



文章编号:1001-9081(2019)03-0750-06

DOI:10.11772/j.issn.1001-9081.2018081669

## 高效的身份基多用户全同态加密方案

涂广升<sup>1,2</sup>, 杨晓元<sup>1,2\*</sup>, 周潭平<sup>1,2</sup>

(1. 网络和信息安全武警部队重点实验室, 西安 710086; 2. 武警工程大学 密码工程学院, 西安 710086)

(\*通信作者电子邮箱 [xyyangwj@126.com](mailto:xyyangwj@126.com))

**摘要:**针对传统的身份基同态加密(IBFHE)方案无法对不同身份标识(ID)下的密文进行同态运算的问题,提出一个基于误差学习(LWE)问题的分层身份基多用户全同态加密方案。该方案利用Clear等(CLEAR M, McGOLDRICK C. Multi-identity and multi-key leveled FHE from learning with errors. Proceedings of the 2015 Annual Cryptology Conference, LNCS 9216. Berlin: Springer, 2015: 630–656)在2015年提出的身份基多用户全同态加密方案([CM15]方案)的转化机制,结合Cash等(CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate a lattice basis. Proceedings of the 2010 Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 6110. Berlin: Springer, 2010: 523–552)在2010年提出的身份基加密(IBE)方案([CHKP10]方案),实现了不同身份标识下的密文同态运算,应用前景更加广阔,在随机预言机模型下为基于身份匿名的选择明文攻击下的不可区分性(IND-ID-CPA)安全。与[CM15]方案相比,该方案在公钥规模、私钥规模、密文尺寸、分层性质和密钥更新周期方面都具有优势。

**关键词:**分层身份基加密;多用户;全同态加密;同态运算;基于误差学习

**中图分类号:** TP309    **文献标志码:**A

### Efficient identity-based multi-identity fully homomorphic encryption scheme

TU Guangsheng<sup>1,2</sup>, YANG Xiaoyuan<sup>1,2\*</sup>, ZHOU Tanping<sup>1,2</sup>

(1. Key Laboratory of Network and Information Security of the Chinese People's Armed Police Force, Xi'an Shaanxi 710086, China;  
2. College of Cryptographic Engineering, Engineering University of the Chinese People's Armed Police Force, Xi'an Shaanxi 710086, China)

**Abstract:** Focusing on the issue that the traditional Identity-Based Fully Homomorphic Encryption scheme (IBFHE) cannot perform homomorphic operations on ciphertexts under different IDentities (ID), a hierarchical identity-based multi-identity fully homomorphic encryption scheme based on Learning With Error (LWE) problem was proposed. In the proposed scheme, the transformation mechanism of identity-based multi-identity homomorphic encryption scheme ([CM15] scheme) proposed by Clear et al. (CLEAR M, McGOLDRICK C. Multi-identity and multi-key leveled FHE from learning with errors. Proceedings of the 2015 Annual Cryptology Conference, LNCS 9216. Berlin: Springer, 2015: 630–656) in 2015 was combined with Identity-Based Encryption (IBE) scheme proposed by Cash et al. (CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate a lattice basis. Proceedings of the 2010 Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 6110. Berlin: Springer, 2010: 523–552) in 2010 ([CHKP10] scheme), guaranteeing IND-ID-CPA (INDistinguishability of IDentity-based encryption under Chosen-Plaintext Attack) security in the random oracle model and realizing ciphertext homomorphic operation under different identities, so the application of this scheme was more promising. Compared with [CM15] scheme, the proposed scheme has advantages in terms of public key scale, private key scale, ciphertext size, and hierarchical properties, and has a wide application prospect.

**Key words:** hierarchical identity-based encryption; multi-identity; fully homomorphic encryption; homomorphic operation; Learning With Error (LWE)

## 0 引言

2009年, Gentry<sup>[1]</sup>提出了第一个基于理想格的全同态加密方案, 全同态加密得到了越来越多密码学家的关注。此后, 新的全同态加密方案相继出现, 其中基于理想格的全同态加密方案(如[GH11b]方案<sup>[2]</sup>)、基于环上的误差学习问题的全同态加密方案(如[BGV12]方案<sup>[3]</sup>)、运用特征向量法的全同

态加密方案(如[GSW13]方案<sup>[4]</sup>)成为研究的热点, 同态加密的效率也在不断提高。

全同态加密方案有多种分类方式, 如果以同态运算能够执行的电路深度为依据, 全同态加密方案可分为“纯”的全同态加密方案和层次型全同态加密方案<sup>[5]</sup>。前者可以对任意深度的电路作任意的运算。层次型全同态加密方案只能执行深度为  $L$  的计算电路, 方案的参数选择依赖于  $L$ 。虽然它并不

收稿日期:2018-08-13;修回日期:2018-10-23;录用日期:2018-10-24。    基金项目:国家重点研发计划项目(2017YFB0802000);国家自然科学基金资助项目(U1636114, 61772550, 61572521);国家密码发展基金资助项目(MMJJ20170112)。

**作者简介:**涂广升(1992—),男,河南驻马店人,硕士研究生,主要研究方向:信息安全、同态密码; 杨晓元(1959—),男,湖南湘潭人,教授,博士生导师,硕士,主要研究方向:信息安全、密码学; 周潭平(1989—),男,江西贵溪人,博士,主要研究方向:信息安全、同态密码。



能达到任意深度电路的要求,但对于多项式深度的电路,在满足用户需求的同时,更加高效实用。

在身份基加密方案中,身份信息作为用户的唯一标识,用户的公钥可以从用户的身份信息字符串和系统的公共参数中获得,对应的私钥为用户私有。2013年Gentry等<sup>[4]</sup>提出了一个新的层次型全同态加密方案。该方案允许计算方在不获得用户的计算密钥(EValuation Key, EVK),而只需要知道系统公共参数信息的情况下,实现对明文的加密和对密文的运算。利用此特性,该方案构造了第一个身份基全同态加密方案;然而它只适用于单用户身份信息场景,即只能对在同一身份信息下加密的密文进行运算。2015年,Clear等<sup>[6]</sup>通过构造屏蔽系统(Masking System, MS)的方法,提出了第一个基于误差学习(Learning With Error, LWE)问题的身份基多用户全同态加密方案(该方案称为[CM15]方案),并证明该方案在随机预言机模型下为IND-ID-CPA(INDistinguishability of IDentity-based encryption under Chosen-Plaintext Attack)安全。

身份基多用户全同态加密方案实现了不同用户密文之间的同态运算,在密文计算领域有着广泛的应用。以两方的密文计算为例,假设C为可信任的权威机构,Alice和Bob为C中的两个不同身份体或不同部门,其身份信息分别为a,b。C为Alice和Bob产生公开的公钥信息,并分配相应的私钥。公共用户可以分别使用Alice和Bob的公开身份信息和公共参数对个人信息进行加密,而后将密文分别发送给Alice和Bob。C将数据上传到半透明的云服务器E,在服务器端进行同态运算,得到新的密文,而后返回给C。权威机构C通过多方计算协议(Multi-Party Computation, MPC),使用Alice和Bob的私钥对密文进行解密,解密后的结果保持同态方案的性质。整个过程中既实现了不同身份信息下密文的同态运算,也能保证用户之间的私钥信息的非交互性,即Alice和Bob互相不知道对方的私钥。这里的实例场景表示不同身份信息的用户数 $\kappa=2$ ,对于更多不同身份信息用户的情况同样适用。

本文利用文献[6]的转化机制,结合Cash等<sup>[7]</sup>提出的分层身份基加密(Hierarchical Identity-Based Encryption, HIBE)方案(该方案被称为[CHKP10]方案),将该方案转化为分层身份基多用户全同态加密方案。相比于传统的身份基全同态加密方案,本方案实现了对不同身份信息下密文的同态运算,能够更好地与其他技术结合(如即时多方计算协议、奇点打孔陷门),应用场景更加广泛。相比于文献[6]中的身份基多用户全同态加密方案,本方案虽然使用相同的转化机制,但本方案采用随机预言机模型下的[CHKP10]方案,文献[6]采用Gentry等<sup>[8]</sup>在2008年发表的利用陷门函数构造的身份基加密方案(该方案被称为[GPV08]方案)。由于RO模型下的[CHKP10]方案相比[GPV08]方案在公钥规模、私钥规模、密文尺寸方面都有一定优势,并且实现了分层功能,因此,在安全性相同(都能达到随机预言机(Random Oracle, RO)模型下的选择安全)的情况下,本方案的密钥更新时间更短,效率更高。

## 1 相关理论基础

### 1.1 全同态加密

全同态加密方案包含四个算法,分别为密钥生成算法、加

密算法、解密算法和密文计算算法<sup>[1,9]</sup>。

**密钥生成算法(KeyGen)** 输入安全参数 $\lambda$ ,输出公钥 $pk$ 和私钥 $sk$ 。

**加密算法(Enc)** 输入公钥 $pk$ 和明文消息 $m \in \{0,1\}$ ,生成密文 $c$ 。

**解密算法(Dec)** 输入密文 $c$ 和密钥 $sk$ ,输出解密结果 $m'$ 。

**同态计算算法(Eval)** 用于对加密后的密文进行同态操作,这也是全同态加密中的关键算法。输入公钥 $pk$ ,运算电路 $C \in \mathbb{C}$ ,密文组 $(c_1, c_2, \dots, c_t)$ ,输出新的密文 $c'$ 。

全同态加密方案应当具有以下几个性质<sup>[9]</sup>:

**正确性** 对任意 $\text{KeyGen}(1^\lambda) \rightarrow (pk, sk), m \in \{0,1\}$ ,有 $\text{Dec}(sk, \text{Enc}(pk, m)) = m$ 成立。对任意 $\text{KeyGen}(1^\lambda) \rightarrow (pk, sk), m \in \{0,1\}, C \in \mathbb{C}$ 表示一个功能函数,有 $C(m_1, m_2, \dots, m_t) = \text{Dec}(sk, (\text{Eval}(pk, C, \text{Enc}(pk, m_1), \text{Enc}(pk, m_2), \dots, \text{Enc}(pk, m_t)))$ 成立。

**紧凑性** 解密电路的深度并不随着计算电路深度的增加而增加,也就是说计算电路产生的密文大小并不取决于计算电路的大小。

**定义1 层次型全同态加密方案** 对于任意 $L \in \mathbb{Z}^+$ ,一个同态加密方案 $\varepsilon^{(L)}$ 能够计算的电路深度为 $L$ ,并且满足上述的紧凑性。设电路大小用 $z$ 表示,紧凑计算的复杂度为 $\text{poly}(\lambda, L, z)$ 则称该方案为层次型全同态方案<sup>[10]</sup>。

### 1.2 分层身份加密(HIBE)

HIBE是在IBE的基础上发展起来的,在密钥生成阶段能够很好地减轻私钥生成器(Private Key Generator, PKG)的工作负担。与IBE方案<sup>[11-12]</sup>(由Setup、KeyGen、Enc、Dec这4个算法组成)相比,HIBE方案有一个新的算法:Lower-level Setup算法。

**Setup** 输入安全参数 $k$ ,输出主私钥(MaSter Key, MSK)和公共参数(Public Parameters, PP)。主密钥MSK为根PKG私有;PP为公共参数,包含用于生成身份信息对应的公钥和密文空间描述等信息。

**Lower-level Setup** 用户根据身份信息设置自己的低层密钥,用于生成下一层身份信息对应的私钥。

**Key generation** 输入 $(PP, MSK, ID)$ ,PKG生成身份信息对应的私钥 $s_{ID}$ 。这里的PKG既可能是根PKG,也可能是身份信息对应的上一层的PKG。

**Encryption** 输入 $(PP, ID, m)$ ,输出密文 $c$ 。其中PP来自根PKG, ID为低层接收方的身份信息,这样可保证发送方不必知道低层用户的密钥参数。

**Decryption** 接收方根据来自根PKG的公共参数PP、用户自己的身份信息对应的私钥解密密文,解密密文得到相应的 $m$ 。

### 1.3 LWE问题

LWE问题最早由Regev<sup>[13]</sup>在2005年提出,已经被证明为一个难解的多项式复杂程度的非确定性(Non-deterministic Polynomial, NP)问题。

**定义2 计算性LWE问题** 设 $\lambda$ 为安全参数,参数 $n = n(\lambda), q = q(\lambda) \geq 2$ 均为整数, $\chi$ 是 $Z_q$ 上的高斯分布,选择 $a_i \xleftarrow{\$} Z_q^n, s \xleftarrow{\$} Z_q^n, e_i \xleftarrow{\$} \chi$ ,计算 $b_i = \langle a_i \cdot s \rangle + e_i \in Z_q$ ,得



到分布  $A_{s,\chi}$ 。在  $A_{s,\chi}$  中选取任意多的样本,输出向量  $s$ 。

**定义3 判定性LWE问题。**设  $\lambda$  为安全参数,参数  $n = n(\lambda), q = q(\lambda) \geq 2$  均为整数,  $\chi$  是  $Z_q$  上的高斯分布,判定性 LWE 问题就是要区分以下两个分布:

$$\begin{aligned} D_0 &= (\mathbf{a}_i, b_i) \in Z_q^n \times Z_q, \text{ 其中 } \mathbf{a}_i \xleftarrow{\$} Z_q^n, b_i \xleftarrow{\$} Z_q, D_1 = \\ &(\mathbf{a}_i, b_i) = (\mathbf{a}_i, \langle \mathbf{a}_i \cdot s \rangle + e_i), \text{ 其中 } \mathbf{a}_i \xleftarrow{\$} Z_q^n, s \xleftarrow{\$} Z_q^n, \\ &e_i \xleftarrow{\$} \chi. \end{aligned}$$

**定理1** 令  $n$  为格的维度,  $q = q(n)$ ,  $\chi$  为  $B$  有界的高斯分布,  $B \geq \omega(\log n) \cdot \sqrt{n}$ , 如果存在一个有效的算法能够解决平均情况下的 LWE 问题,那么<sup>[14]</sup>:

1) 对于任意维度的格,存在一个有效的量子算法,能够解决近似因子为  $\tilde{O}(nq/B)$  的具有间隙的最短向量(Gap Version of Shortest Vector Problem, GapSVP)问题。

2) 对于任意维度的格,如果  $q = q(n) \geq \tilde{O}(2^{\frac{n}{2}})$ ,就存在一个有效的经典算法,能够解决近似因子为  $\tilde{O}(nq/B)$  的 GapSVP 问题。

利用量子归约和经典归约的方法,将 LWE 问题归约到最坏情况下格上困难问题,而格的困难问题已经被证明为难解的 NP 问题。

Regev<sup>[15]</sup> 在 2010 年给出证明,如果存在一个算法能够以指数级别接近于 1 的概率解决判定性 LWE 问题,那么就存在一个更加高效的算法,能以指数级别接近于 1 的概率解决计算性 LWE 问题。即解决判定性 LWE 问题的优势不大于解决 LWE 问题的优势<sup>[16]</sup>。

## 2 分层身份基多用户全同态加密方案

### 2.1 屏蔽系统

由文献[4]的转化机制可知,一个 IBE 方案可以被转化为 IBFHE 方案,如果满足以下三条性质<sup>[4]</sup>:

**性质1** 身份信息 ID 对应的解密密钥为  $s_{ID} \in Z_q^{m'}$ , 对应密文为  $c_{ID} \in Z_q^{m'}$ , 并且向量  $s_{ID}$  的第一个系数为 1。

**性质2** 如果  $c_{ID}$  为加密 0 得到的密文,则  $\langle c_{ID}, s_{ID} \rangle = e$ , 结果为一个小的噪声。

**性质3** 加密 0 得到的密文向量与  $Z_q^{m'}$  上的均匀分布向量不可区分。

为了将身份基全同态加密方案转化为身份基多用户全同态加密方案,应当为 IBE 方案构造一个相应的屏蔽系统,并满足其正确性和安全性。

**定义4** 设  $\varepsilon$  为一个 IBE 方案,满足上述三条性质,  $\varepsilon$  的屏蔽系统  $MS_\varepsilon$  由一对多项式时间算法组成( $GenUnivMask$ ,  $DeriveMask$ ),具体描述如下<sup>[6]</sup>:

$GenUnivMask(PP, ID, \mu)$ :输入  $\varepsilon$  的公共参数  $PP$ ,身份信息  $ID$  和明文  $\mu \in \{0,1\}$ ,输出通用屏蔽  $U \in \{0,1\}^*$ 。

输入  $\varepsilon$  的公共参数  $PP$ ,身份信息  $ID'$  和通用屏蔽  $U \in \{0,1\}^*$ ,输出一对矩阵  $(X, Y) \in (Z_q^{N \times N})^2$ 。

一个屏蔽系统  $MS_\varepsilon$  应当满足以下两条性质:

**正确性** 设  $\lambda$  为安全参数,  $\omega = \omega(\lambda)$  表示误差扩展因子,为  $\lambda$  的多项式级别。对任意的  $(PP, MSK) \leftarrow \varepsilon$ .  $Setup(1^\lambda)$ ,任意的身份信息  $ID, ID'$ ,调用密钥生成函数得到  $s_{ID}$ ,

$s_{ID'}$ ,令  $v_{ID} = Powersoft2(s_{ID}), v_{ID'} = Powersoft2(s_{ID'})$ ,明文空间  $\mu \in \{0,1\}$ ,  $(X, Y) \in (Z_q^{N \times N})^2$  由以上算法得出,则必须满足  $X \cdot v_{ID} + Y \cdot v_{ID'} = \mu \cdot v_{ID'} + e$  成立,其中  $\|e\|_\infty \leq \omega$ 。 $B$ 。

**安全性** 如果对于所有的多项式时间敌手 A,给定公共参数及  $U^* \leftarrow GenUnivMask(PP, ID^*, \mu_b)$ ,其中  $ID^*$  为敌手的目标身份,  $b \xleftarrow{\$} \{0,1\}$  为挑战者随机选择的明文位,攻击者在 IND-ID-CPA( $X \in \{s_{ID}, ID\}$ ) 游戏中成功区分  $\mu_0$  和  $\mu_1$  的概率可以忽略不计,则称该方案是选择性安全的。

### 2.2 本文身份基多用户全同态加密方案

利用文献[6]的转化机制,对 RO 模型下的[CHKP10] 方案构造相应的屏蔽系统  $MS_{[CHKP10]}$ ,从而得到一个新的身份基多用户全同态加密方案,表示为 mHIBFHE,具体方案如下。

1)mHIBFHE.  $setup(d, \lambda)$ :设  $d$  表示身份信息向量的最大长度,  $\kappa$  为参与方不同身份信息个数的最大值,则定义身份信息集合  $I = (ID_1, ID_2, \dots, ID_\kappa)$ 。设  $\ell_q = \lfloor \log q \rfloor + 1$ , 调用文献[8] 中的  $GenBasis(1^n, 1^m, q)$  算法生成统计均匀的矩阵  $A_0 \in Z_q^{n \times m}$ , 构造随机格  $\Lambda^\perp(A_0) = \{y \in Z^n \mid A_0 \cdot y = 0 \bmod q\}$ , 在格中选择一组短的基  $S_0 \in Z^{m \times m}$ 。对于任意  $(i, b) \in [d] \times \{0,1\}$ , 选取一组均匀、相互独立的矩阵  $A_i^b \in Z_q^{n \times m}$ 。随机均匀选取  $z \in Z_q^n$ , 输出  $MPK = (A_0, \{A_i^b\}, z, d); MSK = S_0$ 。

2)mHIBFHE.  $KeyGen(MSK, ID)$ :设  $t \leq d$ , 身份信息  $ID = (id_1, id_2, \dots, id_t) \in \{0,1\}^t$ 。定义  $A_{ID} = (A_0 \parallel A_1^{id_1} \parallel A_2^{id_2} \parallel \dots \parallel A_t^{id_t}) \in Z_q^{n \times (t+1)m}$ , 调用文献[8] 中的函数  $ExtBasis(S_0, A_{ID})$  生成身份信息 ID 对应的  $S_{ID}$ ,作为格  $\Lambda^\perp(A_{ID}) = \{x \in Z^n \mid A_{ID} \cdot x = 0 \bmod q\}$  的一组短基。调用文献[8] 中的函数  $SampleD(S_{ID}, A_{ID}, z_{ID})$  生成  $t_{ID}, s_{ID} = (1, -t_{ID})$ 。令  $A_{ID}' = z_{ID} \parallel A_{ID}$ , 满足  $A_{ID} \cdot t_{ID} = z_{ID} \bmod q, A_{ID}' \cdot s_{ID} = 0 \bmod q$ 。由以上可知,身份 ID 对应的私钥为  $s_{ID}$ 。

设  $ID_i = (id_1, id_2, \dots, id_{t_i}) \in \{0,1\}^{t_i}$  为低层的身份信息,由分层身份基方案的性质可知,  $ID_i$  的前缀为  $ID$ ,即  $ID_i = (ID \parallel \overline{ID})$ ,  $t_i \leq d, A_{ID_i} = A_{ID} \parallel A_{ID} = A_0 \parallel \dots \parallel A_{t_i}^{id_{t_i}} \in Z_q^{n \times (t_i+1)m}$ 。调用函数  $ExtBasis(S_{ID}, A_{ID_i})$  生成身份信息  $ID_i$  对应的  $S_{ID_i}$ ,继续调用函数  $SampleD(S_{ID_i}, A_{ID_i}, z_{ID_i})$ ,生成  $t_{ID_i}, s_{ID_i} = (1, -t_{ID_i})$ ,得到低层身份  $ID_i$  对应的私钥。

3)mHIBFHE.  $enc(PP, ID, \mu)$ :为了在身份 ID 在下加密  $\mu$ ,调用函数  $MS_{[CM15]} \cdot GenUnivMask(PP, ID, \mu)$ ,得到通用屏蔽信息  $U$ 。输出密文组  $CT = (ID, type = 0, enc = U)$ ,  $type = 0$  表示密文为“新鲜”密文。

4)mHIBFHE.  $eval(C, CT_1, CT_2, \dots, CT_\ell)$ :输入电路  $C \in \mathbb{C}$  和一组密文  $CT_1 = (ID_1, type = 0, enc = U_1), CT_2 = (ID_2, type = 0, enc = U_2), \dots, CT_\ell = (ID_\ell, type = 0, enc = U_\ell)$ 。

为了能够对密文进行同态操作,需要对已知新鲜密文  $C \in Z_q^{N \times N}$  进行处理,得到相应的扩展密文  $\bar{C} \in Z_q^{N \times N}$ 。扩展密文从形式上可以表示为  $\kappa \times \kappa$  的矩阵,  $\bar{C}_{i,j}$  表示第  $i$  行第  $j$  列的子块,每个子块都是  $Z_q^{N \times N}$  的矩阵,得到扩展密文的过程如下:

$$\begin{cases} (X_i, Y_i) \leftarrow MS_{[CM15]} \cdot DeriveMask(PP, U, ID_i) \\ \bar{C}_{i,i} \leftarrow Y_i \\ \text{当 } i = r \text{ 时,有 } \bar{C}_{i,r} \leftarrow \text{Flatten}(\bar{C}_{i,r} + X_i) \end{cases}$$



设 $(ID_r, type = 0, enc = U)$ 表示不同参与方中的第 $r$ 个用户得到的新鲜密文,则 $\bar{C}^{(r)} \in Z_q^{\kappa N \times \kappa N}$  ( $\kappa > 2$ ) 的形式如下:

$$\bar{C}^{(r)} = \begin{bmatrix} Y_1 & 0 & \cdots & X_1 & \cdots & 0 \\ 0 & Y_2 & \cdots & X_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & \text{Flatten}(X_r + Y_r) & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & X_\kappa & \cdots & Y_\kappa \end{bmatrix}$$

其中, $X_i$ 位于第 $i$ 列。

对每个输入密文 $C$ 进行相应运算,得到扩展密文 $\bar{C}^{(r)}$ 。将扩展矩阵 $\bar{C}$ 输入电路 $C$ (由与非门电路构成)进行同态运算,得到新的扩展矩阵 $\bar{C}'$ ,对应明文为 $C(\mu_1, \mu_2, \dots, \mu_\kappa)$ ,输出结果为 $CT' = (ID_1, ID_2, \dots, ID_\kappa; type = 1; enc = \bar{C}')$ , $type = 1$ 表示经过同态操作后得到的新密文。由式 $X \cdot v_{ID} + Y \cdot v_{ID'} = \mu \cdot v_{ID} + e$ 可知, $\bar{C}' \cdot v = C(\mu_1, \mu_2, \dots, \mu_\kappa) \cdot v + e'$ 成立。

5)mHIBFHE.dec( $CT, v$ ):分两种情况进行讨论:当 $type = 0$ 时, $CT = (ID_1; type = 0; enc = U)$ , $(X, Y) = MS_{[CM15]}$ .DeriveMask( $PP, U, ID_1$ ),令 $C \leftarrow X + Y$ ,有 $C \cdot v_{ID_1} = \mu \cdot v_{ID_1} + e$ 成立。

当 $type = 1$ 时, $CT = (ID_1, ID_2, \dots, ID_\kappa; type = 1; enc = \bar{C})$ ,令 $C \leftarrow \bar{C}$ ,由式 $X \cdot v_{ID} + Y \cdot v_{ID'} = \mu \cdot v_{ID} + e$ 可知, $C \cdot v = \mu \cdot v + e$ 。

令 $\ell_q = \lfloor \log q \rfloor + 1$ , $v \leftarrow \text{Powersoft2}(s_{ID})$ ,则 $v$ 的前 $\ell_q$ 个系数为 $(2^0, 2^1, \dots, 2^{\ell_q-1})$ ,在前 $\ell_q$ 个系数中选取,选取 $v_j = 2^j \in (q/4, q/2]$ 为 $C$ 的第 $j$ 行,计算 $\mu' = \langle c_i, v \rangle = (\mu \cdot v + e)$ ,对 $\mu'$ 进行取整,得到解密值。

### 2.3 同态运算

设 $C^1, C^2$ 分别为 $\mu_1, \mu_2$ 在 $ID_1, ID_2$ 下加密得到的密文矩阵,对应私钥分别为 $s_{ID_1}, s_{ID_2}$ ,令 $v_1 \leftarrow \text{powersoft2}(s_{ID_1}), v_2 \leftarrow \text{powersoft2}(s_{ID_2})$ ,则 $C^1 \cdot v_1 = \mu_1 \cdot v_1 + e_1, C^2 \cdot v_2 = \mu_2 \cdot v_2 + e_2$ 成立。

令 $\bar{C}$ 表示密文矩阵的扩展矩阵, $v$ 是 $v_1, v_2, \dots, v_\kappa$ 的垂直级联,则有 $\bar{C}^1 \cdot v = \mu_1 \cdot v + e_1, \bar{C}^2 \cdot v = \mu_2 \cdot v + e_2$ 成立。

同态加法运算 Add( $\bar{C}^1, \bar{C}^2$ ): 输入 $(\bar{C}^1, \bar{C}^2)$ ,输出 $\text{Flatten}(\bar{C}^1 + \bar{C}^2)$ ,有 $\text{Add}(\bar{C}^1, \bar{C}^2) \cdot v = (\bar{C}^1 + \bar{C}^2) \cdot v = (\mu_1 + \mu_2) \cdot v + (e_1 + e_2)$ 成立。

同态乘法运算 Multi( $\bar{C}^1, \bar{C}^2$ ): 输入 $(\bar{C}^1, \bar{C}^2)$ ,输出 $\text{Flatten}(\bar{C}^1 \cdot \bar{C}^2)$ ,有

$$\begin{aligned} \text{Multi}(\bar{C}^1 \cdot \bar{C}^2) \cdot v &= (\bar{C}^1 \cdot \bar{C}^2) \cdot v = \bar{C}^1 \cdot (\mu_2 \cdot v + e_2) \\ &= \mu_2 \bar{C}^1 \cdot v + \bar{C}^1 e_2 = \mu_2 (\mu_1 \cdot v + e_1) + \bar{C}^1 e_2 = \mu_1 \mu_2 \cdot v + (\mu_2 e_1 + \bar{C}^1 e_2) \end{aligned}$$

## 3 方案分析

### 3.1 正确性分析

定义5  $B$ 强有界矩阵。设 $B$ 为小于 $q$ 的整数, $C$ 为加密明文 $\mu$ 对应的密文矩阵, $v$ 为对应的私钥,并且有 $C \cdot v = \mu \cdot v + e$ 成立。当 $|\mu| \leq 1$ 时, $\|e\| \leq B$ 且 $\|C_{i,j}\|_\infty \leq 1$ 时,称 $C$ 为 $B$ 强有界矩阵<sup>[4]</sup>。

由文献[4]可知,当密文矩阵 $C_1, C_2 \in Z_q^{N \times N}$ 为 $B$ 强有界

矩阵时,进行同态乘法运算 $(C_1 \cdot C_2) \cdot v = \mu_1 \mu_2 \cdot v + (C_1 e_2 + \mu_2 e_1)$ ,噪声增长为 $\|e'\|_\infty \leq (N+1)B$ 。利用NAND门电路和校平技术,使新的密文为 $\text{Flatten}(C_3) = \text{Flatten}(I_N - C_1 \cdot C_2)$ 仍为强有界矩阵,设置参数 $q/B$ 为 $N$ 的指教级,则当电路深度为 $L$ 时,噪声增长为 $\|e''\|_\infty \leq (N+1)^L B$ 。当满足 $\|e''\|_\infty \leq (N+1)^L B \leq q/8$ 时,保证解密的正确性。

本方案中,扩展矩阵 $\bar{C} \in Z_q^{K \times K}$ 的每一部分都是 $B$ 强有界矩阵,由 $X \cdot v_{ID'} + Y \cdot v_{ID'} = \mu \cdot v_{ID'} + e$ 知, $\bar{C} \cdot v = \mu \cdot v + e$ ,扩展矩阵对应的噪声为 $\|e\|_\infty \leq \omega \cdot B, \omega = \eta + 1 (\eta = n \cdot \ell_q)$ 为噪声扩张因子。则当电路深度为 $L$ 时,噪声增长为 $\|e''\|_\infty \leq \omega (\kappa N + 1)^L B$ 。当满足 $\|e''\|_\infty \leq \omega (\kappa N + 1)^L B \leq q/8$ 时,选取 $q \geq 8\omega B (\kappa N + 1)^L, m = O(n \log q), N = O(m \ell_q)$ ,因此,实例化 $q = B \cdot 2^{O(L \log n \kappa)}$ ,满足 $q/B$ 至多为亚指教级保证解密的正确性。

### 3.2 安全性分析

定理2 假设LWE问题是安全的,对于所有的多项式时间攻击者A,在IND-ID-CPA游戏中成功区分 $\mu_0$ 和 $\mu_1$ 的概率可以忽略不计,那么 $MS_{[\text{CHKP10}]}$ 方案可以达到IND-ID-CPA安全性。

定理3 如果一个IBE方案 $\varepsilon$ 和为该方案构造的屏蔽系统 $MS_\varepsilon$ 在随机预言机下都可以达到IND-ID-CPA安全,那么结合方案 $\varepsilon$ 和屏蔽系统 $MS_\varepsilon$ 得到的身份基多用户全同态加密方案也为随机预言机下的IND-ID-CPA安全<sup>[6]</sup>。

定理4 由文献[7]可知,[CHKP10]方案在RO模型下为IND-ID-CPA安全。假设LWE问题是困难的,那么上述身份基多用户全同态加密方案至少能够达到随机预言机模型下的IND-ID-CPA安全。

证明 方案的安全性可通过以下攻击者A和挑战者C游戏来定义:

- 1) 选定攻击目标身份 $ID^*$ 。
- 2) 初始化参数设置:挑战者运行Setup算法,得到系统公共参数,并公开给攻击者A,并保留主密钥。
- 3) 训练1:攻击者A选择一定数量的身份 $ID_i$ ( $ID_i \neq ID^*$ ),询问随机预言机,得到对应的 $s_{ID_i}$ 。
- 4) 挑战:攻击者在询问预言机结束后,选择 $\mu_0, \mu_1 \in \{0, 1\}$ 交给挑战者,挑战者随机选择 $\mu_b (b \leftarrow \{0, 1\})$ ,并计算 $U^* \leftarrow \text{GenUnivMask}(PP, ID^*, \mu_b)$ ,将结果返回给攻击者A。
- 5) 训练2:攻击者A再次选择一定数量的身份 $ID_i$ ( $ID_i \neq ID^*$ ),询问随机预言机,得到对应的 $s_{ID_i}$ 。
- 6) 猜测:攻击者根据训练过程,对 $b$ 的值进行猜测,得到 $b'$ ,如果 $b' = b$ ,则攻击成功。

攻击者攻击成功的优勢为 $ADV_A^{\text{IND-ID-CPA}} = |pr(b' = b)| - 1/2|$ 。

设 $n$ 为正整数, $q$ 为素数, $m \geq 2n \log q, \chi$ 为 $B$ 有界的 $B_\chi$ 高斯分布。构造两个游戏G0和G1,其中G0表示按照本方案描述的选择安全游戏,G1表示均匀分布下的选择安全游戏。根据 $MS_{[\text{CM15}]}$ 的算法构造可知,如果一个算法能够区分出G0和G1中的 $b_n, b_j$ ,那么就可以在得到 $U$ 后,利用随机预言机,区分出 $\mu_0$ 或 $\mu_1$ 。



Game G0  
procedure Initialize:

$$\begin{aligned} & (A_0, S_0) \leftarrow \text{GenBasis}(1^n, 1^m, q) \\ & A_i^{id_i^*} = H(id_1, id_2, \dots, id_i) \in Z_q^{n \times tm} \\ & z_{ID^*} = G(ID^*) \in Z_q^n, MSK = S_0 \\ & \text{return } MPK = (A_0, A_i^{id_i^*}, z_{ID^*}) \\ & \text{procedure KeyGen:} \\ & A_{ID^*} = A_0 \| A_1^{id_1^*} \| A_2^{id_2^*} \| \dots \| A_t^{id_t^*} \in Z_q^{n \times (t+1)m} \\ & A_{ID^*}' = z_{ID^*} \| A_{ID^*} \in Z_q^{n \times m'}, A_{ID^*}'' = 0 \| A_{ID^*} \in Z_q^{n \times m'} \\ & S_{ID^*} = \text{ExBasis}(S_0, A_{ID^*}), \\ & t_{ID^*} = \text{SampleD}(S_{ID^*}, A_{ID^*}, z_{ID^*}), s_{ID^*} = (1, -t_{ID^*}) \\ & \text{procedure } H, G: \\ & H: \{0,1\}^* \in Z_q^{n \times m}, G: \{0,1\}^* \in Z_q^n \\ & \text{procedure GenUnivMask:} \\ & i \leq \lfloor \log q \rfloor + 1 \text{ 时} \\ & r \xleftarrow{\$} Z_q^n, e \xleftarrow{\$} \chi^{m'}, r2 = \text{powersof2}(r) \\ & b_\eta = A_{ID^*}' \cdot r + e + (\mu \cdot 2^{i-1}, 0 \dots 0) \in Z_q^{m'} \\ & \lfloor \log q \rfloor + 1 < i \leq N \text{ 时, } j \in [\eta] \\ & s \xleftarrow{\$} Z_q^n, f \xleftarrow{\$} \chi^{m'} \\ & \omega_j = (r2_j, 0 \dots 0) \in Z_q^{m'}, b_j = A_{ID^*}' \cdot s + f + \omega_j \in Z_q^{m'} \\ & \text{return } (b_\eta, b_j) \end{aligned}$$

Game G1

procedure Initialize:

$$\begin{aligned} & A_0 \xleftarrow{\$} Z_q^{n \times m}, A_i^{id_i^*} \xleftarrow{\$} Z_q^{n \times tm} \\ & z_{ID^*} \xleftarrow{\$} Z_q^n, MSK = S_0 \\ & \text{return } MPK = (A_0, A_i^{id_i^*}, z_{ID^*}) \\ & \text{procedure KeyGen:} \\ & A_{ID^*} = A_0 \| A_1^{id_1^*} \| A_2^{id_2^*} \| \dots \| A_t^{id_t^*} \in Z_q^{n \times (t+1)m} \\ & A_{ID^*}' = z_{ID^*} \| A_{ID^*} \in Z_q^{n \times m'}, A_{ID^*}'' = 0 \| A_{ID^*} \in Z_q^{n \times m'} \\ & A_{ID^*} \cdot t_{ID^*} = z_{ID^*} \bmod q, s_{ID^*} = (1, -t_{ID^*}) \\ & \text{procedure } H(ID): \\ & \quad \text{if } ID = ID^*; H(ID) = \perp \\ & \quad \text{else compute } (s_{ID^*}, z_{ID^*}); \text{return } (z_{ID^*}) \\ & \text{procedure GenUnivMask:} \\ & \quad i \leq \lfloor \log q \rfloor + 1 \text{ 时: } b_\eta \xleftarrow{\$} Z_q^{m'} \\ & \quad \lfloor \log q \rfloor + 1 < i \leq N \text{ 时, } j \in [\eta]: b_j \xleftarrow{\$} Z_q^{m'} \\ & \text{return } (b_\eta, b_j) \end{aligned}$$

分析 G0 和 G1, 可知:

1) 由于采用 GenBasis  $(1^n, 1^m, q)$  算法生成的矩阵  $A_0$  统计上接近均匀分布; 模拟随机预言机, 当  $ID \neq ID^*$  时,  $H(ID)$  在统计上也接近于均匀分布; 调用 SampleD 函数生成的  $t_{ID^*}$  与随机预言机中满足条件  $A_{ID^*} \cdot t_{ID^*} = z_{ID^*} \bmod q$  得到的  $t_{ID^*}$  在统计上接近均匀分布, 因此, G0 和 G1 中的  $s_{ID^*}$  具有相同的分布。

2) 假设有两个分布  $D_0 = \{(a_i, \langle a_i, s \rangle + e_i) : a_i \xleftarrow{\$} Z_q^n, e_i \xleftarrow{\$} \chi\}$  和  $D_1 = \{(a_i, b_i) : a_i \xleftarrow{\$} Z_q^n, b_i \xleftarrow{\$} Z_q\}$ ,  $a_i$  被用来构造矩阵  $A_{ID^*}$  和向量  $z_{ID^*}$ 。假设多项式时间算法 B 模拟上述的随机预言机, 执行  $MS_{[CM15]} \cdot \text{GenUnivMask}$  函数, 得到  $b_\eta \xleftarrow{\$}$

表 2 本文方案与 [CM15] 方案的比较

Tab. 2 Comparison of the proposed scheme with scheme [CM15]

$x + (\mu \cdot 2^{i-1}, 0 \dots 0) \in Z_q^{m'}$ , 向量  $x = A_{ID^*}' \cdot r + e$  或等于一个随机均匀向量。把  $x$  看作一个 LWE 问题的实例。则当  $x = A_{ID^*}' \cdot r + e$  时,  $b_\eta = A_{ID^*}' \cdot r + e + (\mu \cdot 2^{i-1}, 0 \dots 0) \in Z_q^{m'}$  对应 G0 的结果; 当  $x$  为一个随机均匀向量时,  $b_\eta$  对应 G1 的结果。同理  $b_j$  也适用该游戏。

3) 假设有一个判别器 D, 以一个不可忽略的概率成功判别游戏 G0 和 G1 的分布, 那么存在一个算法 B 可以利用判别器的输出结果来解决一个实例化的判定性 LWE 问题。

4) 由于解决判定性 LWE 问题是困难的, 因此, 攻击者无法区分游戏 G0 和 G1 的分布, 即攻击者无法区分  $b_\eta$  和  $b_j$  的两种分布。因此, 将通用信息  $U$  返回给攻击者, 攻击者即使询问随机预言机也无法区分  $U$  的分布, 无法得出任何关于  $b$  的有用信息。

5) 由以上结论可知,  $MS_{[CHKP10]}$  在随机预言机模型下为 IND-ID-CPA 安全, 文献 [7] 已经证明 [CHKP10] 方案在随机预言机模型下为 IND-ID-CPA 安全, 因此, 本方案为随机预言机模型下 IND-ID-CPA 安全。

### 3.3 性能分析

本文构造了一个基于 LWE 问题的高效分层身份基多用户全同态加密方案, 与其他方案相比, 应用场景更广, 效率更高, 具体表现在以下几个方面:

1) 与 [CHKP10] 方案相比, 将一个简单的 HIBE 方案扩展为 multi-identity HibFHE 方案, 应用前景更加广阔, 实现功能更加多样。

2) 与 [GSW13] 方案提出的 HibFHE 方案相比, 将方案的应用场景由单用户扩展到多用户, 实现了不同用户之间密文的同态计算。同态加法和乘法可以通过  $Z_q$  上矩阵的平凡加法和乘法运算实现上的加法乘法运算, 效率更高, 密文运算后维度不变。并利用 [GSW13] 方案的校平技术, 将噪声控制在  $\omega(\kappa N + 1)^L B$  之内, 保证了解密的正确性。

3) 与 [CM15] 方案相比, 本方案虽然使用相同的转化机制, 但本方案采用的身份基方案为随机预言机模型下的 [CHKP10] 方案, 而 [CM15] 方案采用 [GPV08] 方案。由于 RO 模型下的 [CHKP10] 方案相比 [GPV08] 方案在公钥规模、私钥规模、密文尺寸方面都有一定优势, 并且实现了分层功能, 因此, 在安全性相同(都能达到 RO 模型下的选择安全)的情况下, 本方案的密钥更新时间相对更短、效率更高。具体分析见表 1、表 2。

表 1 本文方案与 [GSW13] 方案和 [CHKP10] 方案的对比

Tab. 1 Comparison of the proposed scheme with scheme [CHKP10] and scheme [GSW13]

方案	同态操作	分层性质	多用户
[GSW] 方案	YES	YES	NO
[CHKP10] 方案	NO	YES	NO
本文方案	YES	YES	YES

表 2 本文方案与 [CM15] 方案的比较

Tab. 2 Comparison of the proposed scheme with scheme [CM15]

方案	公钥规模	私钥规模	密文尺寸	是否支持分层	密钥更新周期	困难性假设
[CM15] 方案	$O(n(m+n)\log q)$	$O(mn \log q)$	$O(\kappa^2 m \log^2 q)$	否	长	LWE 问题
本文方案	$O(n(m+1)\log q)$	$O(m \log q)$	$O(\kappa^2 n \log^2 q)$	是	短	LWE 问题



## 4 结语

本文基于 LWE 问题,利用[CM15]方案中的转化机制,结合[CHKP10]方案,构造了一个高效的分层身份基多用户全同态加密方案,并证明了该方案为随机预言机模型下的 IND-ID-CPA 安全。通过对比分析,本方案应用场景更广、效率更高。

与身份加密相比,属性加密(ABE)能够实现更细粒度的访问控制和一对多的加解密<sup>[17]</sup>。后续工作将研究多密钥全同态加密方案与属性加密的结合,实现属性基多用户全同态加密方案。

### 参考文献 (References)

- [1] GENTRY C. Fully homomorphic encryption using ideal lattices [C]// STOC 2009: Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing. New York: ACM, 2009: 169–178.
- [2] GENTRY C, HALEVI S. Implementing Gentry’s fully-homomorphic encryption scheme [C]// EUROCRYPT 2011: Proceedings of the 2011 Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 6632. Berlin: Springer, 2011: 129–148.
- [3] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping [C]// ITCS ’12: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. New York: ACM, 2012: 309–325.
- [4] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based [C]// CRYPTO 2013: Proceedings of the 2013 Advances in Cryptology, LNCS 8042. Berlin: Springer, 2013: 75–92.
- [5] 陈智罡. 基于格的全同态加密研究与设计[D]. 南京: 南京航空航天大学, 2015: 23. ( CHEN Z G. Research and design of fully homomorphic encryption based on lattice [D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2015: 23. )
- [6] CLEAR M, McCOLDRICK C. Multi-identity and multi-key leveled FHE from learning with errors [C]// Proceedings of the 2015 Annual Cryptology Conference, LNCS 9216. Berlin: Springer, 2015: 630–656.
- [7] CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate a lattice basis [C]// Proceedings of the 2010 Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 6110. Berlin: Springer, 2010: 523–552.
- [8] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions [C]// STOC ’08: Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM, 2008: 197–206.
- [9] 李增鹏, 马春光, 周红生. 全同态加密研究[J]. 密码学报, 2017, 4(6): 561–578. ( LI Z P, MA C G, ZHOU H S. Overview on fully homomorphic encryption [J]. Journal of Cryptologic Research, 2017, 4(6): 561–578. )
- [10] MICCIANCIO D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions [J]. Computational Complexity, 2007, 16(4): 365–411.
- [11] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [C]// Proceedings of the 2001 Annual International Cryptology Conference, LNCS 2139. Berlin: Springer, 2001: 213–229.
- [12] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proceedings of the 1984 Workshop on the Theory and Application of Cryptographic Techniques, LNCS 196. Berlin: Springer, 1984: 47–53.
- [13] 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: ACM, 2005: 84–93.
- [14] PEIKERT C. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract [C]// STOC ’09: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009: 333–342.
- [15] REGEV O. The learning with errors problem (invited survey) [C]// Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity. Piscataway, NJ: IEEE, 2010: 191–204.
- [16] 周潭平. 基于 GLWE 问题的密码体制研究与设计[D]. 西安: 武警工程大学, 2014: 13. ( ZHOU T P. Research and design of cryptosystem based on GLWE problem [D]. Xi'an: Engineering University of the Chinese People's Armed Police Force, 2014: 13. )
- [17] 石悦, 李相龙, 戴方芳. 一种基于属性基加密的增强型软件定义网络安全框架[J]. 信息网络安全, 2018(1): 15–22. ( SHI Y, LI X L, DAI F F. An enhanced security framework of software defined network based on attribute-based encryption [J]. Netinfo Security, 2018(1): 15–22. )

This work is partially supported by the National Key Research and Development Program of China (2017YFB0802000), the National Natural Science Foundation of China (U1636114, 61772550, 61572521), the National Cryptography Development Fund of China (MMJJ20170112).

**TU Guangsheng**, born in 1992, M. S. candidate. His research interests include information security, homomorphic cryptology.

**YANG Xiaoyuan**, born in 1959, M. S., professor. His research interests include information security, cryptography.

**ZHOU Tanping**, born in 1989, Ph. D. His research interests include information security, homomorphic cryptology.