具有短密文的多身份全同态加密构造框架

王学庆[1,2], 王 彪[1,2], 薛 锐[1,2]

[1] 中国科学院信息工程研究所信息安全国家重点实验室 北京 中国 100093
[2] 中国科学院大学网络空间安全学院 北京 中国 100049

摘要 类似于多密钥全同态加密 (Multi-key Fully Homomorphic Encryption, MFHE), 多身份全同态加密 (Multi-id Identity- based Fully Homomorphic Encryption, MIBFHE) 允许对不同用户的密文进行关于任意函数的同态计算, 且后者因具有加密密钥易获取、密钥托管和密钥撤销易实现等特点, 具有更深远的应用前景。

Canetti 等人在 PKC 2017 上给出了一个框架, 可将身份加密方案(Identity-based Encryption, IBE)和 MFHE 方案转换成 MIBFHE 方案。若用基于 DLWE 假设的 IBE 方案和 Brakerski 与 Perlman 的全动态①MFHE 方案(以下简称 BP 方案), 可得到全动态的 MIBFHE 方案, 但密文规模较大, 为 $\mathrm{O}(n^5\log^5 q)$, 这里 n, q 是 DLWE 假设的参数, 且紧致性相比于 MFHE 方案变弱。因密文规模是影响通信效率的主要因素, 本文构造了一个密文规模较小和紧致性较强的 MIBFHE 方案框架, 且仅用了 MFHE 这一个构件, 然后用 BP 方案去实例化, 得到了全动态的、选择性安全的 MIBFHE 方案, 其密文规模为 $\mathrm{O}(n\log q)$.

关键词 多身份的身份全同态加密; 多密钥的全同态加密; 全同态加密; 身份加密
中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2018.09.05

A Framework of Multi-id Identity-based Fully Homomorphic Encryption with Short Ciphertexts

WANG Xueqing[1,2], WANG Biao[1,2], XUE Rui[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Similar to Multi-key Fully Homomorphic Encryption (MFHE), Multi-id Identity-based Fully Homomorphic Encryption (MIBFHE) allows to homomorphically compute on ciphertexts under different users for any computable functions. And MIBFHE may be more useful in practice since it has advantages including that encryption keys are easy to obtain, for the sender, from system parameters and some unique information of the receiver's identity, and that key escrow and key revocation are easily achievable.

Canetti et al., at PKC 2017, proposed a framework of transforming identity-based encryption (IBE) schemes and MFHE schemes into MIBFHE schemes. If we exploit a DLWE-based IBE scheme and Brakerski and Perlman's MFHE scheme (abbr. BP scheme), we will obtain a fully dynamic MIBFHE scheme with ciphertext size $\mathrm{O}(n^5\log^5 q)$, where n, q are proper parameters for DLWE assumption. And additionally, the compactness of MIBFHE is weaker than that of MFHE. In this paper, we only exploit MFHE to construct a MIBFHE framework with smaller ciphertexts and stronger compactness. And then we initiate it with the BP scheme to obtain a fully dynamic and selective secure MIBFHE scheme, whose ciphertext size is $\mathrm{O}(n\log q)$.

Key words: multi-id identity-based fully homomorphic encryption; multi-key fully homomorphic encryption; fully homomorphic encryption; identity-based Encryption

1 引言

全同态加密 (Fully Homomorphic Encryption, FHE) 是一个密码学原语, 它的功能是允许任何人对密文进行任意计算, 满足这样的实际需求: 拥有较少资源的用户, 既能保护持有数据的隐私性, 又能

①全动态是指允许任意多个用户随时可以参与同态计算。

通讯作者: 薛锐, 博士, 研究员, Email: xuerui@iie.ac.cn.

本课题得到国家自然基金项目(No. 61472414; No. 61772514; No. 61602061)资助。
收稿日期: 2017-05-02; 修改日期: 2017-07-03; 定稿日期: 2018-08-20

利用拥有较多资源服务器的强大计算能力, 适用于安全计算、隐私数据检索等应用场景。同态加密(Homomorphic Encryption, HE)的思想最早由 Rivest, Adleman 和 Dertouzos 在 1978 年提出[1], 虽然出现了很多 HE 方案, 如早于同态思想提出的 RSA 加密方案[2]、El Gamal 加密方案[3]、BGN 加密方案[4], 但是这些方案只满足乘法同态、加法同态或较低次数多项式同态, 直到2009年, Gentry才构造出第一个FHE方案[5]。接下来, 基于不同假设、具有更多功能、更高效或构造思想更自然的 FHE 方案[6-14]如雨后春笋般涌现出来。

在 FHE 的发展过程中, 借鉴在传统公钥加密基础上发展出的密钥生成与管理更方便的身份加密(Identity-based Encryption, IBE)[15], 2010 年, Naccache 将如何构造身份全同态加密 (Identity-based Fully Homomorphic Encryption, IBFHE) 方案作为一个公开问题提出[16]; 2013 年, Gentry, Sahai 和 Waters 首次对这一公开问题作出了正面回答[13], 利用他们基于近似特征向量方法构造的、无需计算密钥的层次型全同态加密 (Leveled Fully Homomorphic Encryption, LFHE) 方案(以下简称 GSW), 给出了一个可将已有基于 DLWE 假设的 IBE 方案, 转换为身份层次型全同态加密 (Identity-based Leveled Fully Homomorphic Encryption, IBLFHE) 方案的框架; 2014 年, Clear 和 McGoldrick 利用不可区分混淆(Indistinguishability Obfuscation, **iO**) 方案和可穿孔的伪随机函数(Puncturable Pseudorandom Function, PPRF)[17], 构造了一个可将 FHE 方案转换为 IBFHE 方案的框架; 2015 年, Clear 和 McGoldrick 在 GSW 的基础上, 给出了可将满足特殊条件的 IBE 方案, 转换为多身份层次型全同态加密 (Multi-id Identity-based Leveled Fully Homomorphic Encryption, MIBLFHE) 方案[18] (以下简称 CM15), 其构造方法也可将 GSW 这一 LFHE 方案转换为多密钥的层次型全同态加密(Multi-key Leveled Fully Homomorphic Encryption, MLFHE) 方案, 从而继 López-Alt 等人的第一个基于非标准假设的 MLFHE 方案[19]之后, 得到了第一个基于 DLWE 这一标准假设的方案。虽然 CM15 利用 Gentry, Peikert 和 Vaikuntannathan 的 IBE 方案[20] (以下简称 GPV) 构造了第一个单跳①的 MIBLFHE 方案, 但是其安全性只能在随机谕言机 (Random Oracle, RO) 模型下得到证明, 且其构造方法晦涩复杂。

在 CM15 的基础上, MFHE 的研究取得了较大的进展, 2016 年, Mukherjee 和 Wichs 简化了 CM15 的构造方法, 得到了一个简洁自然的、单跳的 MLFHE 方案 (以下简称 MW16)[21]; 同年, Brakerski 和 Perlman 将 MW16 中的简洁方法用于多密钥的同态解密, 得到了一个短密文的、全动态的 MFHE 方案 (以下简称 BP 方案)[22]; 几乎同时, Peikert 和 Shiehian 灵活化了 MW16 的构造方法, 得到了两个多跳的 MLFHE 方案[23]。

关于 MIBFHE 的发展, 2017 年, Canetti 等人借鉴 Brakerski 等人构造多属性全同态加密的方法[24], 给出了一个构造框架[25], 他们利用 IBE 方案和 MFHE 方案这两种构件。另外, 为了得到同时实现全动态和全同态的 MIBFHE 方案, 我们可以用满足这两个性质的 BP 方案和基于 DLWE 假设的 IBE 方案去实例化, 得到的方案密文规模为 $\mathrm{O}\left(n^5 \log^5 q\right)$, 这里 n, q 是 DLWE 假设的参数。因密文规模是影响通信效率的关键因素, 故考虑如何构造密文规模更小的 MIBFHE 方案, 是一个具有重要理论意义和实际价值的问题。

1 我们的工作

首先, 我们在第 3 节构造了一个可将 MFHE 方案转换成 MIBFHE 方案的框架。经过观察, 我们发现 Canetti 等人的框架有两点不足: (i) 密文规模较大; (ii) 即使 MFHE 的同态结果密文规模不依赖于输入密文数, MIBFHE 的同态结果密文规模也与输入密文数成正比, 即 MIBFHE 的紧致性比 MFHE 的变弱, 而导致这两点不足的原因是: 密文不仅包括用 MFHE 的公钥 pk 对消息的加密, 还包括 pk 和 IBE 的用户公钥 (mpk, id) 对 MFHE 的私钥 sk 的加密。因密文规模是影响通信效率的关键因素, 从实际应用出发, 我们应考虑如何减小密文规模。为了消除这两点不足, 我们考虑只在密文中保留对消息的加密这一部分, 那么就需要用于加密消息的 MFHE 的 pk 与 id 有关, 为了能够解密, 用 MFHE 的 sk 作为 sk_{id}, 从而需要将 id 嵌入 (pk, sk) 的生成过程, 一般的方法是将 id 与生成 (pk, sk) 所用的随机串进行关联, 可用 PRF 实现与 id 相关的随机性, 而为了在证明中划分挑战身份 id^*和解密密钥查询的身份集合$\{id_i\}$, 我们采用 PPRF 实现, 这样我们把 PPRF 的密钥作为方案的主私钥, 为了公布与 sk_{id} 配对的 pk_{id}, 可用 iO 实现, 从而得到了只用 MFHE 构造 MIBFHE 的框架。

① 同态计算的结果密文不能继续参加有新用户参与的同态计算。

虽然我们用到了 iO 这一复杂度较高的工具, 但因只影响到主公钥 mpk 的规模, 且主公钥是公共的, 相比于密文规模, 对通信效率影响较小。

然后, 我们在第 4 节用 BP 方案[22]对第 3 节中构造的框架进行实例化, 得到了同时满足全动态和全同态性质的、密文规模为 $\mathrm{O}(n\log q)$ 的 MIBFHE 方案, 且该方案的紧致性比 Canneti 等人方案的紧致性强。

2 基本概念

在这一章我们将给出本文将要用到的相关符号和概念的定义。

本文约定用 $a \leftarrow_R A$ 表示从集合 A 中均匀随机选取元素 a, 用 $\leftarrow$ (除映射外)表示概率性得出, 用 $:=$ 表示其左边的结果由其右边确定性计算得出, 用 PPT (Probabilistic Polynomial Time) 表示概率多项式时间, 用 $[n]$ 表示集合 $\{1,2,\cdots,n\}$, 令 $\ell_q := \lceil \log_2 q \rceil$.

2.1 带错学习问题(Learning with Errors, LWE)

LWE 问题是带噪声校验位学习 (Learning Parity with Noise, LPN) 问题的一个扩展, 最初由 Regev 提出[26], 有搜索性和判定性两种形式, 通过设置合适的参数, 搜索性 LWE 与判定性 LWE (Decisional LWE, DLWE) 问题的困难性等价, 下面只给出判定性 LWE 问题的定义:

定义 1. 对于任意安全参数 λ, 设两个整数 $n=n(\lambda), q=q(\lambda)\geqslant 2$, 一个支撑集为 $\mathbb{Z}$ 的分布 $\chi=\chi(\lambda)$, 用 $\mathrm{DLWE}_{n,q,\chi}$ 表示的 DLWE 问题是指区分 $\left\{U(\mathbb{Z}_q^{n+1}) := (\vec{a}_i, b_i)\right\}_{\vec{a}_i\leftarrow_R\mathbb{Z}_q^n, b_i\leftarrow_R\mathbb{Z}_q}$ 与 $\left\{A_{\vec{s},\chi} := (\vec{a}_i, \langle\vec{a}_i,\vec{s}\rangle + e_i)\right\}_{\vec{s},\vec{a}_i\leftarrow_R\mathbb{Z}_q^n, e_i\leftarrow\chi}$ 这两个分布。$\mathrm{DLWE}_{n,q,\chi}$ 假设是指不存在求解 $\mathrm{DLWE}_{n,q,\chi}$ 问题的 PPT 算法。

目前已知 Regev 在 2005 年[26]、Peikert 在 2009 年[27]分别给出了从格上的近似最短向量问题到 $\mathrm{DLWE}_{n,q,\chi}$ 问题的量子归约和经典归约, 由于目前尚无求解格上近似最短向量问题的多项式时间量子算法, 因此也没有求解 $\mathrm{DLWE}_{n,q,\chi}$ 问题的多项式时间量子算法, 进而公认基于 $\mathrm{DLWE}_{n,q,\chi}$ 问题的密码学方案是抗量子攻击的。另外, 这些归约中用到的 χ 都是高斯分布, 而高斯分布与取值恰当的 B_χ 有界分布统计不可区分[11], 因此为了简便, 本文方案中的噪声分布都用 B_χ 有界分布。

下面给出 B_χ 有界分布的定义[11, 13]。

定义 2. 设整数集 $\mathbb{Z}$ 上的一个概率分布总体 $\{\chi_n\}_{n\in\mathbb{N}}$, 对于任意常数 $B_\chi>0$, 若 $\Pr_{e\leftarrow\chi_n}\left[|e|>B_\chi\right]=\mathbf{negl}(n)$ 成立, 则称该概率分布总体是 B_χ 有界的。

2.2 多身份全同态加密(Multi-id Identity-based Fully Homomorphic Encryption, MIBFHE)

若一个 IBFHE 方案能同态计算用不同身份加密得到的密文, 则称它是多身份的。基于安全性考虑, MIBFHE 要求只有联合参与同态计算的所有用户, 才能对结果密文进行正确解密。

一个 MIBFHE 方案由以下五个多项式时间算法构成:

-**Setup** $\left(1^\lambda\right)\rightarrow(mpk, msk)$: 概率性的系统参数生成算法 **Setup** 以安全参数 1^λ 为输入, 生成公共参数 mpk 和主私钥 msk.

-**KeyGen** $(msk, id)\rightarrow sk_{id}$: 概率性或确定性的解密密钥生成算法 **KeyGen** 以主私钥 msk 和身份标识 id 为输入, 生成 id 对应的解密密钥 sk_{id}.

-**Enc** $(mpk, id, \mu)\rightarrow c_{id}$: 概率性的加密算法 **Enc** 以公共参数 mpk, 身份标识 id 和消息 μ 为输入, 生成只能用 sk_{id} 解密的密文 c_{id}.

-**Eval** $\left(mpk, f, (c_1,\cdots,c_t)\right)\rightarrow\hat{c}$: 概率性或确定性的同态计算算法 **Eval** 以公共参数 mpk, 电路 f 和与其输入数相同个数的一组密文 $c_1,\cdots,c_t$ 为输入, 这些密文可能对应不同的身份标识 id, 生成结果密文 $\hat{c}$.

-**Dec** $\left(\left(sk_{id_1},\cdots,sk_{id_N}\right),\hat{c}\right)\rightarrow\mu$: 确定性的解密算法 **Dec** 以密文 $\hat{c}$ 和与其对应所有身份标识的解密密钥 $\left(sk_{id_1},\cdots,sk_{id_N}\right)$ 为输入, 联合解密得出消息 μ。

一个 MIBFHE 方案的一些性质定义如下:

-**全动态性。**设 $N=N(\lambda), t=t(\lambda)$, 对任一可同态计算的电路 f, 任意 $\left(id_1,\cdots,id_N\right)$ 和 $\left(\hat{c}_1,\cdots,\hat{c}_t\right)$, 满足 **Dec** $\left(\left(sk_{id_1},\cdots,sk_{id_{js_j}}\right),\hat{c}_j\right)=\mu_j$, 这里 $j\in[t], s_j\in[N]$, $\left\{sk_{id_{j1}},\cdots,sk_{id_{js_j}}\right\}\subseteq\{sk_1,\cdots,sk_N\}$, $(mpk, msk)\leftarrow\mathbf{Setup}(1^\lambda)$, 对于所有的 $i\in[N]$,

$sk_{id_i} \leftarrow \mathbf{KeyGen}(msk, id_i)$, 若

$\Pr[\mathbf{Dec}\big((sk_1,\cdots,sk_N),\mathbf{Eval}\big(mpk, f, (\hat{c}_1,\cdots,\hat{c}_t)\big)\big) \neq f(\mu_1,\cdots,\mu_t)] = \mathbf{negl}(\lambda)$ 成立, 则称 MIBFHE 方案具有全动态性; 否则, **Setup** 算法以 N 作为输入, 即预先给定可参与同态计算的最大用户数。注意, 这里隐含了方案正确性的定义。

-紧致性。对于任意的同态计算结果密文 $\hat{c} \leftarrow \mathbf{Eval}\big(mpk, f, \{c_i\}\big)$, 存在一个多项式 $\mathbf{poly}(\cdot)$, 使得 $|\hat{c}| \leqslant \mathbf{poly}(\lambda)$, 其中 $\mathbf{poly}(\cdot)$ 独立于电路 f 的规模、深度、输入密文数或不同用户数①。

-全同态性。若 f 是任意多项式深度的电路, 即方案可用于同态计算任意多项式深度的电路, 则该方案被称为全同态加密方案; 否则, 若 **Setup** 算法以 L 作为输入, 即预先给定可同态计算电路的最大深度, 则称该方案是层次型全同态加密方案 (Leveled Fully Homomorphic Encryption, LFHE).

-安全性。 MIBFHE 方案的安全性定义与 IBE 的相同, 一般考虑 IND-aID-CPA (又称适应安全性) 和 IND-sID-CPA (又称选择安全性) 这两种安全性, 下面给出 IND-sID-CPA 安全性的形式化定义。

IND-sID-CPA 安全性实验由挑战者 **C** 与敌手 **A** 交互执行:

初始化阶段: A 向 **C** 提交将要挑战的身份标识 id^*;

参数生成阶段: C 根据方案生成 mpk 和 msk, 并将 mpk 发送给 **A**;

解密密钥查询阶段(挑战前): A 选择除 id^* 以外的任意身份标识 id 对解密密钥 oracle 进行多项式次询问, **C** 充当解密密钥 oracle, 回答与 id 对应的解密密钥;

挑战阶段: A 向 **C** 提交 (μ_0, μ_1), 要求 μ_0 与 μ_1 等长, **C** 随机选择 $b \in \{0,1\}$, 调用加密算法生成 μ_b 的密文 c_{id^*} 发送给 **A**;

解密密钥查询阶段(挑战后): A 可以继续选择除 id^* 以外的任意身份标识 id 对解密密钥 oracle 进行多项式次询问, **C** 按照挑战前的方式进行回答;

猜测阶段: A 向 **C** 提交对 b 的猜测 b', 若 $b' = b$, 则输出 1, 否则输出 0.

IND-aID-CPA 安全性定义与 IND-sID-CPA 安全性定义的区别是: 敌手 **A** 在挑战阶段与消息一起选择并提交挑战身份 id^*.

注: 因 MIBFHE 方案是对 IBE, FHE, MFHE 方案的扩展, 由 MIBFHE 的定义易得出后三种方案的定义, 故在此只给出 MIBFHE 的定义。

2.3 不可区分混淆 (Indistinguishability Obfuscation, iO)

iO 作为对虚拟黑盒 (Virtual Black Box, VBB) 混淆的一种弱化方案, 最初由 Barak 等人[28]在 2001 年提出, 它用来保证任意两个功能相同的电路混淆后计算不可区分。

定义 3. 设 **iO** 为一致的 PPT 算法, 若对于一个电路分布簇 $\{C_\lambda\}$, 若 **iO** 满足以下两个条件:

-正确性。对于任一安全参数 $\lambda \in \mathrm{N}$, 任一电路 $C \in C_\lambda$, 任一输入 x, 都有

$$\Pr\big[C'(x) = C(x) : C' \leftarrow \mathbf{iO}(\lambda, C)\big] = 1;$$

-不可区分性。对任意 PPT 敌手 $(\mathbf{Samp}, \mathbf{D})$, $(C_0, C_1, \tau) \leftarrow \mathbf{Samp}(1^\lambda)$, 都存在一个关于 λ 的可忽略函数 ε_{iO}, 使得如果 $\Pr\big[C_0(x) = C_1(x) \text{ for } \forall x\big] > 1 - \varepsilon_{iO}$, 那么 $\big|\Pr\big[\mathbf{D}(\tau, \mathbf{iO}(\lambda, C_0)) = 1\big] - \Pr\big[\mathbf{D}(\tau, \mathbf{iO}(\lambda, C_1)) = 1\big]\big| \leqslant \varepsilon_{iO}$. 则称 **iO** 为不可区分混淆方案。

2.4 可穿孔的伪随机函数 (Puncturable Pseudorandom Function, PPRF)

PPRF 作为一类简单的受限 PRF, 最初由 Sahai 和 Waters 在 2014 年提出[29], 它允许 PPT 敌手首先给定一个多项式规模的输入集合, 即使给敌手一个计算密钥, 该密钥可用来计算除此集合之外所有输入的函数值, 它也难以区分一个值是此集合中输入的函数值还是一个等长的随机元素。

定义 4. 一个可穿孔的伪随机函数 $\mathbf{F} : \mathrm{K} \times \{0,1\}^k \to \{0,1\}^m$ 有两个算法 $(\mathbf{Key}, \mathbf{Puncture})$, 满足以下两个条件:

-穿孔外的功能不变性。对于任意 PPT 敌手 **A**, $\{0,1\}^{k(\lambda)} \supseteq S \leftarrow \mathbf{A}(1^\lambda)$, 对于所有不在 S 中的 $x \in \{0,1\}^{k(\lambda)}$, $\Pr[\mathbf{F}(K, x) = \mathbf{F}(K(S), x) : K \leftarrow \mathbf{Key}(1^\lambda), K(S) \leftarrow \mathbf{Puncture}(K, S)] = 1$ 成立。

-穿孔处的伪随机性。对于任意 PPT 敌手 $(\mathbf{A}_1, \mathbf{A}_2)$, 有 $|\Pr[\mathbf{A}_2(K(S), x, \mathbf{F}(K, x)) = 1] - \Pr[\mathbf{A}_2(K(S), x, y \leftarrow_R \{0,1\}^m) = 1]| \leqslant \mathbf{negl}(\lambda)$ 成立, 其中 $\{0,1\}^{k(\lambda)} \supseteq S \leftarrow \mathbf{A}_1(1^\lambda), x \in S, K \leftarrow \mathbf{Key}(1^\lambda), K(S) \leftarrow \mathbf{Puncture}(K, S)$.

① 因本文用于实例化的 BP 方案只关于电路的规模和输入数具有紧致性, 故我们得到的 MIBFHE 方案也只关于电路的规模和输入数具有紧致性, 即这里的 **poly** 只独立于电路规模和输入数, 是关于安全参数、电路深度和不同用户数的函数。

2.5 Brakerski 和 Perlman 的全动态多密钥全同态加密方案

Brakerski 和 Perlman 在 CRYPTO 2016 给出的方案[22]是目前已知的唯一一个全动态 MFHE 方案, 其中用到一个特殊矩阵 $G := I_{n+1} \otimes \vec{g}^T$, 这里 I_{n+1} 表示 $(n+1)$ -阶单位矩阵, $\vec{g}^T = (2^0, 2^1, 2^2, \cdots, 2^{\ell_q - 1})$ [30], 下面给出该方案的一个简要描述。

-BP. Setup (1^λ): 生成 $\mathrm{DLWE}_{n,q,\chi}$ 假设成立的参数 q, n, m, χ, B_χ, 其中 q 是模数, n 是维数, $m = (n+1)\ell_q$, B_χ -有界的分布 χ 是噪声分布, $B \leftarrow_R \mathbb{Z}_q^{n \times m}$, 输出 $PP = (q, n, m, \chi, B_\chi, B)$.

-BP. KeyGen (PP): 随机选取 $\vec{s} \leftarrow_R \mathbb{Z}_q^n, \vec{e} \leftarrow \chi^m$,

$$A := \begin{pmatrix} \vec{s}^T B + \vec{e}^T \\ -B \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m}, sk := (1, \vec{s}^T)^T \in \mathbb{Z}_q^{n+1},$$

令 $\mathbf{Bit}(sk)$ 表示 sk 的比特分解

对于 $i \in [m], R_i \leftarrow_R \{0,1\}^{m \times m}$

$$\vec{S}[i] := AR_i + \mathbf{Bit}(sk)[i] \cdot G$$

对于

$j_1 \in [m], j_2 \in [m], R_{j_1, j_2} \leftarrow_R \{0,1\}^{m \times m}$, $\vec{R}[i, j_1, j_2]$:

$$= AR_{j_1, j_2} + R_i[j_1, j_2] \cdot G$$

输出

$pk := (A, \vec{S}, \vec{R}) \in \mathbb{Z}_q^{(n+1)\times m} \times (\mathbb{Z}_q^{(n+1)\times m})^m \times (\mathbb{Z}_q^{(n+1)\times m})^{m^3}$ 和 sk.

-BP. Enc $(pk, \mu \in \{0,1\})$: 随机选取 $\vec{r} \leftarrow_R \{0,1\}^m$,

$\vec{c} := A\vec{r} + (\mu \cdot \left\lfloor \frac{q}{2} \right\rfloor, \vec{0}) \in \mathbb{Z}_q^{n+1}$, 输出 $\vec{c}$.

-BP. Eval $(pk, f, (\vec{c}_1, \cdots, \vec{c}_t))$: 由于对于该算法的描述还需要其他背景知识, 过程较复杂, 根据本文需要, 在此不赘述, 请参见文献[22].

-BP. Dec $((sk_1, \cdots, sk_N), \vec{c} \in \mathbb{Z}_q^{(n+1)N})$:

计算 $\delta := \langle (sk_1, \cdots, sk_N), \vec{c} \rangle$, 若 $\delta \leqslant \frac{q}{4}$, 则输出 0, 否则输出 1.

2.6 Canetti 等人的多身份全同态加密构造框架

设 (**MFHE. Setup**, **MFHE. KeyGen**, **MFHE. Enc**, **Eval**, **MFHE. Dec**) 是一个 MFHE 方案, (**IBE. Setup**, **IBE. KeyGen**, **IBE. Enc**, **IBE. Dec**) 是一个 IBE 方案, Canetti 等人[24]利用这两类方案构造了多身份的身份全同态加密方案, 其主要思想是将身份标识到加密密钥的映射与密文计算分开, 即利用 IBE 方案的从身份标识到加密密钥的映射, 和 MFHE 方案的同态计算能力, 既避免了仅利用 IBE 存在密文扩展问题所导致的无法利用已有的适应性安全方案问题, 又解决了仅利用 MFHE 方案存在的身份标识到加密密钥的映射问题。该思想与 Brakerski 等人[25]利用属性加密和多密钥全同态加密构造多属性全同态加密的思想相同。

-Setup (1^λ): $PP_{MFHE} \leftarrow \mathbf{MFHE.Setup}(1^\lambda)$,

$(mpk_{IBE}, msk_{IBE}) \leftarrow \mathbf{IBE.Setup}(1^\lambda)$

输出 $mpk := (PP_{MFHE}, mpk_{IBE})$, $msk := msk_{IBE}$.

-KeyGen (msk, id):

输出 $sk_{id} \leftarrow \mathbf{IBE.KeyGen}(msk_{IBE}, id)$.

-Enc (mpk, id, μ): 将 mpk 分解为

(PP_{MFHE}, mpk_{IBE}),

$(pk_{MFHE}, sk_{MFHE}) \leftarrow \mathbf{MFHE.KeyGen}(PP_{MFHE})$,

$c_{id}^1 \leftarrow \mathbf{MFHE.Enc}(pk_{MFHE}, \mu)$,

$c_{id}^2 \leftarrow \mathbf{IBE.Enc}(mpk_{IBE}, id, sk_{MFHE})$,

输出 $c_{id} := (id, pk_{MFHE}, c_{id}^1, c_{id}^2)$.

-Eval $(f, (c_1, \cdots, c_t))$:

假设 $c_1, \cdots, c_t$ 对应不同的身份下标集合 $I_1, \cdots, I_t$,

且满足 $\{id_i\}_{i \in I_1} \cup \cdots \cup \{id_i\}_{i \in I_t} = \{id_1, \cdots, id_N\}$

对于所有的 $i \in [t]$, 将 c_i 分解为

$(\{id_j\}_{j \in I_i}, \{pk_{MFHE,j}\}_{j \in I_i}, c^1_{\{id_j\}_{j \in I_i}}, c^2_{\{id_j\}_{j \in I_i}})$,

$c^1_{\{id_i\}_{i \in [N]}} \leftarrow \mathbf{MFHE.Eval}(\{pk_{MFHE,i}\}_{i \in [N]}, f,$

$(c^1_{\{id_i\}_{i \in I_1}}, \ldots, c^1_{\{id_i\}_{i \in I_t}}))$, $c^2_{\{id_i\}_{i \in [N]}} := (c^2_{\{id_i\}_{i \in I_1}}, \ldots, c^2_{\{id_i\}_{i \in I_t}})$,

输出 $c_{\{id_i\}_{i \in [N]}} := (\{id_i\}_{i \in [N]}, \{pk_{MFHE,i}\}_{i \in [N]},$

$c^1_{\{id_i\}_{i \in [N]}}, c^2_{\{id_i\}_{i \in [N]}})$.

-Dec $((sk_{id_1}, \cdots, sk_{id_N}), c_{\{id_i\}_{i \in [N]}})$:

首先将 $c_{\{id_i\}_{i \in [N]}}$ 分解为

$(\{id_i\}_{i \in [N]}, \{pk_{MFHE,i}\}_{i \in [N]}, c^1_{\{id_i\}_{i \in [N]}}, c^2_{\{id_i\}_{i \in [N]}})$,

然后将 $c^2_{\{id_i\}_{i \in [N]}}$ 分解为 $(c^2_{id_1}, \cdots, c^2_{id_N})$, 对于所有的 $i \in [N]$, $sk_{MFHE,i} := \mathbf{IBE.Dec}(sk_{id_i}, c^2_{id_i})$, 输出

$\mu := \mathbf{MFHE.Dec}((sk_{MFHE,1}, \cdots, sk_{MFHE,N}), c^1_{\{id_i\}_{i \in [N]}})$.

观察以上构造, 我们发现其新鲜密文不仅包括对消息的加密, 还包括 **MFHE** 的公钥 pk 和 **IBE** 对 **MFHE** 的私钥 sk 的加密, 另外, 其同态计算中的结果密文不得不包括所有输入密文中 **MFHE** 私钥 sk 的密文的级联, 因此即使 **MFHE** 紧致性较强 (如同态结果密文规模仅与不同 id 数有关, 而与输入密文

数无关), **MIBFHE** 的同态结果密文规模也与输入密文数成正比。

为了从以上构造中得到全动态的多身份全同态加密方案, 目前我们可以用基于 $\mathrm{DLWE}_{n,q,\chi}$ 假设的 IBE 方案和 BP 方案去实例化, 因已有的基于 $\mathrm{DLWE}_{n,q,\chi}$ 假设的 IBE 方案[20, 31-32]的密文空间最小为 $\mathbb{Z}_q^m$, 根据 2.5 节, 我们知道 BP 方案的公钥空间为 $\mathbb{Z}_q^{(n+1)\times m}\times(\mathbb{Z}_q^{(n+1)\times m})^m\times(\mathbb{Z}_q^{(n+1)\times m})^{m^3}$ 和密钥空间为 $\mathbb{Z}_q^{n+1}$, 故实例化得到的多身份全同态加密方案的密文规模为 $\mathrm{O}\left(n^5\log^5 q\right)$.

3 具有较短密文和较强紧致性的多身份全同态加密构造框架

如前所述, 我们仅利用 MFHE 这一个构件去构造 MIBFHE, 具体地, 将 *id* 与生成 MFHE 的 (*pk, sk*) 的随机串关联, 嵌入到其生成算法 **KeyGen** 中, 因已有 MFHE 方案 **KeyGen** 算法中的随机元素是从 $\mathbb{Z}_q$ 或 $\mathbb{Z}$ 中, 根据均匀分布或高斯分布选取出的向量或矩阵, 我们不是简单地利用一个 PPRF, 而是针对每一类随机元素, 增加概率抽样算法, 作为 PPRF 生成的随机串与 **KeyGen** 算法所用随机元素之间的桥梁, 也就是将 PPRF 生成的随机串作为概率抽样算法的随机串, 概率抽样算法的输出作为 **KeyGen** 算法的随机元素, 从而使得 PPRF 的输入 *id* 决定 **KeyGen** 算法的输出 $\left(pk_{id}, sk_{id}\right)$,

设 (**MFHE. Setup**, **MFHE. KeyGen**, **MFHE. Enc**, **MFHE. Eval**, **MFHE. Dec**) 是一个 MFHE 方案, 构造的 MIBFHE 方案的身份标识空间为 $\{0,1\}^k$, 噪声分布为 B_χ -有界分布 χ, **iO** 是一个不可区分混淆方案, $\mathbf{F}:\mathrm{K}\times\{0,1\}^k\to\Re_{SampleU}\times\Re_{SampleE}$ 是一个 PPRF, 其中 $\Re_{SampleU},\Re_{SampleE}$ 分别是概率算法 **SampleU**, **SampleE** 的随机数空间, 这里 **SampleU**(A_1,U) 是指从集合 A_1 中按照均匀分布 U 随机抽取出一个元素, **SampleE**(A_2,χ) 是指从集合 A_2 中按照噪声分布 χ 随机抽取出一个元素。

-MIBFHE. Setup (1^λ): $PP\leftarrow$ **MFHE. Setup** (1^λ), $K\leftarrow$ **F. Key** (1^λ), 令 **H** 为程序 $\mathbf{F}_{\mathbf{MapPK}}$ (见图 1)的一个混淆 **iO** $(1^\lambda,\mathbf{F}_{\mathbf{MapPK}})$, 输出 $mpk:=(PP,\mathbf{H})$, $msk:=(PP,K)$.

-MIBFHE. KeyGen $(msk, id\in\{0,1\}^k)$: $(r_{id}^1,r_{id}^2):=\mathbf{F}(K,id)$, $R_{id}:=\mathbf{SampleU}(A_1,U;r_{id}^1)$, $E_{id}:=\mathbf{SampleE}(A_2,\chi;r_{id}^2)$, $(pk_{id},sk_{id}):=$ **MFHE. KeyGen** $(PP;(R_{id},E_{id}))$, 输出 sk_{id}. 注意, 这里的集合 A_1, A_2 由 **MFHE. KeyGen** 算法决定。

-MIBFHE. Enc $(mpk, id\in\{0,1\}^k,\mu)$: $pk_{id}:=\mathbf{H}(id)$, 输出 $c_{id}\leftarrow$ **MFHE. Enc** (pk_{id},μ).

-MIBFHE. Eval $(mpk, f, (c_1,\cdots,c_t))$: 假设 $c_1,\cdots,c_t$ 对应于不同的身份下标集合为 $I_1,\cdots,I_t$, 且满足 $I_1\cup\cdots\cup I_t=\{id_1,\cdots,id_N\}$, 对于任意 $i\in[N]$, $pk_{id_i}:=\mathbf{H}(id_i)$, 输出 $\hat{c}\leftarrow$ **MFHE. Eval** $((pk_{id_1},\cdots,pk_{id_N}), f, (c_1,\cdots,c_t))$.

-MIBFHE. Dec $((sk_{id_1},\cdots,sk_{id_N}),\hat{c})$: 输出 $\mu:=$ **MFHE. Dec** $((sk_{id_1},\cdots,sk_{id_N}),\hat{c})$.

输入: $id\in\{0,1\}^k$

参数: PP, K

1. $(r_{id}^1,r_{id}^2):=\mathbf{F}(K,id)$,
2. $R_{id}:=\mathbf{SampleU}(A_1,U;r_{id}^1)$,
   $E_{id}:=\mathbf{SampleE}(A_2,\chi;r_{id}^2)$,
   $(pk_{id},sk_{id}):=\mathbf{MFHE.KeyGen}(PP;(R_{id},E_{id}))$,
3. 输出 pk_{id}.

图 1 程序 $\mathbf{F}_{\mathbf{MapPK}}$

Figure 1 Program $\mathbf{F}_{\mathbf{MapPK}}$

注: 虽然 **MIBFHE** 因用 **iO** 有较大的公共参数, 但若用相同的 **MFHE** 方案进行实例化, MIBFHE 的密文比 Canneti 等人方案的密文小很多, 而公共参数无需在用户之间传输、甚至无需存储, 对方案使用效率影响较低, 密文则是影响效率的更重要因素, 因此 **MIBFHE** 的整体效率高于 Canneti 等人方案的效率。

定理 1. 若方案 **MFHE** 是 IND-CPA 安全的, **iO** 是一个计算不可区分混淆方案和 **F** 是一个可穿孔的伪随机函数, 则方案 **MIBFHE** 是 IND-sID-CPA 安全的。

证明. 假设存在一个 PPT 的敌手 **A,** 攻击 **MIBFHE** 方案 IND-sID-CPA 安全性的优势为 $\varepsilon_{\mathbf{MIBFHE}}(\lambda)$, 我们将采用实验序列的方式证明 $\varepsilon_{\mathbf{MIBFHE}}(\lambda)$ 可忽略, 其中每个实验都由挑战者 **C** 与敌手 **A** 交互执行:

Game 0. 这是定义 IND-sID-CPA 安全性的原始实验, 首先敌手 **A** 向挑战者提交将要挑战的身份标识 id^*,

然后在参数生成阶段，**C** 调用 $(mpk, msk) \leftarrow \mathbf{MIBFHE.Setup}(1^\lambda)$，并将 mpk 发送给 **A**. 在解密查询阶段，当 **A** 对 id_i 进行查询时，**C** 检查 id_i 是否等于 id^*，若是，则拒绝回答，否则调用 $sk_{id_i} \leftarrow \mathbf{MIBFHE.KeyGen}(msk, id_i)$，将 sk_{id_i} 发送给 **A,** 这样的查询可执行关于 λ 的任意多项式次。在挑战阶段，当收到 **A** 发送的一对等长消息 (μ_0, μ_1) 时，**C** 从 $\{0,1\}$ 中随机选择 b，调用 $c_{id^*} \leftarrow \mathbf{MIBFHE.Enc}(mpk, id^*, \mu_b)$，将 c_{id^*} 发送给 **A.** 在挑战后的解密查询阶段，对于 **A** 的询问，**C** 像挑战前一样处理。在猜测阶段，**A** 发送 b' 给 **C,** 若 $b' = b$，**C** 输出 1，否则输出 0.

Game 1. 在参数生成阶段，**C** 生成 $K \leftarrow \mathbf{F.Key}(1^\lambda)$ 后，调用 $K(\{id^*\}) \leftarrow \mathbf{F.Puncture}(K, \{id^*\})$，在挑战前后的解密密钥查询阶段，**C** 利用 $K(\{id^*\})$ 而不是 K 回答 **A** 的解密查询，其他与 Game 0 中相同。

Game 2. **C** 不在挑战阶段利用 **H** 生成 pk_{id^*}，而是在参数生成阶段如下生成：生成 $K \leftarrow \mathbf{F.Key}(1^\lambda)$ 后，$(r^1_{id^*}, r^2_{id^*}) := \mathbf{F}(K, id^*)$, $R_{id^*} := \mathbf{SampleU}(A_1, U; r^1_{id^*})$, $E_{id^*} := \mathbf{SampleE}(A_2, \chi; r^2_{id^*})$, $(pk_{id^*}, sk_{id^*}) := \mathbf{MFHE.KeyGen}(PP; (R_{id^*}, E_{id^*}))$. 另外，将用来生成 **H** 的程序 $\mathbf{F}_{\mathbf{MapPK}}$ 改变为 $\overline{\mathbf{F}}_{\mathbf{MapPK}}$（见图 2）. 其他与 Game 1 中相同。

输入：$id \in \{0,1\}^k$

参数：$PP, K(\{id^*\}), pk_{id^*}$

1. 若 $id = id^*$，则输出 pk_{id^*}.
2. $(r^1_{id}, r^2_{id}) := \mathbf{F}(K(\{id^*\}), id)$,
3. $R_{id} := \mathbf{SampleU}(A_1, U; r^1_{id})$,
   $E_{id} := \mathbf{SampleE}(A_2, \chi; r^2_{id})$,
   $(pk_{id}, sk_{id}) := \mathbf{MFHE.KeyGen}(PP; (R_{id}, E_{id}))$,
4. 输出 pk_{id}.

图 2　程序 $\overline{\mathbf{F}}_{\mathbf{MapPK}}$

Figure 2　Program $\overline{\mathbf{F}}_{\mathbf{MapPK}}$

Game 3.. **C** 用 $(r^1_{id^*}, r^2_{id^*}) \leftarrow_R \Re_{SampleU} \times \Re_{SampleE}$ 代替 $(r^1_{id^*}, r^2_{id^*}) := \mathbf{F}(K, id^*)$，其他与 Game 2 中相同。

Game 4. **C** 不先选取 $(r^1_{id^*}, r^2_{id^*})$，再分别利用它们作为随机串选取 R_{id^*} 和 E_{id^*}，而是直接选取 R_{id^*} 和 E_{id^*}，以作为 **MFHE.KeyGen** 所用的随机串生成 pk_{id^*}，其他与 Game 3 中相同。

Game 5. **C** 不先选取 R_{id^*} 和 E_{id^*}，而是直接调用 $\mathbf{MFHE.KeyGen}(PP)$ 生成 (pk_{id^*}, sk_{i^*d})，其他与 Game 4 中相同。

接下来对以上实验进行分析，令 S_i 表示敌手 **A** 在 Game i $(0 \leqslant i \leqslant 5)$ 中取得成功这一事件。

因 Game 0 是 IND-sID-CPA 安全性的原始实验，故

$$\left|\Pr[S_0] - \frac{1}{2}\right| = \varepsilon_{\mathbf{MIBFHE}}(\lambda). \tag{1}$$

Game 1 与 Game 0 的唯一不同是在解密密钥查询阶段，Game 0 中 **C** 用 K 回答 **A** 对 id_i 的查询，而 Game 1 中用的是 $K(\{id^*\})$，根据 PPRF 穿孔外的功能不变性，可得对于任意 $id_i \neq id^*$，$\mathbf{F}(K, id_i) = \mathbf{F}(K(\{id^*\}), id_i)$，即这两个实验中的 $(r^1_{id_i}, r^2_{id_i})$ 相等，从而分别用 $(r^1_{id_i}, r^2_{id_i})$ 作为随机串选取的 R_{id_i} 和 E_{id_i} 相等，用 R_{id_i} 和 E_{id_i} 作为 **MFHE.KeyGen** 的随机串生成的 sk_{id_i} 相等，故

$$\Pr[S_1] = \Pr[S_0]. \tag{2}$$

Game 2 与 Game 1 的不同有：(i) pk_{id^*} 的生成位置和生成方式不同；(ii) 用来生成混淆方案 **H** 的程序不同。(i) Game 1 中 **C** 在挑战阶段利用 **H** 生成 pk_{id^*}，而 Game 2 中 **C** 在参数生成阶段直接利用 K，因 Game 1 中生成 **H** 的程序 $\mathbf{F}_{\mathbf{MapPK}}$ 是直接用 K 生成任意 id 对应的 pk_{id}，根据不可区分混淆方案 **iO** 的正确性，得对于 PPT 敌手 **A,** 这两个实验中生成的 pk_{id^*} 相同，且 pk_{id^*} 的生成位置不同对 **A** 的猜测不会有任何影响；(ii) 根据 PPRF 穿孔外的功能不变性，可得对于任意输入 id，$\mathbf{F}_{\mathbf{MapPK}}$ 与 $\overline{\mathbf{F}}_{\mathbf{MapPK}}$ 的输出相同，从而根据不可区分混淆方案 **iO** 的不可区分性，得 **A** 成功区分 $\mathbf{H} \leftarrow \mathbf{iO}(1^\lambda, \mathbf{F}_{\mathbf{MapPK}})$ 与 $\mathbf{H} \leftarrow \mathbf{iO}(1^\lambda, \overline{\mathbf{F}}_{\mathbf{MapPK}})$ 的概率可忽略，设其概率为 $\varepsilon_{\mathbf{iO}}(\lambda)$,

故

$$\left|\Pr[S_2] - \Pr[S_1]\right| = \varepsilon_{\mathbf{iO}}(\lambda). \tag{3}$$

Game 3 与 Game 2 中 $(r^1_{id^*}, r^2_{id^*})$ 的生成方式不同，根据 PPRF 穿孔处的伪随机性，得 **A** 成功区分 $(r^1_{id^*}, r^2_{id^*}) := \mathbf{F}(K, id^*)$ 与 $(r^1_{id^*}, r^2_{id^*}) \leftarrow_R \Re_{SampleU} \times$

$\mathfrak{R}_{SampleE}$ 的概率可忽略, 设其概率为 $\varepsilon_{\mathbf{PPRF}}(\lambda)$, 故

$$\left|\Pr[S_3]-\Pr[S_2]\right|=\varepsilon_{\mathbf{PPRF}}(\lambda). \tag{4}$$

因 Game 3 中 $(r^1_{id^*}, r^2_{id^*})$ 是随机选取的, 敌手 **A** 无法区分以下两种方式: Game 3 中先选随机串再利用随机串选取 R_{id^*} 和 E_{id^*}, Game 4 中在调用生成 R_{id^*} 和 E_{id^*} 的算法时选取所用随机串,

$$\text{故 } \Pr[S_4]=\Pr[S_3]. \tag{5}$$

$$\text{同理有 } \Pr[S_5]=\Pr[S_4]. \tag{6}$$

引理 1. 假设方案 **MFHE** 是 IND-CPA 安全的, 则敌手 **A** 在 Game 5 中的成功优势可忽略。

证明. 利用 **A** 构造攻击 **MFHE** 方案 IND-CPA 安全性的敌手 **B**: **B** 收到自己的挑战者所发送的 (PP, pk) 和 **A** 提交的 id^*, 令 $pk_{id^*}:=pk$, 调用 $K\leftarrow \mathbf{F}.\mathbf{Key}(1^\lambda), K(\{id^*\})\leftarrow \mathbf{F}.\mathbf{Puncture}(K,\{id^*\})$, 利用 PP, pk_{id^*} 和 $K(\{id^*\})$ 作为参数构造程序 $\overline{\mathbf{F}}_{\mathbf{MapPK}}$, 生成 $\mathbf{H}\leftarrow \mathbf{iO}(1^\lambda, \overline{\mathbf{F}}_{\mathbf{MapPK}})$, 将 $mpk:=\mathbf{H}$ 发送给 **A**. 在解密查询阶段, **B** 利用 $K(\{id^*\})$ 生成解密密钥对 **A** 进行回答。在挑战阶段, 收到 **A** 发送的一对等长消息 (μ_0,μ_1), **B** 将其转发给自己的挑战者, 得到密文作为 c_{id^*} 发送给 **A**. 在猜测阶段, 收到 **A** 发送的猜测 b', **B** 将其作为自己的猜测发送给挑战者。

显然我们构造的 **B** 是一个 PPT 敌手, 设其成功优势为 $\varepsilon_{\mathbf{MFHE}}(\lambda):=\left|\Pr[\mathbf{B}\text{成功}]-\frac{1}{2}\right|$, 通过观察, 我们发现 **B** 成功模拟了 Game 5 为 **A** 创设的环境, 因而 $\Pr[\mathbf{B}\text{成功}]=\Pr[\mathbf{A}\text{成功}]=\Pr[S_5]$, 从而

$$\left|\Pr[S_5]-\frac{1}{2}\right|=\varepsilon_{\mathbf{MFHE}}(\lambda), \tag{7}$$

由 **MFHE** 方案的 IND-CPA 安全性, 得 $\varepsilon_{\mathbf{MFHE}}(\lambda)$ 可忽略, 故 **A** 在 Game 5 中的成功优势可忽略。

综合式(1)-(7), 可得

$$\varepsilon_{\mathbf{MIBFHE}}(\lambda)\leqslant \varepsilon_{\mathbf{iO}}(\lambda)+\varepsilon_{\mathbf{PPRF}}(\lambda)+\varepsilon_{\mathbf{MFHE}}(\lambda).$$

4 全动态的多身份全同态加密方案

目前只有 Brakerski 和 Perlman 给出了全动态的 MF HE 方案[22], 现用该方案对第 3 节中的 MIBFHE 框架进行实例化, 因在此实例化中, 只有 **MIBFHE**.**Setup** 和 **MIBFHE**.**KeyGen** 与框架中的相应算法不同, 故下面只给出这两个算法的描述。

设 (**BP. Setup**, **BP. KeyGen**, **BP. Enc**, **BP. Eval**, **BP. Dec**) 是 Brakerski 和 Perlman 的全动态 MFHE 方案, $\mathbf{F}_1:\mathrm{K}_1\times\{0,1\}^k\to\mathfrak{R}_{SampleU1}\times\mathfrak{R}_{SampleE}$, $\mathbf{F}_2:\mathrm{K}_2\times\{0,1\}^k\times[(n+1)\ell_q]\to\mathfrak{R}_{SampleU2}$, $\mathbf{F}_3:\mathrm{K}_3\times\{0,1\}^k\times[m^2(n+1)\ell_q]\to\mathfrak{R}_{SampleU3}$ 是三个 PPRF, $\mathfrak{R}_{SampleU1}, \mathfrak{R}_{SampleE}, \mathfrak{R}_{SampleU2}, \mathfrak{R}_{SampleU3}$ 分别是概率算法 **SampleU1**, **SampleE**, **SampleU2**, **SampleU3** 的随机数空间。

-MIBFHE.**Setup** (1^λ):

$(q,n,m,\chi,B_\chi,B)\leftarrow \mathbf{BP}.\mathbf{Setup}(1^\lambda)$,

$K_1\leftarrow \mathbf{F}_1.\mathbf{Key}(1^\lambda), K_2\leftarrow \mathbf{F}_2.\mathbf{Key}(1^\lambda)$,

$K_3\leftarrow \mathbf{F}_3.\mathbf{Key}(1^\lambda)$, 令 **H** 为程序 $\mathbf{F}_{\mathbf{PK}}$ (见图 3)的一个混淆 $\mathbf{iO}(1^\lambda, \mathbf{F}_{\mathbf{PK}})$, 输出 $mpk:=\mathbf{H}$,

$msk:=(A,K_1,K_2,K_3)$, 其中 mpk, msk 中都隐含参数 q,n,m,χ,B_χ.

-MIBFHE.**KeyGen** $(msk, id\in\{0,1\}^k)$:

$(r^{1,1}_{id}, r^{1,2}_{id}):=\mathbf{F}_1(K_1,id)$,

对于任意 $i\in[(n+1)\ell_q], r^{2,i}_{id}:=\mathbf{F}_2(K_2,id,i)$,

对于任意 $j\in[m^2(n+1)\ell_q], r^{3,j}_{id}:=\mathbf{F}_3(K_3,id,j)$,

$\vec{s}:=\mathbf{SampleU1}(\mathbb{Z}_q^n, U; r^1_{id}), \vec{e}:=\mathbf{SampleE}(\mathbb{Z}^m, \chi; r^2_{id})$,

对任意 $i\in[(n+1)\ell_q]$, $R_{1,i}:=\mathbf{SampleU2}(\{0,1\}^{m\times m}, U; r^{2,i}_{id})$, 对任意 $j\in[m^2]$, $R_{2,i,j}:=\mathbf{SampleU3}(\{0,1\}^{m\times m}, U; r^{3,(i-1)m^2+j}_{id})$,

$(pk_{id}, sk_{id}):=$

$$\mathbf{BP}.\mathbf{KeyGen}\left(A;\left(\vec{s},\vec{e},\left\{R_{1,i},\left\{R_{2,i,j}\right\}_{j\in[m^2]}\right\}_{i\in[(n+1)\ell_q]}\right)\right),$$

输出 sk_{id}.

因该方案的密文空间就是 BP 方案的密文空间 $\mathbb{Z}_q^{n+1}$, 故本方案的密文规模 $\mathrm{O}(n\log q)$ 远远小于 Canneti 等人实例化方案的密文规模 $\mathrm{O}(n^5\log^5 q)$.

定理 2. 若方案 **BP** 是 IND-CPA 安全的, **iO** 是一个计算不可区分混淆方案, **F** 是一个可穿孔的伪随机函数, 则方案 **MIBFHE** 是 IND-sID-CPA 安全的。

证明. 根据文献[22]中 Lemma 4.1 的证明和定理 1 的证明, 可得出该定理的证明。

输入: $id \in \{0,1\}^k$

参数: A, K_1, K_2, K_3

1. $(r_{id}^{1,1}, r_{id}^{1,2}) := \mathbf{F_1}(K_1, id)$,
2. 对于任意 $i \in [(n+1)\ell_q]$, $r_{id}^{2,i} := \mathbf{F_2}(K_2, id, i)$,
3. 对于任意 $j \in [m^2(n+1)\ell_q]$, $r_{id}^{3,j} := \mathbf{F}_3(K_3, id, j)$,
4. $\vec{s} := \mathbf{SampleU1}(\mathbb{Z}_q^n, U; r_{id}^1)$, $\vec{e} := \mathbf{SampleE}(\mathbb{Z}^m, \chi; r_{id}^2)$,
   对任意 $i \in [(n+1)\ell_q]$, $R_{1,i} := \mathbf{SampleU2}(\{0,1\}^{m\times m}, U; r_{id}^{2,i})$,
   对任意 $j \in [m^2]$, $R_{2,i,j} := \mathbf{SampleU3}(\{0,1\}^{m\times m}, U; r_{id}^{3,(i-1)m^2+j})$,
   $$(pk_{id}, sk_{id}) := \mathbf{BP.KeyGen}\left(B; \left(\vec{s}, \vec{e}, \left\{R_{1,i}, \left\{R_{2,i,j}\right\}_{j\in[m^2]}\right\}_{i\in[(n+1)\ell_q]}\right)\right),$$
5. 输出 pk_{id}.

图 3 程序 $\mathbf{F_{PK}}$ #

Figure 3 Program $\mathbf{F_{PK}}$

5 总结

观察到Canetti等人的MIBFHE构造框架的不足: 密文规模大和紧致性弱, 本文构造了密文规模较小和紧致性较强的 MIBFHE 框架, 相比于前者用到 MFHE 和 IBE 两种构件, 本文中的构造仅需 MFHE 一个构件。若用 Brakerski 和 Perlman 的 MFHE 方案去实例化这两个框架 (Canetti 等人的框架还需用基于 DLWE 假设的 IBE 方案), 可得 Canetti 等人实例化方案的密文规模为 $O(n^5 \log^5 q)$, 而实例化我们框架所得方案的密文规模为 $O(n \log q)$. 然而, 我们的方案只能实现选择安全性, 且用到了 **iO** 这一目前复杂性较高的工具, 故如何构造更高效的、密文规模较小的、适应性安全的 MIBFHE 方案, 是我们将来要研究的问题。

参考文献

[1] R. Rivest, L. Adleman, and M. Dertouzos, "On Data Banks and Privacy Homomorphisms," *Foundations of Secure Computation*, pp. 169-177, 1978.

[2] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[3] T. ElGaml, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[4] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," *in Theory of Cryptography Conference (TCC'05),* pp. 325-341, 2005.

[5] C. Gentry, "Fully Homomorphic Encryption using Ideal Lattices," *in Proc of the 41st Annual ACM Symposium on Theory of Computing (STOC'09)*, pp. 169-178, 2009.

[6] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntannathan, "Fully Homomorphic Encryption over the Integers," *in Proc of the 29th International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'10)*, pp. 24-43, 2010.

[7] Z. Brakerski, and V. Vaikuntanathan, "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages," *in Proc of the 31st Annual Conference on Advances in Cryptology (CRYPTO'11)*, pp. 505-524, 2011.

[8] Z. Brakerski, and V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard) LWE," *in IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS'11)*, pp. 97-106, 2011.

[9] N. P. Smart, and F. Vercautern, "Fully Homomorphic SIMD Operations," *in Des. Codes Cryptography*, vol. 71, no. 1, pp. 57-81, 2014.

[10] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," *in Proc of the 3rd Innovations in Theoretical Computer Science Conference (ITCS'2012)*, pp. 309-325, 2012.

[11] Z. Brakerski, "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP," *in Proc of the 32nd Annual Conference on Advances in Cryptology (CRYPTO'12)*, pp. 868-886, 2012.

[12] Z. Brakerski, C. Gentry, and S. Halevi, "Packed Ciphertexts in LWE-Based Homomorphic Encryption," *in Proc of the 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC'13),* pp. 1-13, 2013.

[13] C. Gentry, A. Sahai, and B. Waters, "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based," *in Proc of the 33rd Annual Cryptology Conference (CRYPTO'13)*, pp. 75-92, 2013.

[14] S. Halevi, and V. Shoup, "Bootstrapping for HElib," *in Proc of the 34th International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'15)*, pp. 641-670, 2015.

[15] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *in Advances in Cryptology (CRYPTO'84)*, pp. 47-53, 1984.

[16] D. Naccache, "Is Theoretical Cryptograohy any Good in Practice?" Invited talk at CRYPTO/CHES'10. 2010.

[17] M. Clear, and C. McGoldrick, "Bootstrappable Identity-Based Fully Homomorphic Encryption," *in Cryptology and Network Security-13th International Conference (CANS'14)*, pp. 1-19, 2014.

[18] M. Clear, and C. McGoldrick, "Multi-identity and Multi-key Leveled FHE from Learning with Errors," *in Proc of the 35th Annual Cryptology Conference (CRYPTO'15)*, pp. 630-656, 2015.

[19] A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-Fly

Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption," *in Proc of the 44th annual ACM symposium on Theory of computing (STOC'12)*, pp. 1219-1234, 2012.

[20] C. Gentry, C. Peikert, and V. Vaikuntanathan, "How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions," *in Proc of the 40th annual ACM symposium on Theory of computing (STOC'08)*, pp. 197-206, 2008.

[21] P. Mukherjee, and D. Wichs, "Two Round Multiparty Computation via Multi-key FHE," *in Proc of the 35th International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'16)*, pp. 735-763, 2016.

[22] Z. Brakerski, and R. Perlman, "Lattice-Based Fully Dynamic Multi-key FHE with Short Ciphertexts," *in Proc of the 36th Annual Cryptology Conference (CRYPTO'16)*, pp. 190-213, 2016.

[23] C. Peikert, and S. Shiehian, "Multi-Key FHE from LWE, Revisted," *in Theory of Cryptography-14th International Conference (TCC'16-B)*, pp. 217-238, 2016.

[24] R. Canetti, S. Raghuraman, S. Richelson, and V. Vaikuntanathan, "Chosen-Ciphertext Secure Fully Homomorphic Encryption," *in Proc of the 20th International Conference on Practice and Theory in Public-Key Cryptography (PKC'17)*, pp. 213-240, 2017.

[25] Z. Brakerski, D. Cash, R. Tsabary, and H. Wee, "Targeted Homomorphic Attribute Based Encryption," *in Theory of Cryptography-14th International Conference (TCC'16-B)*, pp.330-360. 2016.

[26] O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," *in Proceedings of the 37th Annual {ACM} Symposium on Theory of Computing (STOC'05)*, pp. 84-93, 2005.

[27] C. Peikert, "Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem," *in Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09)*, pp. 333-342, 2009.

[28] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and Ke Yang, "On the (Im)possibility of Obfuscating Programs," *in Proc of the 21st Annual Conference on Advances in Cryptology (CRYPTO'01)*, pp.1-18, 2001.

[29] A. Sahai, and B. Waters, "How to Use Indistinguishability Obfuscation: Deniable Encryption, and More," *in Proceedings of the 46th Annual {ACM} Symposium on Theory of Computing (STOC'14)*, pp. 475-484, 2014.

[30] D. Micciancio, and C. Peikert, "Trapdoors for Lattices: Similar, Tighter, Faster, Smaller," *in Proc of the 31st International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'12)*, pp. 700-718, 2012.

[31] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai Trees, or How to Delegate a Lattice Basis," *in Proc of the 29th International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'10)*, pp. 523-552, 2010.

[32] S. Agrawal, D. Boneh, and X. Boyen, "Efficient Lattice (H)IBE in the Standard Model," *in Proc of the 29th International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'10)*, pp. 553-572, 2010.

王学庆 于 2013 年在云南大学信息与计算科学专业获得理学学士学位。现在中国科学院信息工程研究所信息安全国家重点实验室硕博连读。研究领域为公钥密码学。研究兴趣包括: 格密码、全同态加密。Email: wangxueqing@iie.ac.cn

薛锐 于 1999 年在北京师范大学数学专业获得理学博士学位。现任中国科学院信息工程研究所信息安全国家重点实验室研究员。研究领域为公钥密码学、安全协议。研究兴趣包括: 公钥密码学、安全协议的形式化分析。Email: xuerui@iie.ac.cn

王彪 于 2012 年在北京科技大学材料科学与工程专业获得硕士学位。现在中国科学院信息工程研究所信息安全国家重点实验室攻读博士学位。研究领域为公钥密码学。研究兴趣包括: 全同态加密、格密码。Email: wangbiao@iie.ac.cn