymbol{C}_1, \boldsymbol{C}_2)$**:** 对身份$id$ 下的两个密文$\boldsymbol{C}_1, \boldsymbol{C}_2 \in \mathbb{Z}_q^{(2m+r)\times N}$，同态加法定义为

$$\boldsymbol{C}_+ = \boldsymbol{C}_1 + \boldsymbol{C}_2 \in \mathbb{Z}_q^{(2m+r)\times N}.$$

Eval$(pp, id, \times, \boldsymbol{C}_1, \boldsymbol{C}_2)$**:** 对身份$id$ 下的两个密文$\boldsymbol{C}_1, \boldsymbol{C}_2 \in \mathbb{Z}_q^{(2m+r)\times N}$，同态乘法定义为

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

4.2. 正确性分析

现在我们分析一下所提出的基于身份的全同态加密方案的正确性。

引理 6. 给定身份$id \in \mathbb{Z}_q^n$、消息矩阵$\boldsymbol{M} \in \mathbb{Z}_q^{r\times r}$ 和密文$\boldsymbol{C} \in \mathbb{Z}_q^{(2m+r)\times N}$，且$\boldsymbol{C}$ 的误差矩阵为$\boldsymbol{E} \in \mathbb{Z}_q^{r\times N}$，如果$\boldsymbol{E} = \boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C} - \boldsymbol{M}\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G} \in \mathbb{Z}_q^{r\times N}$，且满足$\|\boldsymbol{E}\| < q/4$，则$\mathsf{Decrypt}(pp, sk_{id}, \boldsymbol{C}) = \boldsymbol{M}$。

证明. 对密文$\boldsymbol{C} \in \mathbb{Z}_q^{(2m+r)\times N}$，由于

$$\begin{aligned}
&\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C} = \boldsymbol{E} + \boldsymbol{M}\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G} \\
&= \boldsymbol{E} + \boldsymbol{M}\begin{pmatrix} \boldsymbol{I}_r \\ -\boldsymbol{S}'_{id} \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} \boldsymbol{I}_r \otimes \boldsymbol{g}^{\mathsf{T}} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I}_{2m} \otimes \boldsymbol{g}^{\mathsf{T}} \end{pmatrix} \\
&= \boldsymbol{E} + \left(\boldsymbol{M}\left(\boldsymbol{I}_r \otimes \boldsymbol{g}^{\mathsf{T}}\right) \,\middle|\, -\boldsymbol{M}\boldsymbol{S}'_{id}\left(\boldsymbol{I}_{2m} \otimes \boldsymbol{g}^{\mathsf{T}}\right) \right) \\
&= \boldsymbol{E} + \left(\begin{pmatrix} \mu_{1,1} & \cdots & \mu_{1,r} \\ \vdots & \ddots & \vdots \\ \mu_{r,1} & \cdots & \mu_{r,r} \end{pmatrix} \begin{pmatrix} 1,\ldots,2^{\ell-1} & & \\ & \ddots & \\ & & 1,\ldots,2^{\ell-1} \end{pmatrix} \,\middle|\, -\boldsymbol{M}\boldsymbol{S}'_{id}\left(\boldsymbol{I}_{2m} \otimes \boldsymbol{g}^{\mathsf{T}}\right) \right) \\
&= \boldsymbol{E} + \left(\begin{pmatrix} \mu_{1,1}\cdot 1,\ldots,\mu_{1,1}\cdot 2^{\ell-1} & \cdots & \mu_{1,r}\cdot 1,\ldots,\mu_{1,r}\cdot 2^{\ell-1} \\ \vdots & \ddots & \vdots \\ \mu_{r,1}\cdot 1,\ldots,\mu_{r,1}\cdot 2^{\ell-1} & \cdots & \mu_{r,r}\cdot 1,\ldots,\mu_{r,r}\cdot 2^{\ell-1} \end{pmatrix} \,\middle|\, -\boldsymbol{M}\boldsymbol{S}'_{id}\left(\boldsymbol{I}_{2m} \otimes \boldsymbol{g}^{\mathsf{T}}\right) \right),
\end{aligned}$$

又由于$2^{\ell-2} = q/2$，$\|\boldsymbol{E}\| < q/4$。因此$\boldsymbol{C}$ 可解密得到消息矩阵$\boldsymbol{M} \in \mathbb{Z}_q^{r\times r}$。 □

对密文$\boldsymbol{C}\leftarrow\mathsf{Encrypt}(pp,id,\boldsymbol{M})$，我们注意到

$$\begin{aligned}\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}&=\boldsymbol{S}_{id}^{\mathsf{T}}\Big(\boldsymbol{F}_{id}^{\mathsf{T}}\boldsymbol{V}+\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{P}_{i,j}\Big)\\&=\big(\boldsymbol{F}_{id}\boldsymbol{S}_{id}\big)^{\mathsf{T}}\boldsymbol{V}+\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}+\boldsymbol{S}_{id}^{\mathsf{T}}\Big(\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{P}_{i,j}\Big)\\&=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}+\boldsymbol{S}_{id}^{\mathsf{T}}\Big(\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{P}_{i,j}\Big)\\&=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{P}_{i,j}\\&=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{S}_{id}^{\mathsf{T}}\left(\boldsymbol{F}_{id}^{\mathsf{T}}\boldsymbol{V}_{i,j}+\boldsymbol{Z}_{i,j}+\begin{pmatrix}\boldsymbol{W}_{i,j}\boldsymbol{S}_{id}^{\mathsf{T}}\\\boldsymbol{0}\end{pmatrix}\boldsymbol{G}\right)\\&=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\left(\big(\boldsymbol{F}_{id}\boldsymbol{S}_{id}\big)^{\mathsf{T}}\boldsymbol{V}_{i,j}+\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}_{i,j}+\boldsymbol{S}_{id}^{\mathsf{T}}\begin{pmatrix}\boldsymbol{W}_{i,j}\boldsymbol{S}_{id}^{\mathsf{T}}\\\boldsymbol{0}\end{pmatrix}\boldsymbol{G}\right)\\&=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\big(\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}_{i,j}+\boldsymbol{W}_{i,j}\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\big)\\&=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{Z}_{i,j}+\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{W}_{i,j}\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\\&=\boldsymbol{S}_{id}^{\mathsf{T}}\Big(\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{Z}_{i,j}\Big)+\Big(\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{W}_{i,j}\Big)\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\\&=\boldsymbol{S}_{id}^{\mathsf{T}}\Big(\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{Z}_{i,j}\Big)+\boldsymbol{M}\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}.\end{aligned}$$

于是，误差矩阵$\boldsymbol{E}=\boldsymbol{S}_{id}^{\mathsf{T}}\big(\boldsymbol{Z}+\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{Z}_{i,j}\big)$，并且

$$\begin{aligned}\|\boldsymbol{E}\|&=\Big\|\boldsymbol{S}_{id}^{\mathsf{T}}\Big(\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{Z}_{i,j}\Big)\Big\|\\&\le\sqrt{r}\cdot\|\boldsymbol{S}_{id}\|\cdot\Big\|\boldsymbol{Z}+\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{Z}_{i,j}\Big\|\\&\le\sqrt{r}\cdot\big(\|\boldsymbol{I}_r\|+\|\boldsymbol{S}'_{id}\|\big)\cdot\Big(\|\boldsymbol{Z}\|+\Big\|\textstyle\sum_{i,j\in[r]}\mu_{i,j}\cdot\boldsymbol{Z}_{i,j}\Big\|\Big)\\&\le\sqrt{r}\cdot\big(\|\boldsymbol{I}_r\|+\|\boldsymbol{S}'_{id}\|\big)\cdot\Big(\|\boldsymbol{Z}\|+\textstyle\sum_{i,j\in[r]}|\mu_{i,j}|\cdot\|\boldsymbol{Z}_{i,j}\|\Big)\\&\le\sqrt{r}\cdot\big(\|\boldsymbol{I}_r\|+\|\boldsymbol{S}'_{id}\|\big)\cdot\Big(\|\boldsymbol{Z}\|+\textstyle\sum_{i,j\in[r]}p\cdot\|\boldsymbol{Z}_{i,j}\|\Big)\\&\le\sqrt{r}\cdot\big(\|\boldsymbol{I}_r\|+\|\boldsymbol{S}'_{id}\|\big)\cdot\Big(\|\boldsymbol{Z}\|+p\cdot\textstyle\sum_{i,j\in[r]}\|\boldsymbol{Z}_{i,j}\|\Big)\\&\le\sqrt{r}(1+\sigma\sqrt{2m})\cdot(1+p\cdot r^2)\cdot\|\boldsymbol{Z}\|\\&\le\sqrt{r}(1+\sigma\sqrt{2m})(1+p\cdot r^2)(\|\boldsymbol{X}\|+\|\boldsymbol{Y}\|+\|\boldsymbol{R}^{\mathsf{T}}\cdot\boldsymbol{Y}\|)\\&\le\sqrt{r}(1+\sigma\sqrt{2m})(1+p\cdot r^2)(\alpha q\sqrt{r}+\alpha q\sqrt{m}+\sqrt{m}\cdot\|\boldsymbol{R}\|\cdot\|\boldsymbol{Y}\|)\\&\le\sqrt{r}(1+\sigma\sqrt{2m})(1+p\cdot r^2)(\alpha q\sqrt{r}+\alpha q\sqrt{m}+\sqrt{m}\cdot\sqrt{m}\cdot\alpha q\sqrt{m})\\&=\sqrt{r}(1+\sigma\sqrt{2m})(1+p\cdot r^2)(\sqrt{r}+\sqrt{m}+m\sqrt{m})\alpha q.\end{aligned}$$

其中因为$\|\boldsymbol{M}\|_\infty\le p$，即$|\mu_{i,j}|\le p$。我们令$B=\sqrt{r}(1+\sigma\sqrt{2m})(1+p\cdot r^2)(\sqrt{r}+\sqrt{m}+m\sqrt{m})\alpha q$。

对密文$\boldsymbol{C}_+\leftarrow\mathsf{Eval}(pp,id,+,\boldsymbol{C}_1,\boldsymbol{C}_2)$和$\boldsymbol{C}_\times\leftarrow\mathsf{Eval}(pp,id,\times,\boldsymbol{C}_1,\boldsymbol{C}_2)$，其中$\boldsymbol{C}_1\in\mathbb{Z}_q^{(2m+r)\times N}$和$\boldsymbol{C}_2\in\mathbb{Z}_q^{(2m+r)\times N}$，它们的误差矩阵为$\boldsymbol{E}_1=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_1-\boldsymbol{M}_1\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\in\mathbb{Z}_q^{r\times N}$和$\boldsymbol{E}_2=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_2-\boldsymbol{M}_2\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\in$

$\mathbb{Z}_q^{r\times N}$，且满足$\|\boldsymbol{E}_1\|<q/4$ 和$\|\boldsymbol{E}_2\|<q/4$，我们注意到

$$\begin{aligned}\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_+ &= \boldsymbol{S}_{id}^{\mathsf{T}}(\boldsymbol{C}_1+\boldsymbol{C}_2)=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_1+\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_2\\ &= (\boldsymbol{E}_1+\boldsymbol{E}_2)+(\boldsymbol{M}_1+\boldsymbol{M}_2)\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\,,\\ \boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_\times &= \boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)=\big(\boldsymbol{E}_1+\boldsymbol{M}_1\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\big)\boldsymbol{G}^{-1}(\boldsymbol{C}_2)\\ &= \boldsymbol{E}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)+\boldsymbol{M}_1\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\boldsymbol{G}^{-1}(\boldsymbol{C}_2)=\boldsymbol{E}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)+\boldsymbol{M}_1\boldsymbol{S}_{id}^{\mathsf{T}}(\boldsymbol{C}_2)\\ &= \boldsymbol{E}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)+\boldsymbol{M}_1\big(\boldsymbol{E}_2+\boldsymbol{M}_2\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\big)=\big(\boldsymbol{E}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)+\boldsymbol{M}_1\boldsymbol{E}_2\big)+\boldsymbol{M}_1\boldsymbol{M}_2\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\,.\end{aligned}$$

于是，误差矩阵$\boldsymbol{E}_+=\boldsymbol{E}_1+\boldsymbol{E}_2$ 和$\boldsymbol{E}_\times=\boldsymbol{E}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)+\boldsymbol{M}_1\boldsymbol{E}_2$，并且

$$\begin{aligned}\|\boldsymbol{E}_+\| &= \|\boldsymbol{E}_1+\boldsymbol{E}_2\|\le\|\boldsymbol{E}_1\|+\|\boldsymbol{E}_2\|\,,\\ \|\boldsymbol{E}_\times\| &= \|\boldsymbol{E}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)+\boldsymbol{M}_1\boldsymbol{E}_2\|\le\|\boldsymbol{E}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)\|+\|\boldsymbol{M}_1\boldsymbol{E}_2\|\\ &\le \sqrt{r}\cdot\|\boldsymbol{E}_1^{\mathsf{T}}\|\cdot\|\boldsymbol{G}^{-1}(\boldsymbol{C}_2)\|+\sqrt{r}\cdot\|\boldsymbol{M}_1^{\mathsf{T}}\|\cdot\|\boldsymbol{E}_2\|\\ &\le \sqrt{r}\cdot\sqrt{N}\cdot\|\boldsymbol{E}_1\|\cdot\|\boldsymbol{G}^{-1}(\boldsymbol{C}_2)\|+\sqrt{r}\cdot\sqrt{r}\cdot\|\boldsymbol{M}_1^{\mathsf{T}}\|_\infty\cdot\|\boldsymbol{E}_2\|\\ &\le \sqrt{r}\cdot\sqrt{N}\cdot\|\boldsymbol{E}_1\|\cdot\sqrt{N}+\sqrt{r}\cdot\sqrt{r}\cdot\|\boldsymbol{M}_1\|_\infty\cdot\|\boldsymbol{E}_2\|\\ &= \sqrt{r}N\cdot\|\boldsymbol{E}_1\|+r\cdot\|\boldsymbol{M}_1\|_\infty\cdot\|\boldsymbol{E}_2\|\\ &\le \sqrt{r}N\cdot\|\boldsymbol{E}_1\|+rp\cdot\|\boldsymbol{E}_2\|\,.\end{aligned}$$

这里，$\|\boldsymbol{M}_1\|_\infty\le p$。

对密文$\boldsymbol{C}_f\leftarrow\mathsf{Eval}(pp,id,f,\boldsymbol{C}_1,\ldots,\boldsymbol{C}_\kappa)$，其中算术电路$f:(\mathbb{Z}_q^{r\times r})^\kappa\to\mathbb{Z}_q^{r\times r}$，且电路深度$d\le L$，通过迭代应用同态加法和乘法，我们可以计算得到$\boldsymbol{C}_f\in\mathbb{Z}_q^{(2m+r)\times N}$。显然，$\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_f=\boldsymbol{E}_f+f(\boldsymbol{M}_1,\ldots,\boldsymbol{M}_\kappa)\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}$。于是$\boldsymbol{C}_f$ 的误差矩阵$\boldsymbol{E}_f=\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{C}_f-f(\boldsymbol{M}_1,\ldots,\boldsymbol{M}_\kappa)\boldsymbol{S}_{id}^{\mathsf{T}}\boldsymbol{G}\in\mathbb{Z}_q^{r\times N}$。如果$\boldsymbol{C}_1,\ldots,\boldsymbol{C}_\kappa$ 的误差矩阵满足$\|\boldsymbol{E}_1\|,\ldots,\|\boldsymbol{E}_\kappa\|\le B$，则$\|\boldsymbol{E}_f\|\le(\sqrt{r}N+rp)^dB\le(\sqrt{r}N+rp)^LB$。根据引理 6，如若$(\sqrt{r}N+rp)^LB<q/4$，我们可解密$\boldsymbol{C}_f$ 得到消息矩阵$f(\boldsymbol{M}_1,\ldots,\boldsymbol{M}_\kappa)$。

4.3. 安全性证明

接下来，我们在标准模型下证明所提出的基于身份的整数矩阵全同态加密方案满足 INDr-sID-CPA 安全性。定义h 是从$\mathbb{Z}^{(2m+r)\times r}$ 到$\mathbb{Z}_q^{(2m+r)\times N}$ 的函数，且对$\boldsymbol{S}_{id}\in\mathbb{Z}^{(2m+r)\times r}$，$h(\boldsymbol{S}_{id})=\begin{pmatrix}\boldsymbol{W}_{i,j}\boldsymbol{S}_{id}^{\mathsf{T}}\\ \boldsymbol{0}\end{pmatrix}\boldsymbol{G}\in\mathbb{Z}_q^{(2m+r)\times N}$，其中$\boldsymbol{W}_{i,j}\in\{0,1\}^{r\times r}$。

定理 1. 假定第 4.1 节提出的基于身份的整数矩阵全同态加密方案关于函数h 是循环安全的。那么$\mathsf{LWE}_{n,q,D_{\mathbb{Z},\alpha q}}$ 问题若是困难的，第 4.1 节提出的基于身份的整数矩阵全同态加密方案就是 INDr-sID-CPA 安全的。具体地，假设存在多项式时间 INDr-sID-CPA 敌手$\mathcal{A}$，它以优势$\mathsf{Adv}_{\mathcal{E},\mathcal{A}}^{\text{INDr-sID-CPA}}(\lambda)$ 攻破第 4.1 节提出的基于身份的整数矩阵全同态加密方案，则存在多项式时间算法$\mathcal{B}$，它以优势$\mathsf{Adv}_{\text{LWE},\mathcal{B}}(\lambda)$ 解决$\mathsf{LWE}_{n,q,D_{\mathbb{Z},\alpha q}}$ 问题，并且

$$\mathsf{Adv}_{\mathcal{E},\mathcal{A}}^{\text{INDr-sID-CPA}}(\lambda)\le(r^2+1)\cdot\mathsf{Adv}_{\text{LWE},\mathcal{B}}(\lambda)+\mathsf{negl}(\lambda)\,.$$

证明. 我们通过一个游戏序列证明这个定理。令X_i 表示敌手在游戏Game_i 中获胜，即表示事件$b=b'$。

Game_0：它是敌手$\mathcal{A}$ 和挑战者之间的 INDr-sID-CPA 游戏。由定义 5 可知

$$\mathsf{Adv}_{\mathcal{E},\mathcal{A}}^{\text{INDr-sID-CPA}}(\lambda)=\left|\Pr[X_0]-1/2\right|.$$

Game_1：与Game_0 相比，挑战者修改了系统参数的生成。具体如下：挑战者在设置阶段随机选择$\boldsymbol{R}^* \xleftarrow{\$} \{-1,1\}^{m\times m}$，令$\boldsymbol{A}_1=\boldsymbol{A}\boldsymbol{R}^*-H(id^*)\boldsymbol{B}$，其中$id^*$ 是$\mathcal{A}$ 在初始阶段确定的目标身份。我们注意，在挑战阶段挑战者利用这里确定的$\boldsymbol{R}^*$ 生成挑战密文$\boldsymbol{C}^*$。由剩余哈希引理 [19] 可知，$\boldsymbol{A}_1$ 统计接近于均匀分布。于是Game_0 和Game_1 中的$\boldsymbol{A}_1$ 是统计接近的。因此

$$\left|\Pr[X_0]-|\Pr[X_1]\right|\leq \mathsf{negl}(\lambda).$$

Game_2：与Game_1 相比，挑战者修改了系统参数的生成和对私钥询问的回答。具体如下：

(1) 在设置阶段，挑战者随机选择矩阵$\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$。

(2) 在设置阶段，挑战者调用算法$\mathsf{TrapGen}(n,q)$ 生成矩阵$\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$ 和$\Lambda^{\perp}(\boldsymbol{B})$ 的一组基$\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}^{m\times m}$，且满足$\|\widetilde{\boldsymbol{T}_{\boldsymbol{B}}}\|\leq O(\sqrt{n\log q})$。

(3) 在阶段 1 和阶段 2，挑战者利用陷门$\boldsymbol{T}_{\boldsymbol{B}}$ 回答私钥询问$id\neq id^*$。因为$\boldsymbol{F}'_{id}=\left(\boldsymbol{A}|\boldsymbol{A}_1+H(id)\boldsymbol{B}\right)=\left(\boldsymbol{A}|\boldsymbol{A}\boldsymbol{R}^*+(H(id)-H(id^*))\boldsymbol{B}\right)\in\mathbb{Z}_q^{n\times 2m}$，于是挑战者调用算法$\mathsf{SampleRight}(\boldsymbol{A},(H(id)-H(id^*))\boldsymbol{B},\boldsymbol{R}^*,\boldsymbol{T}_{\boldsymbol{B}},\boldsymbol{U},\sigma)$ 生成矩阵$\boldsymbol{S}'_{id}\in\mathbb{Z}^{2m\times r}$，设定$\boldsymbol{S}_{id}=\begin{pmatrix}\boldsymbol{I}_r\\-\boldsymbol{S}'_{id}\end{pmatrix}\in\mathbb{Z}^{(2m+r)\times r}$，并把它作为私钥$sk_{id}$ 发送给$\mathcal{A}$。高斯参数σ 因为设置得足够大，根据引理 2 和引理 3 可知，Game_1 与Game_2 中的$\boldsymbol{S}'_{id}$ 是统计接近的。

鉴于Game_1 与Game_2 中的系统参数和对私钥询问的回答都是统计接近的，故

$$\left|\Pr[X_1]-|\Pr[X_2]\right|\leq \mathsf{negl}(\lambda).$$

Game_3：相比Game_2，它修改了公钥$\{\boldsymbol{P}^*_{i,j}\}_{i,j\in[r]}$ 的生成，具体如下：设置$\boldsymbol{P}^*_{i,j}=\boldsymbol{F}_{id^*}^{\mathsf{T}}\boldsymbol{V}_{i,j}+\boldsymbol{Z}_{i,j}\in\mathbb{Z}_q^{(2m+r)\times N}$。而在$\mathsf{Game}_2$ 中，$\boldsymbol{P}^*_{i,j}=\boldsymbol{F}_{id^*}^{\mathsf{T}}\boldsymbol{V}_{i,j}+\boldsymbol{Z}_{i,j}+\begin{pmatrix}\boldsymbol{W}_{i,j}\boldsymbol{S}_{id^*}^{\mathsf{T}}\\\boldsymbol{0}\end{pmatrix}\boldsymbol{G}\in\mathbb{Z}_q^{(2m+r)\times N}$。由于所提出的方案关于$g(\boldsymbol{S}_{id^*})=\begin{pmatrix}\boldsymbol{W}_{i,j}\boldsymbol{S}_{id^*}^{\mathsf{T}}\\\boldsymbol{0}\end{pmatrix}\boldsymbol{G}\in\mathbb{Z}_q^{(2m+r)\times N}$ 是循环安全的，因此

$$\left|\Pr[X_2]-\Pr[X_3]\right|\leq \mathsf{negl}(\lambda).$$

Game_4：相比Game_3，它又修改了公钥$\{\boldsymbol{P}^*_{i,j}\}_{i,j\in[r]}$ 的生成，具体如下：随机选择$\boldsymbol{P}^*_{i,j}\xleftarrow{\$}\mathbb{Z}_q^{(2m+r)\times N}$。可以看出，$\mathcal{A}$ 若能区分Game_3 和Game_4，我们就可以利用$\mathcal{A}$ 解决$\mathsf{LWE}_{n,q,D_{\mathbb{Z},\alpha q}}$ 问题。故而

$$\left|\Pr[X_3]-\Pr[X_4]\right|\leq r^2\cdot\mathsf{Adv}_{\text{LWE},\mathcal{B}}(\lambda).$$

Game_5：相比Game_4，挑战者修改了挑战密文$\boldsymbol{C}^*$ 的生成。具体如下：在挑战阶段，当$b=0$ 时，挑战者随机选择$\boldsymbol{C}^*\xleftarrow{\$}\mathbb{Z}_q^{(2m+r)\times N}$。而在$\mathsf{Game}_4$ 中，当$b=0$ 时，$\boldsymbol{C}^*=\boldsymbol{F}_{id^*}^{\mathsf{T}}\boldsymbol{V}+\boldsymbol{Z}+$

$\sum_{i,j\in[r]}\mu^*_{i,j}\cdot\boldsymbol{P}^*_{i,j}\in\mathbb{Z}_q^{(2m+r)\times N}$。可以看出，$\mathcal{A}$ 若能区分Game_4 和Game_5，我们就可以利用$\mathcal{A}$解决$\mathsf{LWE}_{n,q,D_{\mathbb{Z},\alpha q}}$ 问题。因而

$$\left|\Pr[X_4]-\Pr[X_5]\right|\leq \mathsf{Adv}_{\mathrm{LWE},\mathcal{B}}(\lambda)\,.$$

在Game_5 中，不管b 的值如何，挑战密文都是从密文空间中随机选择的，因此

$$\left|\Pr[X_5]-1/2\right|=0\,.$$

综上，我们得到

$$\begin{aligned}\mathsf{Adv}^{\text{INDr-sID-CPA}}_{\mathcal{E},\mathcal{A}}(\lambda)&=|\Pr[X_0]-1/2|\\&\leq|\Pr[X_1]-1/2|+\mathsf{negl}(\lambda)\\&\leq|\Pr[X_2]-1/2|+\mathsf{negl}(\lambda)\\&\leq|\Pr[X_3]-1/2|+\mathsf{negl}(\lambda)\\&\leq|\Pr[X_4]-1/2|+r^2\cdot\mathsf{Adv}_{\mathrm{LWE},\mathcal{B}}(\lambda)+\mathsf{negl}(\lambda)\\&\leq|\Pr[X_5]-1/2|+(r^2+1)\cdot\mathsf{Adv}_{\mathrm{LWE},\mathcal{B}}(\lambda)+\mathsf{negl}(\lambda)\\&=(r^2+1)\cdot\mathsf{Adv}_{\mathrm{LWE},\mathcal{B}}(\lambda)+\mathsf{negl}(\lambda)\,.\end{aligned}$$

□

4.4. 参数设定

所提出方案的参数需要满足以下要求：

- $m\geq 6n\log q$，以运行$\mathsf{TrapGen}$ 算法；
- $\sigma\geq\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\|\cdot\omega(\sqrt{\log m})$，其中$\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\|\leq O(\sqrt{n\log q})$，以运行$\mathsf{SampleLeft}$ 算法；
- $\sigma\geq\|\widetilde{\boldsymbol{T}_{\boldsymbol{B}}}\|\cdot m\cdot\omega(\sqrt{\log m})$，其中$\|\widetilde{\boldsymbol{T}_{\boldsymbol{B}}}\|\leq O(\sqrt{n\log q})$，以运行$\mathsf{SampleRight}$ 算法；
- $(\sqrt{r}N+rp)^L B<q/4$，其中$B=\sqrt{r}(1+\sigma\sqrt{2m})(1+p\cdot r^2)(\sqrt{r}+\sqrt{m}+m\sqrt{m})\alpha q$，以把$\boldsymbol{C}_f\leftarrow\mathsf{Eval}(pp,id,f,\boldsymbol{C}_1,\ldots,\boldsymbol{C}_\kappa)$ 解密为$f(\boldsymbol{M}_1,\ldots,\boldsymbol{M}_\kappa)$；
- $\alpha>2\sqrt{n}/q$，以把GapSVP 问题归约到LWE 问题。

于是，我们设定参数$(n,m,r,\sigma,p,q,\alpha)$ 如下：

$$\begin{aligned}n&=\Theta(\lambda)\,,\\m&=O(nL\log n)\,,\\r&=\mathsf{poly}(n)\,,\\\sigma&=m^{3/2}\cdot\omega(\sqrt{\log n})\,,\\p&=\mathsf{poly}(n)\,,\end{aligned}$$

$$q = 2^{O(L\log n)},\ \text{且 } q \text{ 为 2 的幂},$$
$$\alpha = \sqrt{m}\cdot 2^{-O(L\log n)}.$$

这里，我们提出了一个层次型基于身份的全同态加密方案，它加密整数矩阵，支持整数矩阵加法和乘法同态运算。

5. 结论

随着云计算、大数据和人工智能等新一代信息技术的快速发展，基于身份的全同态加密引起了人们的广泛关注。本论文提出了一个层次型基于身份的整数矩阵全同态加密方案，并在标准模型下基于LWE 问题证明了它是 INDr-sID-CPA 安全的。迄今为止，人们仅提出了一个基于身份的比特矩阵全同态加密方案 [12]，尚未提出基于身份的整数矩阵全同态加密方案。因此，本论文提出的这个基于身份的全同态加密方案，不仅具有重要的理论意义，而且还将有助于解决云计算、大数据和人工智能等新一代信息技术发展面临的有关安全问题。

参考文献

[1] Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. *Proceedings of the 41st 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. and Garay, J.A., Eds., *Advances in Cryptology—CRYPTO 2013. Lecture Notes in Computer Science*, Vol. 8042, Springer, Berlin, Heidelberg, 75-92. https://doi.org/10.1007/978-3-642-40041-4_5

[3] Smart, N.P. and Vercauteren, F. (2014) Fully Homomorphic Simd Operations. *Designs, Codes and Cryptography*, **71**, 57-81. https://doi.org/10.1007/s10623-012-9720-4

[4] Hiromasa, R., Abe, M. and Okamoto, T. (2016) Packing Messages and Optimizing Bootstrapping in GSW-FHE. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **99**, 73-82. https://doi.org/10.1587/transfun.E99.A.73

[5] Wang, B., Wang, X. and Xue, R. (2018) Leveled FHE with Matrix Message Space. In: Chen, X., Lin, D. and Yung, M., Eds., *Information Security and Cryptology. Inscrypt 2017. Lecture Notes in Computer Science*, Vol. 10726, Springer, Cham, 260-277. https://doi.org/10.1007/978-3-319-75160-3_17

[6] Bai, Y., Shi, X., Wu, W., *et al.* (2020) seIMC: A GSW-Based Secure and Efficient Integer

Matrix Computation Scheme with Implementation. *IEEE Access*, **8**, 98383-98394. https://doi.org/10.1109/ACCESS.2020.2996000

[7] Shamir, A. (1984) Identity-Based Cryptosystems and Signature Schemes. In: Blakley, G.R. and Chaum, D., Eds., *Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science*, Vol. 196, Springer, Berlin, Heidelberg, 47-53. https://doi.org/10.1007/3-540-39568-7_5

[8] Agrawal, S., Boneh, D. and Boyen, X. (2010) Efficient Lattice (H)IBE in the Standard Model. In: Gilbert, H., Ed., *Advances in Cryptology—EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science*, Vol. 6110, Springer, Berlin, Heidelberg, 553-572. https://doi.org/10.1007/978-3-642-13190-5_28

[9] 叶青, 胡明星, 汤永利, 等. 基于 LWE 的高效身份基分级加密方案 [J]. 计算机研究与发展, 2017, 54(10): 2193-2204.

[10] Wang, F., Wang, K. and Li, B. (2015) An Efficient Leveled Identity-Based FHE. In: Qiu, M., Xu, S., Yung, M. and Zhang, H., Eds., *Network and System Security. NSS 2015. Lecture Notes in Computer Science*, Vol. 9048, Springer, Cham, 303-315. https://doi.org/10.1007/978-3-319-25645-0_20

[11] 康元基, 顾纯祥, 郑永辉, 等. 利用特征向量构造基于身份的全同态加密体制 [J]. 软件学报, 2016, 27(6): 1487-1497.

[12] 陈虹, 黄洁, 陈红霖, 等. 身份基矩阵层级全同态加密方案 [J]. 计算机科学与探索, 2020, 14(10): 1702-1711.

[13] Ajtai, M. (1999) Generating Hard Instances of the Short Basis Problem. In: Wiedermann, J., van Emde Boas, P. and Nielsen, M., Eds., *Automata, Languages and Programming. Lecture Notes in Computer Science*, Vol. 1644, Springer, Berlin, Heidelber, 1-9. https://doi.org/10.1007/3-540-48523-6_1

[14] 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

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

[16] Regev, O. (2009) On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, **56**, Article No. 34. https://doi.org/10.1145/1568318.1568324

[17] Peikert, C. (2009) Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem. *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC 2009)*, Bethesda, 31 May 2009-2 June 2009, 333-342. https://doi.org/10.1145/1536414.1536461

[18] Micciancio, D. and Mol, P. (2011) Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions. In: Rogaway, P., Ed., *Advances in Cryptology—CRYPTO 2011. Lecture Notes in Computer Science*, Vol. 6841, Springer, Berlin, Heidelberg, 465-484. https://doi.org/10.1007/978-3-642-22792-9_26

[19] Dodis, Y., Ostrovsky, R., Reyzin, L., *et al.* (2008) Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing*, **38**, 97-139. https://doi.org/10.1137/060651380