

文章编号:1007-5321(2018)01-0125-09

DOI:10.13190/j.jbupt.2017-163

改进的格上基于多身份全同态加密方案

汤永利, 胡明星, 叶青, 秦攀科, 于金霞

(河南理工大学 计算机科学与技术学院, 河南 焦作 454000)

摘要: 针对格上基于多身份的全同态加密方案(mIBFHE)中陷门函数低效的问题,提出一种改进的格上 mIBFHE 方案. 首先利用 MP12 陷门函数结合对偶 Regev 算法构造出一种可转化的基于身份的加密(IBE)方案,并构造出一种支持标准模型下 IBE 方案转化的 Mask 系统;然后基于该系统利用特征向量思想将构造出的 IBE 方案转化为 mIBFHE 方案. 对比分析结果表明,新方案较同类方案在陷门生成和原像采样阶段均有效率提升,且格的维数、密文和运算密文尺寸等明显缩短. 在标准模型下,方案的安全性归约至格上容错学习问题的难解性,并包含严格的安全性证明.

关键词: 格; 基于多身份的加密; 全同态加密; 标准模型; 容错学习问题

中图分类号: TP309

文献标志码: A

Improved Multi-Identity Based Fully Homomorphic Encryption Scheme over Lattices

TANG Yong-li, HU Ming-xing, YE Qing, QIN Pan-ke, YU Jin-xia

(School of Computer Science and Technology, Henan Polytechnic University, Henan Jiaozuo 454000, China)

Abstract: Aiming at low efficiency of trapdoor function in multi-identity based fully homomorphic encryption (mIBFHE) schemes, a new mIBFHE scheme was proposed. Firstly, the MP12 trapdoor function with Dual-Regev algorithm was combined to construct a transformable identity-based encryption (IBE) scheme, and a Mask system which supports to transform IBE scheme presented to mIBFHE scheme under standard model. Then, based on presented Mask system and eigenvector idea, the IBE schemes was transformed to mIBFHE scheme. Comparing with the similar schemes, the efficiency of the scheme is improved in trapdoor generation and preimage sampling stage, and the lattice dimension, the size of ciphertext and evaluated ciphertext, etc. are obviously reduced. The security of the presented scheme strictly is reduced to the hardness of learning with errors problem in the standard model.

Key words: lattices; multi-identity based encryption; fully homomorphic encryption; standard model; learning with errors

基于多身份的全同态加密方案,利用基于身份加密(IBE, identity-based encryption)方案无需公钥证书的特性来解决 FHE(fully homomorphic encryption)

方案公钥尺寸过大的问题,从而更有效地管理密钥,降低密钥和密文的尺寸,为加快全同态加密方案的应用具有重要意义. Gentry 等^[1]利用特征向量

收稿日期:2017-08-14

基金项目:“十三五”国家密码发展基金项目(MMJ20170122);河南省科技厅项目(142300410147);河南省教育厅项目(12A520021, 16A520013);河南理工大学博士基金项目(B2014-044)

作者简介:胡明星(1994—),男,硕士生, E-mail: 18236885186@163.com;叶青(1981—),女,硕士生导师.

思想提出首个基于身份的全同态加密 (IBFHE, identity-based fully homomorphic encryption) 方案. Clear 等^[2]提出一种可自举的 IBFHE 方案,该方案的同态运算具有可任意次计算的优点. 康元基等^[3-4]分别利用任意次分圆环和 NTRU 格的特性提出高效的 IBFHE 方案,但二者均基于随机预言模型. Clear 等^[5]于 Crypto'15 上对 Gentry 等^[1]的工作进行了改进,提出一种基于多身份的全同态加密 (mIBFHE, multi-identity based fully homomorphic encryption) 方案,但该方案是随机预言模型下可证明是安全的. 以上方案的陷门函数过于低效,主要采用的是陷门生成算法^[6-8],因其含有计算复杂的 HNF 和矩阵求逆操作而过于复杂,且所基于的 Gentry 等^[8]的原像采样算法需执行高精度实数的正交化迭代运算,导致原像采样的复杂度过高,不具有实际应用性.

为使格上 mIBFHE 方案更具有实际应用性,必须解决陷门函数低效的问题. 作者针对文献^[5]所述的 mIBFHE 方案,提出一种改进方案. 主要包括: 1) 利用 Micciancio 和 Peikert^[9]于 Eurocrypt'12 上提出的 MP12 陷门函数,结合文献^[10]中的对偶 Regev 算法,构造出一种可转化的基于身份的加密方案; 2) 对文献^[5]中转化机制中的 Mask 系统进行重构,提出一种支持标准模型下 IBE 转化的 Mask 系统; 3) 结合该系统和特征向量的思想将 1) 中提出的 IBE 方案成功转化为 mIBFHE 方案.

1 预备知识

1.1 格的相关定义

定义 1 (格的定义) 设 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m$ 是 \mathbb{R}^n 上 m 个线性无关向量,格 Λ 定义为所有这些向量的整数线性组合,即 $\Lambda = \left\{ \sum_{i=1}^m x_i \mathbf{b}_i : x_i \in \mathbb{Z}, i=1, 2, \dots, m \right\}$, 其中向量组 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m$ 称为格的一组基.

定义 2 (q 元格) 设 $q, n, m \in \mathbb{Z}, A \in \mathbb{Z}_q^{n \times m}$, 且 $\mathbf{u} \in \mathbb{Z}_q^n$, 定义

$$\begin{aligned} \Lambda^\perp(A) &= \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\} \\ \Lambda_u^\perp(A) &= \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{u} \bmod q\} \end{aligned} \quad (1)$$

即所有与矩阵 A 行向量模 q 内积为 0 的 m 维列向量构成格 $\Lambda^\perp(A)$; 格 $\Lambda_u^\perp(A)$ 是格 $\Lambda^\perp(A)$ 的陪集, 满足 $\Lambda_u^\perp(A) = \Lambda^\perp(A) + \mathbf{t}$, 其中 $\mathbf{t} \in \Lambda_u^\perp(A)$.

定义 3 (离散高斯分布) 对任意 $\sigma > 0$, 定义以向量 \mathbf{c} 为中心, σ 为参数的格 Λ 上的离散高斯分

布为

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

其中: $\mathbf{y} \in \Lambda, \rho_{\sigma, \mathbf{c}}(\mathbf{y}) = \exp(-\pi \|\mathbf{y} - \mathbf{c}\|^2 / \sigma^2)$.

1.2 相关算法和困难问题

本文方案构造所基于的 MP12 陷门生成算法和与之对应的 MP12 原像采样算法分别由引理 1 和引理 2 给出; 对偶 Regev 算法的具体描述请参阅文献^[10]; 方案的正确性证明基于引理 1、引理 2、定义 4 和定义 5; 方案的安全性证明基于引理 1、引理 3、引理 4 和定义 4.

引理 1^[10] 设整数 $n \geq 1, q \geq 2$ 和充分大的 $m = O(n \log q)$, $\bar{m} = m - nk, w = nk, k = \lceil \log q \rceil$, 可逆矩阵 $H \in \mathbb{Z}_q^{n \times n}$, 构造公开的矩阵 $G \in \mathbb{Z}_q^{n \times w}$. 选取一个均匀随机矩阵 $\bar{A} \in \mathbb{Z}_q^{n \times \bar{m}}$, 存在概率多项式时间 (PPT, probabilistic polynomial time) 算法 TrapGen $(1^n, q)$, 输出矩阵 $A = [\bar{A} | HG - \bar{A}R] \in \mathbb{Z}_q^{n \times m}$ 和陷门矩阵 $R \in \mathbb{Z}_q^{\bar{m} \times w}$, 陷门尺寸 $s_1(R) \leq \sqrt{m} \omega(\sqrt{\log n})$, 其中 A 在 $\mathbb{Z}_q^{n \times m}$ 上是统计均匀的, R 是矩阵 A 的陷门.

引理 2^[9] 与引理 1 参数相同, 设 $\sigma = s_1(R) \times \omega(\sqrt{\log n})$ 是充分大的高斯参数, 存在概率多项式时间算法 SampleL $(A_{\text{id}}, M, R, \mathbf{0}, \sigma)$, 其中 $M \in \mathbb{Z}_q^{n \times w}$, $A_{\text{id}} = [\bar{A} | H_{\text{id}}G - \bar{A}R] \in \mathbb{Z}_q^{n \times m}$, 输出向量 $\mathbf{e} \in \mathbb{Z}^m$, 且 \mathbf{e} 的分布与 $\mathcal{D}_{A_{\text{id}}^\perp(A_{\text{id}}), \sigma \omega(\sqrt{\log n})}$ 统计不可区分,

$$\Pr[\mathbf{e} \leftarrow \mathcal{D}_{A_{\text{id}}^\perp(A_{\text{id}}), \sigma \omega(\sqrt{\log n})} : \|\mathbf{e}\| > \sigma \sqrt{m}] \leq \text{negl}(n)$$

引理 3^[11] 与引理 1 参数相同, 设 $\sigma = s_1(R) \|\bar{R}\| \omega(\sqrt{\log n})$ 是充分大的高斯参数, 存在 PPT 算法 SampleR $(A, G, T_G, \mathbf{0}, \sigma)$, 输出向量 $\mathbf{e} \in \mathbb{Z}^{m+d}$, 且 \mathbf{e} 的分布与 $\mathcal{D}_{A_{\text{id}}^\perp(A_{\text{id}}), \sigma \omega(\sqrt{\log n})}$ 统计不可区分.

引理 4^[10] 与引理 1 参数相同, 对于除了至多 $2q^{-n}$ 部分的 $A \in \mathbb{Z}_q^{n \times m}$ 和任意高斯参数 $\sigma \geq \omega(\sqrt{\log m})$, 有 $\mathbf{e} \in D_{\mathbb{Z}_q^m, \sigma}$, 其中 $D_{\mathbb{Z}_q^m, \sigma}$ 为离散高斯分布, 所得 $\mathbf{u} = \mathbf{A}\mathbf{e} \bmod q$ 的分布和 \mathbb{Z}_q^n 上的均匀分布是统计不可区分的.

定义 4^[12] 容错学习问题. 设 n 为正整数, q 为素数, 对任意 $0 < \alpha \leq 1/\omega(\sqrt{\log n})$, 定义 Ψ_α 为中心是 0, 标准差是 $\alpha/\sqrt{2\pi}$ 的 $[0, 1)$ 上的正态分布, 对应的 \mathbb{Z}_q 上的离散分布为 $\bar{\Psi}_\alpha$. 设 χ 为 \mathbb{Z}_q 上的容错分布, (\mathbb{Z}_q, n, χ) -LWE 问题实例由未指明的挑战预言机 \mathcal{O} 构成: 预言机 \mathcal{O} 是带噪音的伪随机预言机 \mathcal{O}_s 或者是真随机的预言机 \mathcal{O}_s , 2 种预言机的输出如下.

\mathcal{O}_s : 输出的采样值形式为 $(u_i, v_i) = (u_i, u_i^T s + x_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, 其中 $s \in \mathbb{Z}_q^n$ 是随机均匀且不变的秘密向量;

\mathcal{O}_s : 输出 $\mathbb{Z}_q^n \times \mathbb{Z}_q$ 上的真随机且均匀的采样值.

(\mathbb{Z}_q, n, χ) -LWE 问题允许对挑战预言机 \mathcal{O} 重复查询. 笔者称一个攻击算法 \mathcal{A} 可以解决 (\mathbb{Z}_q, n, χ) -LWE 问题, 如果 $\text{LWE-adv}[\mathcal{A}] = |\Pr[\mathcal{A}^{\mathcal{O}} = 1] - \Pr[\mathcal{A}^{\mathcal{O}_s} = 1]|$ 是不可忽略的, 其中 $\text{LWE-adv}[\mathcal{A}]$ 表示 \mathcal{A} 解决 (\mathbb{Z}_q, n, χ) -LWE 问题的优势.

定义 5^[1] 设整数 $B < q$, 对于分布集合 $\{\chi_n\}_{n \in \mathbb{N}}$, 如果对所有的整数有 $\Pr_{e \leftarrow \chi_n}[\|e\| > B] = \text{negl}(n)$, 则称分布 χ_n 是 B -界分布.

2 方案构造

2.1 符号说明

对文中符号进行说明, 如表 1 所示.

表 1 符号说明

符号	意义
$A^{m \times n}$	m 行 n 列矩阵
A_i	矩阵 A 的第 i 行
u	向量, 默认为列向量形式
u^T	向量 u 的转置
$\ S\ $	向量集合 S 的长度, 等于其中所有向量欧几里得范数的最大值
$\ \tilde{S}\ $	向量集合 S 的 Gram-Schmidt 范数的最大值
$s_1(R)$	矩阵 R 的最大奇异值
\parallel	矩阵或向量的拼接
$\lfloor \cdot \rfloor$	向下取整
$\text{negl}(n)$	n 的可忽略函数: $f(n) < (n^{-c})$, c 为常数
$\text{poly}(n)$	n 的多项式函数: $f(n) = O(n^c)$, c 为常数

2.2 高效的基于身份的加密方案

基于 MP12 陷门函数, 结合对偶 Regev 算法完成格上高效 IBE 方案构造, 其结合的理论依据是: Gentry 等^[10] 于 STOC'08 上提出基于对偶 Regev 算法的格上 IBE 方案, 并指出基于常规 LWE 加密算法构造格上 IBE 方案存在用户公钥指数稀疏的问题; Micciancio 等^[9] 于 Eurocrypt'12 上提出 MP12 陷门函数, 并指出其可提高以往格上 IBE 方案, 但未给出具体方案及思路.

为方便 mIBFHE 方案的构造, 对对偶 Regev 算法进行改造, 结合 MP12 高效陷门函数完成方案构

造. 所构造的方案与同类方案相比, 在不降低方案安全性的前提下, 使格的维数、主私钥尺寸、身份公钥尺寸和密文尺寸均有效缩短 (见 4.1 节效率分析). 方案的基本参数包括: 均匀随机矩阵 $A \in \mathbb{Z}_q^{n \times m}$ 和其陷门矩阵 $R \in \mathbb{Z}_q^{\bar{m} \times w}$, 其中 n 是安全参数, 充分大的 $m = O(n \log q)$, $m' = m + 1$, $\bar{m} = m - nk$, $w = nk$, $k = \lceil \log q \rceil$, 模数 $q = q(n)$; 构造公开的矩阵 $G = I_n \otimes g^T \in \mathbb{Z}_q^{n \times nk}$, 其中 $g^T = [1, 2, 2^2, \dots, 2^{k-1}] \in \mathbb{Z}_q^k$, I_n 为 $n \times n$ 单位矩阵; FRD 函数^[11] $H: \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q^{n \times n}$.

IBE-Setup(1^n): 输入安全参数 n , 选取一个均匀随机矩阵 $\bar{A} \in \mathbb{Z}_q^{n \times \bar{m}}$, 选取一个 n 维均匀随机向量 $u \in \mathbb{Z}_q^n$, 运行引理 1 的 MP12 陷门生成算法 TrapGen($1^n, 1^{\bar{m}}, q, I_n$), 输出矩阵 $A = [\bar{A} | -\bar{A}R] \in \mathbb{Z}_q^{n \times m}$ 和 A 的陷门矩阵 $R \in \mathbb{Z}_q^{\bar{m} \times w}$, 输出系统主公钥 $\text{MPK} = (A, u)$, 主私钥 $\text{MSK} = R$.

IBE-Extract($\text{MPK}, \text{MSK}, \text{id}$): 输入主公钥 MPK 、主私钥 MSK 和用户身份向量 $\text{id} \in \mathbb{Z}_q^n$. 利用 FRD 函数 $H: \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q^{n \times n}$ 将用户身份向量 id 映射为一个可逆矩阵 $H_{\text{id}} \in \mathbb{Z}_q^{n \times n}$, 构造用户身份公钥矩阵为 $A_{\text{id}} = [\bar{A} | H_{\text{id}}G - \bar{A}R] \in \mathbb{Z}_q^{n \times m}$, 设 $A'_{\text{id}} = [u | A_{\text{id}}] \in \mathbb{Z}_q^{n \times m'}$, 运行引理 2 中的 MP12 原像采样算法 SampleL($A_{\text{id}}, R, I_n, u, \sigma$), 输出用户密钥 $e_{\text{id}} \in \mathbb{Z}_q^m$, 重新定义用户密钥为 $s_{\text{id}} = (1, -e_{\text{id}}) \in \mathbb{Z}_q^{m'}$, 满足 $A'_{\text{id}} s_{\text{id}} = 0$.

IBE-Encrypt($\text{MPK}, \text{id}, \mu$): 输入主公钥 MPK 、用户身份向量 $\text{id} \in \mathbb{Z}_q^n$ 和待加密的明文消息 $\mu \in \{0, 1\}$. 设 $\mu \in \mathbb{Z}_q^{m'}$ 是除第一分量是 $\mu \lfloor q/2 \rfloor$ 的 m' 维零向量. 选取均匀随机向量 $s \leftarrow \mathbb{Z}_q^n$, 选取均匀随机矩阵

$$\bar{R} \leftarrow \begin{bmatrix} -1 & 1 \end{bmatrix}^{\bar{m} \times w}, \text{ 计算 } c = s^T A'_{\text{id}} + \mu + \begin{bmatrix} x \\ y \\ \bar{R}^T y \end{bmatrix} \in \mathbb{Z}_q^{m'},$$

其中容错值 $x \leftarrow \mathbb{Z}_q$, 容错向量 $y \leftarrow \mathbb{Z}_q^{\bar{m}}$, 输出密文 $c \in \mathbb{Z}_q^{m'}$.

IBE-Decrypt($\text{MPK}, s_{\text{id}}, c$): 输入主公钥 MPK 、用户密钥 s_{id} 和待解密密文 c . 设 $\delta \leftarrow \langle s_{\text{id}}, c \rangle$, 如果 $\delta < \lfloor q/4 \rfloor$, 输出 1, 否则输出 0.

2.3 支持标准模型下 IBE 转化的 Mask 系统

Clear 等^[5] 提出的转化机制能将满足相应转化条件的 IBE 方案转化为 mIBFHE, 其转化机制要求 IBE 方案满足以下条件:

1) 密文和用户密钥均为向量形式, 且用户密钥向量的第一个分量是 1;

2) 若密文 c 是对消息比特“0”的加密, 则 c 与用户密钥的点积 $\langle s_{id}, c \rangle$ 相对模数 q 是可忽略不计的;

3) 在LWE难题的假设下, 对消息比特“0”的加密密文与 \mathbb{Z}_q 上的均匀向量不可区分;

4) 存在一个正确且安全的Mask系统。

不难看出, 2.2节构造的IBE方案满足前3个条件。事实上, 满足前3个条件可利用Gentry等^[1]构造的转化机制将IBE方案成功转化为IBFHE方案。如果再满足条件4), 则可以利用Clear等的转化机制将IBE转化为mIBFHE方案。

步骤4)中的Mask系统是构造mIBFHE方案的关键机制, 下面对该机制的作用和功能进行举例解释: 假设 C_1 和 C_2 分别是明文 μ_1 和 μ_2 利用身份 id_1 和 id_2 加密得到的密文, 令 v_{id_1} 和 v_{id_2} 分别是身份 id_1 和 id_2 对应的同态解密密钥。则有解密算式 $C_1 v_{id_1} = \mu_1 v_{id_1} + z_1$, $C_2 v_{id_2} = \mu_2 v_{id_2} + z_2$ 成立, 其中 $z_1, z_2 \in \mathbb{Z}_q^N$ 为容错向量。如果想对密文 C_1 和 C_2 进行同态运算, 即将它们输入到同一运算电路 C 中。紧凑性条件要求输出的密文尺寸与参与者数量 D 多项式相关。假设运算密文涉及的参与方为 $D=2$, 则输出的运算结果为 $C' \in \mathbb{Z}_q^{2N \times 2N}$, 那么 C' 的解密结果应为 $\mu' = C(\mu_1, \mu_2)$, 即

$$C' \begin{bmatrix} v_{id_1} \\ v_{id_2} \end{bmatrix} = \mu' \begin{bmatrix} v_{id_1} \\ v_{id_2} \end{bmatrix} + z' \quad (2)$$

其中 $z' \in \mathbb{Z}_q^{2N}$ 为容错向量。可以看出, 输出密文的尺寸与参与者数量 D 呈二次增长关系, 则满足紧凑性条件。这个例子的难题是如何生成 C' , Mask系统可解决该难题。

令 $C'_1 \in \mathbb{Z}_q^{2N \times 2N}$ 为密文 C_1 的膨胀密文, 则

$$C'_1 \begin{bmatrix} v_{id_1} \\ v_{id_2} \end{bmatrix} = \mu_1 \begin{bmatrix} v_{id_1} \\ v_{id_2} \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} \quad (3)$$

其中 $z' \in \mathbb{Z}_q^{2N}$ 为容错向量。将 C' 视为由 2×2 个 $\mathbb{Z}_q^{N \times N}$ 子矩阵构成, 令 i, j 分别表示 C' 行和列, 为满足式(3)的上半部分, 可将 $C'_1(1, 1) \leftarrow C_1$, $C'_1(1, 2) \leftarrow 0$; 为满足式(3)的下半部分, 需利用Mask系统计算矩阵 $X, Y \in \{0, 1\}^{N \times N}$ 以满足

$$X v_{id_1} + Y v_{id_2} = \mu_1 v_{id_2} + z_2 \quad (4)$$

因此, 在参与同态运算时, 利用Mask系统可完成各个参与者的膨胀密文的构造, 进而完成mIBFHE方案的构造。

而Clear等^[5]提出的转化机制所依赖的Mask

系统只针对随机预言模型下的IBE方案。该转换机制利用文献[2]的IBE构造方法, 需依赖随机预言机将用户身份信息哈希成用户公钥, 然后利用数字签名的原理由用户公钥生成用户私钥。针对2.2节构造的标准模型下的IBE方案, 下面给出一种支持标准模型下IBE转化的Mask系统。利用文献[13]中盆景树模型的方法消除方案对随机预言机的依赖, 在系统主公钥矩阵中拼接均匀随机向量, 然后结合文献[9]或文献[13]中的陷门派生算法和文献[10]或文献[9]中的原像采样算法生成用户私钥。

首先给出以下基础操作:

已知 $m' = m + 1$, 令 $\ell_q = \lfloor \log q + 1 \rfloor$, $N = m' \ell_q$, $\eta = n \ell_q$, 对任意的 m' 维向量 a, b , $\text{BitDecomp}(a)$ 表示 N 维向量 $(a_{1,0}, \dots, a_{1,\ell_q-1}, \dots, a_{m',0}, \dots, a_{m',\ell_q-1})$, 其中 $a_{i,j}$ 表示 a_i 分量的第 j 个二进制位, $\text{BitDecomp}^{-1}(a) = \left(\sum 2^j a_{1,j}, \dots, \sum 2^j a_{m',j} \right)$ 是 BitDecomp 的逆运算, $\text{Flatten}(a) = \text{BitDecomp}(\text{BitDecomp}^{-1}(a))$, $\text{Powersof2}(b) = (b_1, 2b_1, \dots, 2^{\ell_q-1} b_1, \dots, b_{m'}, 2b_{m'}, \dots, 2^{\ell_q-1} b_{m'})$, 且有以下等式成立:

$$\begin{aligned} \langle \text{BitDecomp}(a), \text{Powersof2}(b) \rangle &= \langle a, b \rangle \\ \langle a, \text{Powersof2}(b) \rangle &= \langle \text{BitDecomp}^{-1}(a), b \rangle = \\ &= \langle \text{Flatten}(a), \text{Powersof2}(b) \rangle \end{aligned}$$

基于以上基础操作, 所提出的支持标准模型下IBE转化的Mask系统由以下2个算法构成。

1) $\text{GenUnivMask}(\text{MPK}, id, \mu)$: 输入系统主公钥 MPK , 用户身份信息 id 和明文 μ 。选取一个 n 维均匀随机向量 $u \in \mathbb{Z}_q^n$, 利用引理1中的TrapGen算法生成均匀随机矩阵 A , 设用户公钥 $A^{id} \leftarrow u \parallel A \in \mathbb{Z}_q^{n \times m'}$, 对于 $i \in [N]$, 有

如果 $i \leq \ell_q$: 对于 $j \in [\eta - 1]$: 调用2.2节中的IBE加密算法对明文信息 $\mu \cdot 2^i$ 进行加密输出 $b_\eta \in \mathbb{Z}_q^{m'}$, 最后将 b_1^T, \dots, b_η^T 拼接成矩阵 B_i 。

如果 $i > \ell_q$: 选取均匀随机向量 $r \leftarrow \mathbb{Z}_q^n$, 容错向量 $\bar{v}_m' \leftarrow \mathbb{Z}_q^{m'}$, 计算 $c \leftarrow (A^{id})^T r + z' \in \mathbb{Z}_q^{m'}$, $r_2 \leftarrow \text{Powersof2}(r) \in \mathbb{Z}_q^n$ 。对于 $j \in [\eta]$: 选取均匀随机向量 $s \leftarrow \mathbb{Z}_q^n$, 容错向量 $f \leftarrow \mathbb{Z}_q^{m'}$, 设 $\omega_j \leftarrow (r_2, 0, \dots, 0) \in \mathbb{Z}_q^{m'}$, 调用2.2节中的IBE加密算法对 ω_j 进行加密输出 $b_\eta \in \mathbb{Z}_q^{m'}$, b_1^T, \dots, b_η^T 拼接成矩阵 B_i 。令 $d \leftarrow 0 \in \{0, 1\}^N$, $d_i \leftarrow \mu$, 计算 $u_i \leftarrow \text{BitDecomp}^{-1}(d) + \text{Flatten}(c)$ 。

最后, B_1, \dots, B_N 垂直拼接成矩阵 $B \in \mathbb{Z}_q^{(N \times \eta) \times m'}$, u_1^T, \dots, u_N^T 组成矩阵 $U \in \mathbb{Z}_q^{N \times m'}$, 输出 $U =$

(\mathbf{B}, \mathbf{U}) .

2) DeriveMask(MPK, \mathbf{U} , \mathbf{id}'): 输入系统主公钥 MPK, $\mathbf{U} = (\mathbf{B}, \mathbf{U})$ 和任意的用户身份 \mathbf{id}' . 令 $\mathcal{H} = \{H: \{0,1\}^* \rightarrow \mathbb{Z}_q^n\}$ 为一类一般的单向(或抗碰撞)哈希函数, 设 $\mathbf{id}' = \text{BitDecomp}(\mathbf{id}') \in \mathbb{Z}^n$, $1 \leftarrow (0, \dots, 0, 1) \in \mathbb{Z}_q^n$. 在 $j \in [N]$ 区间内: 如果 $j \leq \lfloor \ell \rfloor$, 计算 $\mathbf{x}_j \leftarrow \text{Powersof2}(1)\mathbf{B}_j$, 若 $\ell \leq j \leq [N]$, 计算 $\mathbf{x}_j \leftarrow \text{Powersof2}(H(\mathbf{id}'))\mathbf{B}_j$, $\mathbf{x}_1^T, \dots, \mathbf{x}_N^T$ 垂直拼接成 $\mathbf{X}'_i \in \mathbb{Z}_q^{N \times m'}$, 最后计算 $\mathbf{X} \leftarrow \text{BitDecomp}(\mathbf{X}') \in \{0,1\}^{N \times N}$, $\mathbf{Y} \leftarrow \text{BitDecomp}(\mathbf{U}) \in \{0,1\}^{N \times N}$, 输出 (\mathbf{X}, \mathbf{Y}) .

2.4 基于多身份的全同态加密方案

在 2.2 节高效的基于身份的加密方案和 2.3 节支持标准模型下 IBE 转化的 Mask 系统的基础上, 构造多身份的全同态加密方案相对容易. 基本参数与 2.3 节相同, 方案的具体构造如下.

mIBFHE-Setup(n, L, D): 输入安全参数 n , 系统支持的最大同态运算电路深度 L 和一次同态运算中可支持的不同身份的数量 D . 调用 2.2 节 IBE 方案中的 IBE-Setup(1^n) 算法, 输出系统主公钥 $\text{MPK} = (\mathbf{A}, \mathbf{u})$, 主私钥 $\text{MSK} = \mathbf{R}$.

mIBFHE-KeyGen(MSK, \mathbf{id}): 输入主公钥 $\text{MPK} = (\mathbf{A}, \mathbf{u})$ 和用户身份向量 $\mathbf{id} \in \mathbb{Z}_q^n$, 调用 2.2 节 IBE 方案中的 IBE-Extract(MPK, MSK, \mathbf{id}) 算法, 输出用户密钥 $\mathbf{s}_{\mathbf{id}} = (1, -\mathbf{e}_{\mathbf{id}}) \in \mathbb{Z}^{m'}$.

mIBFHE-Encrypt(MPK, \mathbf{id}, μ): 输入主公钥 $\text{MPK} = (\mathbf{A}, \mathbf{u})$, 用户身份向量 $\mathbf{id} \in \mathbb{Z}_q^n$ 和待加密明文消息 $\mu \in \{0,1\}$, 将 μ 转化为第一分量是 $\mu \lfloor q/2 \rfloor$ 的 m' 维零向量 $\boldsymbol{\mu} \in \mathbb{Z}_q$. 调用 2.3 节的 GenUnivMask(MPK, $\mathbf{id}, \boldsymbol{\mu}$) 算法, 输出 $U \in \{0,1\}^*$. 输出密文 $\mathbf{C} = (\mathbf{id}, \text{type} = 0, \text{enc} = U)$, 其中 $\text{type} = 0$ 表示该密文是“新鲜”密文(未经同态运算的密文).

mIBFHE-Eval(MPK, $\mathbf{C}, \mathbf{C}_1, \dots, \mathbf{C}_\ell$): 输入主公钥 MPK, 密文运算电路 \mathbf{C} 和一系列密文 $\mathbf{C}_1 = (\mathbf{id}_1, \text{type} = 0, \text{enc} = U_1), \dots, \mathbf{C}_\ell = (\mathbf{id}_\ell, \text{type} = 0, \text{enc} = U_\ell)$. 令 $I = \{\mathbf{id}_1, \mathbf{id}_2, \dots, \mathbf{id}_\ell\}$ 表示不同身份的集合, $|I| = \tau \leq D$ 表示不同身份的个数. 若 $\tau > D$ 即超出系统一次同态运算可支持的身份数量, 算法终止. 设 $\mathbf{id}_1, \mathbf{id}_2, \dots, \mathbf{id}_\tau$ 是输入的一系列用户身份中不相同的用户身份. 在对密文进行同态运算前, 需要将每个与用户身份 $\mathbf{id}_1, \mathbf{id}_2, \dots, \mathbf{id}_\tau$ 对应的密文 $\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_\ell$ 转换为 $\tau N \times \tau N$ 的膨胀密文. 令 $(\mathbf{id}_r, \text{type} = 0, \text{enc} = U_r)$ 是相关身份 \mathbf{id}_r 的密文, 其中 $r \in [\tau]$, 膨胀密文 $\hat{\mathbf{C}}$ 的具体计算过程如下.

先将 $\hat{\mathbf{C}} \in \mathbb{Z}_q^{\tau N \times \tau N}$ 设置为零矩阵, 可将 $\hat{\mathbf{C}}$ 视为由 $\tau \times \tau$ 个子矩阵组成, 将第 i 行 j 列的子矩阵表示为 $\hat{\mathbf{C}}_{i,j} \in \mathbb{Z}_q^{N \times N}$. 在 $i \in [\tau]$ 中, 调用 2.3 节的 DeriveMask(MPK, \mathbf{U}, \mathbf{id}') 算法, 返回 $(\mathbf{X}_i, \mathbf{Y}_i)$, 令 $\hat{\mathbf{C}}_{i,i} \leftarrow \mathbf{Y}_i, \hat{\mathbf{C}}_{i,r} \leftarrow \mathbf{C}_{i,r} + \mathbf{X}_i$.

将输出的 τ 个膨胀密文输入运算电路 \mathbf{C} 进行同态运算, 若每个 $\hat{\mathbf{C}}^{(i)}$ 加密的明文消息是 $\mu_i \in \{0, 1\}$, 则输出运算结果 $\hat{\mathbf{C}}'$ 加密的明文消息是 $\mathbf{C}(\mu_1, \dots, \mu_\ell)$. 最后, 输出三元组 $\bar{\mathbf{C}} = (\mathbf{id}_1, \dots, \mathbf{id}_\ell, \text{type} = 1, \text{enc} = \hat{\mathbf{C}}')$, 其中 $\text{type} = 1$ 表示该密文已同态运算一次.

mIBFHE-Decrypt(MPK, $\mathbf{v}_{\mathbf{id}_1}, \dots, \mathbf{v}_{\mathbf{id}_\ell}, \text{CT}$): 输入主公钥 MPK, 待解密密文 $\bar{\mathbf{C}} = (\mathbf{id}_1, \dots, \mathbf{id}_\ell, \text{type}, \text{enc})$ 和与用户身份 $\mathbf{id}_1, \dots, \mathbf{id}_\ell$ 相对应的用户密钥 $\mathbf{v}_{\mathbf{id}_1}, \dots, \mathbf{v}_{\mathbf{id}_\ell} \in \mathbb{Z}_q^N$. 令 $\mathbf{v} = (\mathbf{v}_{\mathbf{id}_1}^T \parallel \dots \parallel \mathbf{v}_{\mathbf{id}_\ell}^T)^T \in \mathbb{Z}_q^{dN}$ 为 $\mathbf{v}_{\mathbf{id}_1}, \dots, \mathbf{v}_{\mathbf{id}_\ell}$ 垂直拼接而成的向量. 如果 $\text{type} = 0$, 将 enc 解析为 U 并计算 $(\mathbf{X}, \mathbf{Y}) \leftarrow (\text{MPK}, \mathbf{U}, \mathbf{id}_1)$, 设 $\mathbf{C} \leftarrow \mathbf{X} + \mathbf{Y}$; 如果 $\text{type} = 1$, 将 enc 解析为 $\hat{\mathbf{C}}'$ 并设 $\mathbf{C} \leftarrow \hat{\mathbf{C}}'$. 已知向量 \mathbf{v} 的前 ℓ_q 个系数为 $1, \dots, 2^{\ell_q-1}$, 设索引 i 满足 $v_i = 2^i \in (q/4, q/2]$, 令 \mathbf{c}_i 为密文 \mathbf{C} 的第 i 行, 计算 $x_i \leftarrow \langle \mathbf{c}_i, \mathbf{v} \rangle$, 输出解密结果 $\mu \leftarrow \lfloor x_i / v_i \rfloor$.

3 安全性证明

通常, 一个格上 IBFHE 方案的安全性应满足选择身份攻击和选择明文攻击下的密文不可区分性(IND-ID-CPA). 格上 mIBFHE 方案的安全性因 Mask 系统存在而稍有不同, 仅是在安全游戏中敌手被给予的挑战密文被 2.3 节中的 $U^* \leftarrow \text{GenUnivMask}(\text{MPK}, \mathbf{id}^*, \boldsymbol{\mu}_b)$ 所代替(具体见以下安全性证明部分). 根据安全强度不同, 分为适应性选择身份选择明文攻击(IND-aID-CPA)和选择性选择身份选择明文攻击(IND-sID-CPA), 区别在于后者敌手需在攻击的初始化阶段向挑战者宣布欲攻击的目标身份, 而前者可等到挑战阶段才宣布, 且后者可在挑战阶段前的用户密钥查询阶段对任意的用户身份进行适应性的查询, 后者的唯一限制是挑战阶段不能宣布之前查询过密钥的用户身份作为攻击目标. 笔者的方案是 IND-sID-CPA 安全的, 且挑战密文与密文空间的随机元素不可区分(IND-rsID-CPA), 因此保证了方案的语义安全和接收方的匿名性, 且主公钥的私密性可被其创建的密文保护.

本方案采用 Agrawal 等^[11]在 Eurocrypt'10 上提出的标准模型下的 IND_r-sID-CPA 安全模型进行安全性证明. 基于该安全模型进行安全证明的还有 Clear 等^[2]提出的可自举 IBFHE 方案和康元基等^[3]提出的环 LWE 上 IBFHE 方案.

正确性:本文方案的解密正确性由定理 1 刻画.

定理 1 mIBFHE 方案的解密是正确的,对任意的 $(\text{MPK}, \text{MSK}) \leftarrow \text{Setup}(\lambda, L, D)$, 用户身份 $\text{id}_1, \dots, \text{id}_r \in \mathcal{I}$, \mathcal{I} 为合法的用户身份空间, 私钥向量 $\mathbf{v}_{\text{id}_i} \leftarrow \text{Powersof2}(\text{KeyGen}(\text{MSK}, \text{id}_i)) \in \mathbb{Z}_q^N$, $U \leftarrow \text{GenUnivMask}(\text{MPK}, \text{id}_i, \mu)$, $(X_i, Y_i) \leftarrow \text{DeriveMask}(\text{MPK}, U, \text{id}_i')$, 密文空间中的任意密文 C , 有 $\Pr[\text{Decrypt}(\text{MPK}, \mathbf{v}_{\text{id}_1}, \dots, \mathbf{v}_{\text{id}_r}, C) = \mu] = 1 - \text{negl}(n)$ 成立.

证明 方案解密算法的输出为

$$\begin{aligned} x_i/v_i &= \langle \mathbf{c}_i, \mathbf{v} \rangle / v_i = \\ &\langle (\mu(\mathbf{I}_N)_i + \text{BitDecomp}(\mathbf{c}_i)), \mathbf{v} \rangle / v_i = \\ &(\mu v_i) / v_i = \mu \end{aligned}$$

为保证密文中的噪声小于 $q/4$ 且 q/B 与安全参数 n 亚指数相关, 对参数设定如下: 由引理 1 可知, 其 TrapGen 算法要求 $m \geq 2n \log q$, 参数 B 的取值取决于 B_{preimage} 和 B_χ , 由引理 2 可知 $B_{\text{preimage}} \leq \sigma \sqrt{m}$, 由定义 4 和定义 5 可知 $B_\chi \geq \sqrt{m} \log n$, 则 $B = R_{\text{quality}} \times m \log^2 n$, 其中 R_{quality} 为陷门质量, 即陷门矩阵 R 的最大奇异值 $s_1(R)$, 因此 $B = m^{1.5} \log^2 n$. 设 α 是方案密文中容错项的膨胀因子, 2.2 节 IBE 方案的 $\alpha = \|\tilde{R}\| \omega(\sqrt{\log n})$, 则 $q = B \cdot 2^{O(L \log n D)}$. 方案的参数设定如表 2 所示.

表 2 基于多身份的全同态加密方案的参数设置

参数	值
m	$2n \log q$
σ	$\sqrt{m} \omega(\sqrt{\log n})$
$1/\alpha$	$m^2 \omega(\sqrt{\log n})$
q	$m^{1.5} \log^2 n 2^{O(L \log n D)}$
B	$m^{1.5} \log^2 n$

安全性:本文方案的安全性由定理 2 刻画.

定理 2 若 $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE 的难解性成立, 则在标准模型下 mIBFHE 方案是 IND_r-sID-CPA 安全的.

证明 定理证明采用基于游戏序列的证明方法, 证明敌手无法区分定义 4 中预言机 \mathcal{O} 的输出是来自伪随机预言机 \mathcal{O}_s 还是真随机预言机 $\mathcal{O}_\$, 从而$

证明敌手无法以不可忽略的优势在 IND_r-sID-CPA 的 Game 中获胜.

Game 0 Game 0 是一个标准的攻击本方案的敌手 \mathcal{A} 与挑战者 \mathcal{C} 之间进行的 IND_r-sID-CPA 游戏.

Game 1 令 $\text{id}^* \in \mathcal{I}$ 为敌手的目标用户身份. 挑战者对预言机 \mathcal{O} 进行询问并获取一组实例 $(u_i, v_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, 其中 $i = 1, \dots, m$, 利用实例 $(u_i, v_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ 生成随机均匀矩阵 $A \in \mathbb{Z}_q^{n \times m}$, 矩阵 A 的第 i 列是向量 $u_i, i = 1, \dots, m$, 并将向量 u 作为公共随机向量 $u \in \mathbb{Z}_q^n$. 将主公钥 $\text{MPK} = (A, u)$ 发送给敌手 \mathcal{A} .

Game 0 与 Game 1 是统计不可区分的, 原因在于: 利用实例 (u_i, v_i) 生成的随机均匀矩阵 A 与引理 1 中的 TrapGen 算法输出的矩阵 A 是统计不可区分的, 且公共随机向量 u 均为随机均匀选取, 由引理 4 可知随机均匀选取的向量 u 与 Game 0 中的 $u = A_{\text{id}} \cdot e_{\text{id}}$ 是统计接近的, 因此 Game 0 与 Game 1 是统计不可区分的.

Game 2 与 Game 1 不同的是, 利用引理 1 中的 TrapGen 算法来生成 $G \in \mathbb{Z}_q^{n \times w}$ 和格 $\Lambda_q^\perp(G)$ 的公开陷门矩阵 T_G , A 仍保留为 Game1 中的形式, 则 $A_{\text{id}} = A + [\mathbf{0} \parallel H_{\text{id}} G] = [\bar{A} \parallel [H_{\text{id}} - H_{\text{id}^*}] G - \bar{A} R]$, 由 FRD 函数的性质^[10]可知, $[H_{\text{id}} - H_{\text{id}^*}]$ 为可逆矩阵, 则挑战者 \mathcal{C} 可使用陷门矩阵 T_G 进行原像采样来回应敌手 \mathcal{A} 的私钥查询: 若 $\text{id} \neq \text{id}^*$, 调用引理 3 中 $e_{\text{id}} \leftarrow \text{SampleR}(A, (H_{\text{id}} - H_{\text{id}^*}) G, T_G, u, \sigma)$ 算法, 输出 e_{id} 并回应给攻击者; 若 $\text{id} = \text{id}^*$, 则 $[H_{\text{id}} - H_{\text{id}^*}]$ 为零矩阵不可逆, 游戏终止.

Game 1 与 Game 2 是统计不可区分的, 原因在于: 由引理 3 可知, 当 $\sigma > s_1(R) \|\bar{R}\| \omega(\sqrt{\log n})$ 时, e_{id} 的分布与 Game 1 中的分布 $\mathcal{D}_{\Lambda_q^\perp(A_{\text{id}}), \sigma}$ 是统计不可区分的. 因此 Game2 中的私钥查询回应方法和矩阵 G 的构造与 Game1 是统计不可区分的.

For $i \in [q]$:

Game $i+1$ 与之前的 Game 不同的是: 将如 2.3 节所示的 GenUnivMask 算法中的 b_η 替换为随机选取的 $b_\eta \leftarrow \mathbb{Z}_q^{m'}$. 假设存在攻击者 \mathcal{P} 能以不可忽略的优势来区分 Game i 与 Game $i+1$, 那么可以利用 \mathcal{P} 来构造一个算法 \mathcal{B} 求解格上 LWE 实例. 采用与 Game 1 中相同的方式构造公共参数 (A, u) , 且对攻击者的用户密钥查询方式与 Game 2 相同.

\mathcal{B} 运行与之前 Game 相同的 GenUnivMask 算

法,但不同的是:将 GenUnivMask 算法中的 \mathbf{b}_η 替换为 $\mathbf{b}_\eta \leftarrow \mathbf{x}^* + (\mu 2^i, 0, \dots, 0) \in \mathbb{Z}_q^{m'}$, 其中 $\mathbf{x}^* \in \mathbb{Z}_q^{m'}$ 是一个 LWE 挑战向量,该向量有 2 种可能:输出伪随机预言机 \mathcal{O}_s 或真随机预言机 \mathcal{O}_s , \mathcal{O}_s 和 \mathcal{O}_s 的输出分别与 Game i 和 Game $i + 1$ 是统计不可区分的. 因此,算法 \mathcal{B} 能够输出攻击者 \mathcal{A} 的猜测来对 LWE 问题求解.

For $\ell_q < i \leq N$:
For $j \in [\eta]$:

Game(i, j):与之前 Game 不同的是:将如 3.3 节所示的 GenUnivMask 算法中的 \mathbf{B}_i 替换为随机选取的 $\mathbf{b}_j \leftarrow \mathbb{Z}_q^{m'}$. 与上述对 Game i 和 Game $i + 1$ 是统计不可区分的分析相同,Game(i, j) 与 Game($i, j + 1$) 同样是统计不可区分的.

Game($i, \eta + 1$):与之前 Game 不同的是:将如 3.3 节所示的 GenUnivMask 算法中的 \mathbf{u}_i 替换为随机选取的 $\mathbf{u}_i \leftarrow \mathbb{Z}_q^{m'}$. 同样可利用上述对 Game i 和 Game $i + 1$ 是统计不可区分的分析,来证明 Game(i, η) 与 Game($i, \eta + 1$) 是统计不可区分的.

可知,直到 Game($N, \eta + 1$) 结束,可以得出结论:明文比特信息 μ 被完全地安全隐藏在 GenUnivMask 算法所输出的 U 中,敌手从信息 U 中能获取到的优势为零. 因此,敌手无法猜测出与之交互的是伪随机预言机 \mathcal{O}_s 还是真随机预言机 \mathcal{O}_s .

4 效率分析

4.1 基于身份加密方案效率分析

由于所构造的基于多身份的全同态加密方案是利用特征向量的思想由基于身份的加密方案转化而来,所以前者的效率很大程度上取决于后者. 另外,为更好地理解基于多身份的全同态加密方案的效率分析,首先对基于身份加密方案的效率进行分析.

这里选择 2 个经典的与本文方案安全性相同的格上 IBE 方案进行效率对比: Agrawal 等^[11] 于 Eurocrypt'10 上提出的标准模型下选择性安全的高效格上 IBE 方案(简称 CHKP 方案)和 Cash 等^[13] 于 Eurocrypt'10 上提出的首个标准模型下选择性安全的格上 IBE 方案(简称 ABB 方案). 效率对比见表 3.

表 3 格上基于身份加密方案效率对比

方案	格的维数	主私钥尺寸	身份公钥尺寸	密文尺寸	LWE 容错率($1/\alpha$)
CHKP	$6n \log q$	$m \times m$	$(k + 1)nm \log q$	$(km + 1) \log q$	$\tilde{O}(n^{2n})$
ABB	$6n \log q$	$m \times m$	$(3m + 1)n \log q$	$(2m + 1) \log q$	$\tilde{O}(n^{1.5})$
Ours	$2n \log q$	$(m \times m)/4$	$(m + 1)n \log q$	$(m + 1) \log q$	$\tilde{O}(n)$

由表 3 可看出,本文方案的主要效率参数和 LWE 容错率都有优化,表明与其他方案相比本方案的效率较好,且所基于的 LWE 问题更具有较高难解性.

首先是格的维数,由于 CHKP 方案和 ABB 方案基于文献[8]的陷门生成算法,为满足所基于困难问题同程度的安全性和支持方案主公钥参数与均匀分布的统计不可区分性需要较高的格维数. 本方案的主私钥尺寸是在合理高斯分布上选取的一组短向量,而不是 CHKP 方案和 ABB 方案的某个格矩阵的一组基,且这组基可在无质量变差的情况下由主私钥生成. CHKP 方案将用户身份看成一系列比特串,并为每一比特生成一个均匀随机的矩阵,然后拼接成用户的身份公钥矩阵,导致该矩阵的维数过大. 而 ABB 方案和本文方案均采用 FRD 函数^[11],将用户身份映射成一个 $n \times n$ 满秩矩阵,身份公钥矩阵的维数明显降低. 因为本方案的用户私钥不再利用陷

门派生算法和原像采样算法相结合的方式生成,所以仅须生成一个均匀随机矩阵即可生成身份公钥. 密文的尺寸与身份公钥尺寸直接相关. 由于公开且构造特殊矩阵 \mathbf{G} 参数的引入,本方案具有较低的 LWE 容错率,由 \mathbf{G} 矩阵的构造容易计算 $\|\mathbf{G}\| = \sqrt{5}$, 则 $1/\alpha \geq 2\sqrt{5}\sigma\omega(\sqrt{\log n})$.

4.2 基于多身份全同态加密方案效率分析

为充分展示本方案的效率,除与 2015 年 Clear 和 McGoldrick 于 Crypto'15 上提出的格上基于多身份的全同态加密方案^[5] (简称 CM 方案)相比外,还选择了 Wang 等^[14] 利用混淆器构造的一种高效的格上基于身份的全同态加密方案(简称 WH 方案). 相比之下,本文方案基于标准模型,在陷门生成和原像采样上的计算效率明显提升,在格的维数、陷门、密文、运算密文尺寸明显缩短. 设安全参数 n 为 284,方案支持的最大运算电路深度为 $L = 50$,为满足解密正确性需设 $\log q = \lceil cL \log L = 4 \times 50 \times$

log 50]=1 129,c=4 为常数,设方案在一次同态运算中所支持的不同的用户身份的最大数量是 $D=$

20. 对比结果如表 4 所示,其中 RO 表示随机预言模型,SM 表示标准模型. 效率对比见表 4.

表 4 格上基于多身份的全同态加密方案的效率对比

方案	安全模型	效率参数				计算效率(\mathbb{Z}_q 乘法次数)		
		格的维数	陷门尺寸/GB	密文尺寸/TB	明文-密文扩展率	运算密文尺寸/TB	陷门生成	原像采样
CM	RO	1 923 816	430. 86	$\approx 60. 55 \times 10^7$	$\approx 53. 26 \times 10^{20}$	$\approx 11. 51 \times 10^9$	$\approx 26. 71 \times 10^{17}$ 次乘 $\approx 26. 71 \times 10^{17}$ 次加	$\approx 13. 70 \times 10^{24}$ 次乘 $\approx 13. 71 \times 10^{24}$ 次加
WH	SM	1 603 180	299. 21	$\approx 16. 82 \times 10^8$	$\approx 14. 79 \times 10^{21}$	$\approx 31. 96 \times 10^9$	$\approx 15. 83 \times 10^{17}$ 次乘 $\approx 15. 82 \times 10^{17}$ 次加	$\approx 66. 06 \times 10^{23}$ 次乘 $\approx 66. 06 \times 10^{23}$ 次加
Ours	SM	641 272	11. 97	$\approx 67. 28 \times 10^6$	$\approx 59. 18 \times 10^{19}$	$\approx 12. 78 \times 10^8$	$\approx 25. 86 \times 10^9$ 次乘 $\approx 25. 85 \times 10^9$ 次加	$\approx 23. 15 \times 10^{10}$ 次乘 $\approx 23. 16 \times 10^{10}$ 次加

由表 4 看出,相比 CM 和 WH 方案,本文方案基于标准模型,且在效率参数和计算效率等方面均有优化.

效率参数方面,首先在格的维数上,本方案较最优的 WH 方案有 2.5 倍的降低,原因在于:所基于的 MP12 陷门生成算法输出的矩阵 $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ 的维数仅为 $2n \log q$ 时,矩阵 \mathbf{A} 的分布与均匀分布的统计距离即可满足为安全参数 n 的可忽略函数. 另外,陷门生成算法所输出陷门的生成质量较好,即陷门的最大奇异值较低,陷门不再是格 $\Lambda^\perp(\mathbf{A})$ 的格基,而是从特定概率分布随机抽取的短向量组成的陷门矩阵. 因此陷门矩阵的尺寸相比 CM 方案较小. 此外,低维数和小的陷门尺寸也是密文、运算密文尺寸较短和明文-密文扩展率较低的主要原因. 应当注意的是,在相同的安全性下,WH 方案的格维数虽然比 CM 方案低,但密文、运算密文和明文-密文扩展率劣于 CM 方案的原因在于:WH 方案基于的混淆器原理需要方案中的参数 $N=(2m+1) \log q$ 即密文矩阵的维数,因而导致上述原因. 运算密文即 2.4 节 mIBFHE 方案中所述的膨胀密文,其尺寸取决于参与运算用户身份的数量 D 和密文尺寸,这里对运算密文尺寸的计算忽略了膨胀密文矩阵里填充的零矩阵,因此尺寸近似等于 19 倍的密文尺寸.

计算效率方面,格上 mIBFHE 陷门函数的高效与否主要与其构成算法(陷门生成和原像采样)有关. 在陷门生成上,笔者提出的陷门生成算法运行过程中不存在计算代价高的 HNF 和矩阵求逆操作,陷门生成的复杂度仅相当于 2 个随机矩阵的一次乘运算. 因此,相比其他方案本方案,在陷门生成的计

算效率上明显降低. 在原像采样上,较其他方案显著降低,原因在于本方案的原像采样算法使用小整数作为输入项且支持并行化运算,而 CM 和 WH 方案所基于的文献[9]的原像采样算法是输入项为高精度实数的正交化迭代运算;另一个原因是,方案的原像采样算法存在的部分高代价计算可线下进行,从而节省了线上资源消耗和用户时间.

综上,本文方案陷门函数的效率和密文尺寸以及其他效率参数均得到不等程度的优化.

5 结束语

针对格上基于多身份的全同态加密方案中陷门函数低效的问题,提出一种改进的方案. 首先基于 MP12 陷门函数构造出一种高效的且可转化的 IBE 方案,并构造出一种支持标准模型下 IBE 方案转化的 Mask 系统,然后结合该系统并利用特征向量的思想将构造出的 IBE 方案转化为 mIBFHE 方案. 对比同类方案,本方案的陷门函数有明显的效率优势,且重要的效率参数均有所缩短. 在标准模型下,方案的安全性满足 INDr-sID-CPA 安全.

所提方案的不足在于标准模型下方案安全性仅满足 IND-sID-CPA 安全,在某些安全需求更高的应用场景中会有使用限制. 如何构造标准模型下 IND-aID-CPA 安全的格上 HIBE 方案是值得进一步研究的问题.

参考文献:

[1] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based [C] // Proceedings of

- CRYPTO 2013. Santa Barbara: Springer, 2013: 75-92.
- [2] Clear M, McGoldrick C. Bootstrappable identity-based fully homomorphic encryption [C] // Proceedings of International Conference on Cryptology and Network Security. New York: Springer, 2014: 1-19.
- [3] 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.
- Kang Yuanji, Gu Chunxiang, Zheng Yonghui, et al. Identity-based fully homomorphic encryption from eigen-vector[J]. Journal of Software, 2016, 27(6): 1487-1497.
- [4] 段然, 顾纯祥, 祝跃飞, 等. NTRU 格上高效的基于身份的全同态加密体制[J]. 通信学报, 2017, 38(1): 66-75.
- Duan Ran, Gu Chunxiang, Zhu Yuefei, et al. Efficient identity-based fully homomorphic encryption over NTRU [J]. Journal on Communications, 2017, 38(1): 66-75.
- [5] Clear M, McGoldrick C. Multi-identity and multi-key leveled FHE from learning with errors[C] // Proceedings of CRYPTO 2015. Santa Barbara: Springer, 2015: 630-656.
- [6] Ajtai M. Generating hard instances of the short basis problem[C] // Proceedings of Automata, Languages and Programming. [S.l.]: Springer, 1999: 1-9.
- [7] 来齐齐, 胡予濮, 陈原, 等. 辅助输入安全的损耗陷门函数的构造[J]. 北京邮电大学学报, 2014, 37(6): 6-10.
- Lai Qiqi, Hu Yupu, Chen Yuan, et al. Construction of auxiliary-input secure lossy trapdoor functions[J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37(6): 6-10.
- [8] Alwen J, Peikert C. Generating shorter bases for hard random lattices [C] // Proceedings of the 26th International Symposium on Theoretical Aspects of Computer Science. Freiburg: Springer, 2009: 535-553.
- [9] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C] // Proceeding of the 40th ACM Symposium on Theory of Computing. Victoria: ACM, 2008: 197-206.
- [10] Micciancio D, Peikert C. Trapdoors for lattices: simpler, tighter, faster, smaller[C] // Proceeding of EUROCRYPT 2012. Cambridge: Springer, 2012: 700-718.
- [11] Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model[C] // Proceeding of EUROCRYPT 2010. Riviera: Springer, 2010: 553-572.
- [12] Regev O. On lattices, learning with errors, random linear codes, and cryptography[C] // Proceedings of the 37th Annual ACM Symposium on Theory of Computing. New York: Springer, 2005: 84-93.
- [13] Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis[C] // Proceeding of EUROCRYPT 2010. Riviera: Springer, 2010: 523-552.
- [14] 王威力, 胡斌. 利用混淆器构造多身份的全同态加密体制[J]. 密码学报, 2017, 4(2): 165-175.
- Wang Weili, Hu Bin. Multi-identity-based fully homomorphic encryption from obfuscation[J]. Journal of Cryptologic Research, 2017, 4(2): 165-175.