

基于NTRU自举的多密钥全同态加密方案

郑俊华¹, 江宏伟¹, 刘荣¹, 李沂修², 李闻¹, 翁健²

(1. 中国烟草总公司广东省公司, 广东 广州 510610; 2. 暨南大学网络空间安全学院, 广东 广州 510632)

摘要: 多密钥全同态加密 (multi-key fully homomorphic encryption, MK-FHE) 技术支持对不同密钥加密的密文进行同态运算, 能够直接应用于现实中的多用户数据融合计算场景, 如多方协同计算和联邦学习。目前, 主流的多密钥全同态加密主要通过自举技术实现对LWE (learning with error) 加密密文的多密钥同态计算。将单密钥密文扩展为多密钥密文的时间效率和存储开销与自举技术密切相关, 通常需要大量的同态评估密钥以及复杂的运算。因此, 如何结合更优的自举技术设计多密钥全同态加密方案, 进而提升计算效率与降低存储开销成为研究的关键问题。基于NTRU (number theory research unit) 自举技术, 设计了一种针对LWE密文的高效多密钥全同态加密方案。与其他方案相比, 所提方案在密文扩展过程中具有更高的计算效率。此外, 对所提方案的正确性进行了详细阐述和分析, 并在理论上将所提方案与现有主流的多密钥全同态加密方案进行了多维度对比, 结果显示所提方案具有更优的计算效率。最后, 探索了该方案在多行业多源销售数据跨部门监管场景中的潜在应用, 在保护数据隐私的前提下帮助税务部门实现税务核验, 有助于推动各行业的数字化转型和健康发展。

关键词: 多密钥全同态加密; 协同计算; 自举技术; 加密技术

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024085

Multi-key fully homomorphic encryption scheme based on NTRU bootstrapping

ZHENG Junhua¹, JIANG Hongwei¹, LIU Rong¹, LI Yixiu², LI Wen¹, WENG Jian²

1. CNTC Guangdong Tobacco Corporation, China National Tobacco Corporation, Guangzhou 510610, China

2. College of Cyber Security, Jinan University, Guangzhou 510632, China

Abstract: Multi-key fully homomorphic encryption (MK-FHE) technology supports homomorphic operations on ciphertexts encrypted with different keys, and can be directly applied to real-world multi-user data fusion computing scenarios, such as multi-party collaborative computing and federated learning. At present, mainstream multi-key

收稿日期: 2024-08-05; 修回日期: 2024-11-06

通信作者: 李沂修, 810069458@qq.com

基金项目: 广东省烟草专卖局(公司)科技项目(粤烟科项202207); 广州市科技计划项目(2024A03J0464)

Foundation Items: Science and Technology Project of CNTC Guangdong Corporation (Guangdong Tobacco Science and Technology Project 202207), Guangzhou Science and Technology Plan Project(2024A03J0464)

引用格式: 郑俊华, 江宏伟, 刘荣, 等. 基于NTRU自举的多密钥全同态加密方案[J]. 网络与信息安全学报, 2024, 10(6): 123-136.

Citation Format: ZHENG J H, JIANG H W, LIU R, et al. Multi-key fully homomorphic encryption scheme based on NTRU bootstrapping[J]. Chinese Journal of Network and Information Security, 2024, 10(6): 123-136.

fully homomorphic encryption mainly uses bootstrapping technology to achieve multi-key homomorphic computing of LWE (learning with errors) encrypted ciphertexts. The time efficiency and storage overhead of expanding single-key ciphertexts to multi-key ciphertexts are closely related to the bootstrapping technology, which usually requires a large number of homomorphic evaluation keys and complex operations. Therefore, designing a multi-key fully homomorphic encryption scheme in combination with a better bootstrapping technology to improve computational efficiency and reduce storage overhead had become a key research issue. Based on the NTRU (number theory research unit) bootstrapping technology, an efficient multi-key fully homomorphic encryption scheme for LWE ciphertexts was designed. Compared with other schemes, the proposed scheme exhibited higher computational efficiency in the ciphertext expansion process. In addition, the correctness of the proposed scheme was elaborated and analyzed in detail. The proposed scheme was compared with the existing mainstream multi-key fully homomorphic encryption scheme in theory. The results show that the proposed scheme has better computational efficiency. Finally, the potential application of the scheme in cross-departmental supervision scenarios of multi-industry and multi-source data sales data was explored, which helped the tax department to realize tax verification under the premise of protecting data privacy, and helped promote the digital transformation and healthy development of various industries.

Keywords: multi-key fully homomorphic encryption (MK-FHE), collaborative computation, bootstrapping technique, encryption technology

0 引言

随着数字技术日趋成熟, 全球经济高速发展时期已逐渐由传统结构开始向数字经济转型^[1]。通过对不同结构且敏感的数据进行协同分析, 从而更好地提高决策能力, 是企业实现数字化转型的关键任务。目前, 各行各业已经开始积极推动商业数字化转型工作。然而, 在多行业多来源的数据流通、聚合、计算等过程中, 依然面临着多种安全挑战, 如行业内部与外部数据的安全聚合、协同计算等问题。传统密码学相关技术可以为企业保护核心数据存储及行业数据隐私安全, 但其仍存在一定局限性, 如传统密码学不支持密文下的数据运算、无法抵抗量子计算机攻击等。

近年来, 隐私计算技术^[2]被广泛应用于各种领域, 用以解决多方数据处理过程中所需要的隐私计算需求。在隐私计算的发展过程中主要包含 3 种主流技术路线: 以全同态加密、多方安全计算等为代表的基于密码学的隐私计算^[3], 以联邦学习为代表的基于人工智能的隐私计算^[4]、以可信执行环境为代表的基于可信硬件的隐私计算^[5-6]。其中, 全同态加密是实现数据隐私计算的关键技术之一, 它支持在不暴露明文数据的前提下, 允许第三方(如云服务提供商)对加密的数据进行计算, 从而实现数据的“可算不可见”。

全同态加密的这一特性对于实际应用具有重要意义, 张晓均等^[7]改进了 BGN (Boneh-Goh-Nissim) 同态加密算法, 在医疗数据安全与隐私保护场景中提出了一种具有容错机制的可验证医疗密态数据聚合方案。任艳丽等^[8]基于 CKKS (Cheon-Kim-Kim-Song) 同态加密算法, 提出了一种隐私保护的卷积神经网络预测方案, 对用户隐私数据和模型参数进行保护。李宇溪等^[9]基于同态加密机制, 提出一种支持 K -近邻搜索的移动社交网络隐私保护方案。肖文乾等^[10]提出了一种加法同态加密与多高位嵌入的加密域图像可逆信息隐藏方法, 用以提升图像网络传输的安全性和信息传输效率。

全同态加密在各行各业中均具有广泛的应用前景, “可算不可见”的隐私计算属性能够满足多源数据融合计算需求。然而, 传统的单密钥全同态加密在多用户场景下还存在功能可扩展性问题。例如, 在多行业多来源销售数据安全聚合与协同计算的场景下, 以烟草行业中的税费统计计算为例, 首先需要统计各行业中不同种类的销售数据进行聚合, 随后再按照相应税率对各类商品的整体税费进行协同计算。然而, 销售数据具有较强的隐私性, 因为销售数据中包含个人信息、商品价格等隐私信息, 这些数据关乎个人信息及商业机密等信息。因此, 如何在保护不同行业多来源数据隐私性的同时, 又能满足来自不同参与

方数据的安全聚合及协同计算，就需要使用多密钥全同态加密技术。

多密钥全同态加密允许不同密钥下的加密数据之间执行同态运算，这使得不同来源的数据（对应不同密钥）可以在加密状态下进行安全聚合及计算。显然，多密钥全同态加密契合本文对多源数据安全聚合、协同计算的需求。然而，多密钥全同态加密目前依然存在一定的缺陷，如公钥长度较大、密文计算复杂、密文扩展效率低等问题。

2012年，López-Alt等^[11]基于NTRU密码体制提出了第一个多密钥全同态加密（multi-key fully homomorphic encryption, MK-FHE）方案，各方使用自己的公钥对私有数据进行加密，不同密钥下的密文将进一步扩展，以支持多密钥同态评估。然而，这种结构的安全性是基于多项式环的一个新的假设。2015年，Clear等^[12]提出了首个基于容错学习问题（learning with error, LWE）的GSW（Gentry-Sahai-Waters）型MK-FHE构造。GSW型MK-FHE方案安全性高，运算过程无须进行密钥切换，但密文随着用户数量增长，加解密速度和同态运算效率不高。2016年，Mukherjee等^[13]提出了一种基于GSW的MK-FHE的构造，该构造简化了Clear的方案，并允许一轮交互的分布式运算，提升了运算效率。2019年，Chen等^[14]基于TFHE框架设计了概念上更简单的MK-FHE方案，但生成计算密钥长度较大。上述方案依然存在密文扩展效率较低、扩展密文长度较大等问题。2022年，Xu等^[15]在Bonte等^[16]构建的FINAL方案和Klucznik等^[17]构建的NTRU-v-um方案基础上，基于自举技术提出了一种密文扩展更快的多密钥全同态加密方案。

自举技术成为多密钥全同态加密方案效率及密钥长度优化的关键技术。基于自举技术的多密钥全同态加密方案的密文扩展效率完全取决于自举技术的效率，即更高效的自举技术能够构造更快的多密钥全同态加密方案。例如，基于FHEW（fastest homomorphic encryption in the west）、TFHE（fully homomorphic encryption over the Torus）等自举技术设计的MK-FHE方案在同态解

密过程中为RGSW（ring gentry-Sahai-Waters）内积运算方式，这要求同态解密密钥也为RGSW密文，相较于基于NTRU的自举技术，其具有更大的密钥长度及更复杂的运算过程。2023年，Xiang等^[18]基于NTRU提出了一种快速盲旋转的自举技术，相较于其他自举技术，该方案在自举密钥长度上占有较大优势，因为该方案的自举密钥为向量型的NTRU密文，相应地其同态解密过程中的密文运算方式可以被理解为RLWE（ring-learning with errors）内积，自举密钥结构及运算方式的优化使其在全同态加密过程中具有更好的优势。为了解决多密钥全同态加密运算过程中的效率低等问题，本文基于NTRU自举技术提出了一种MK-FHE方案，主要的贡献如下。

1) 本文基于NTRU自举技术设计了一种高效多密钥全同态加密方案。相较于其他基于自举技术的多密钥全同态加密方案，本文基于NTRU自举方案具有更小的同态解密密钥长度，具有更高效的同态解密计算。

2) 本文受Bonte等提出的方案对三元组密钥处理的启发，设计了一种能够对多密钥位同时处理的自举密钥生成方法，能够有效减小同态解密过程中所需的内积次数。

3) 本文从正确性、安全性角度对方案进行了详细分析。同时，本文从方案特性、评估密钥长度等方面与现有的多密钥全同态加密方案进行了多维度对比，证明了本文所提出的多密钥全同态加密方案具有更优的性质。此外，本文着眼于多行业多源数据的安全聚合和协同计算需求，探讨了该方案在多参与方协同计算的多方场景的潜在应用，并给出了应用模型。

1 背景知识

1.1 同态加密与多密钥同态加密

1.1.1 同态加密

1978年，Rivest等首次提出同态加密（homomorphic encryption, HE）^[19]的概念，其定义如下。

定义1（同态加密）：如果加密算法满足式（1），则称该加密算法为全同态加密：

$$E(m_1) \cdot E(m_2) = E(m_1 \cdot m_2), \forall m_1, m_2 \in M \quad (1)$$

其中, E 为加密算法, $\cdot$ 表示某种抽象运算, 一般表示为加法和乘法。

1.1.2 多密钥全同态加密

传统的全同态加密技术只适用于属于同一个用户的所有密文进行同态计算, 但在现实场景中通常需要对多个用户不同密钥下的加密数据进行同态运算。通常一个多密钥全同态加密方案包括 6 种算法 (Setup、KeyGen、Enc、Dec、Extend 和 Eval), 具体描述如下。

1) 初始化算法 $pp \leftarrow \text{Setup}(1^\lambda, 1^L, 1^k)$: 给定一个安全参数 λ , 最大电路深度 L , 最大参与计算方数量 k , 输出一个公共参数 pp 。

2) 密钥生成算法 $pk, sk \leftarrow \text{KeyGen}(pp)$: 使用给定的公共参数 pp , 为每一方生成公钥 pk 和密钥 sk 。

3) 加密算法 $C \leftarrow \text{Enc}(pk, m)$: 输入给定公钥 pk 和待加密的明文消息 m , 输出一个新的与 pk 对应的对 m 进行加密的密文 C 。在不丢失通用性的情况下, 每个密文都包含了对应方的私钥和电路层级信息。

4) 解密算法 $m \leftarrow \text{Dec}(\{sk_i\}_{1 \leq i \leq k}, C)$: 给定一个相关方的密钥序列 $SK = \{sk_i\}_{1 \leq i \leq k}$ 和 SK 下对应于 $PK = \{pk_i\}_{1 \leq i \leq k}$ 的待计算的密文 C 。恢复并输出消息 m 。

5) 密文扩展算法 $\hat{C} \leftarrow \text{Extend}((PK = \{pk_i\}_{1 \leq i \leq k}), C)$: 在 $SK = \{sk_i\}_{1 \leq i \leq k-1}$ 的条件下输入对应的待计算的密文 C , 其中 PK 由公钥 pk 和公共扩展矩阵组成, 则在 $SK = \{sk_i\}_{1 \leq i \leq k}$ 下输出扩展后的密文 $\hat{C}$ 。

6) 同态运算算法 $C' \leftarrow \text{Eval}(\{pk_i\}_{1 \leq i \leq k}, \mathbb{C}\{C_s\}_{1 \leq s \leq s})$: 给定一个最大深度为 L 的布尔电路 $\mathbb{C}$ 和 s 个待计算的密文 $\{C_s\}_{1 \leq s \leq s}$ 线路, 以及它们的公钥序列 $PK = \{pk_i\}_{1 \leq i \leq k}$, 求值并输出一个密文 C' 。输出的密文隐式包含相关方的 k 个索引。

1.1.3 分圆环

定义 2 (分圆环): $R = \frac{\mathbb{Z}[X]}{f(x)}$, 其中 $\mathbb{Z}[X]$

表示以整数集 $\mathbb{Z}$ 为系数, X 为不定元的所有多项

式, $f(x)$ 取第 $2N$ 个分圆多项式 $\phi_{2N} = X^N + 1$, 在 $\mathbb{Z}[X]$ 上是不可约的。其对应的剩余类环为

$$R_Q = \frac{\mathbb{Z}_Q[X]}{f(x)},$$

表示环中任意(多项式)元素的系数被约束在模 Q 空间中。注意, R 及 R_Q 具有相同的基, 因存在双射 $X \rightarrow a$ 使得 R, R_Q 同构于 $\mathbb{Z}[a], \mathbb{Z}_Q[a]$, 其中 a 为 ϕ_{2N} 的一个 $2N$ 次本原单位根, 因此以不定元 X 为生成元可抽象生成一个循环群, 即 $\{1, X^1, X^2, \dots, X^{N-1}\}$ 。

1.2 NTRU、LWE 和 RLWE 问题

1998 年, Hoffstein 等^[20]设计了名为 NTRU Encrypt 的公钥密码系统, 使用基于格的加密算法来加密数据。2005 年, Regev^[21]在一项重要的工作中引入了错误学习问题。2010 年, Lyubashevsky 等^[22]引入了分圆环上的 LWE 变种, 称为环 LWE (RLWE)。本文的相关定义是基于 NTRU、LWE 和 RLWE 的决策版本, 是多密钥全同态加密结构安全性的底层难题。

1.2.1 LWE 和 RLWE 问题

定义 3 (决策-LWE) 对于正整数 n 和 q , 以及 $\mathbb{Z}$ 上的误差分布 χ 。LWE $_{n,q,\chi}$ 问题要求确定给定的样本 $(b, a) \in \mathbb{Z}_q^{n+1}$ 是否按以下方式分布: ① 采样 $a \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \chi$ 并对某个称为密钥的向量 $s \in \mathbb{Z}_q^n$, 输出 $(b = \langle a, s \rangle + e \bmod q, a)$; ② 在 $\mathbb{Z}_q^{n+1}$ 上的均匀分布, LWE $_{n,q,\chi}$ 假设是指在给定合理的计算资源下, 没有有效的算法能够在多项式时间内解决 LWE $_{n,q,\chi}$ 问题, 即在计算上是困难的。

非正式地, 称 $(b = \langle a, s \rangle + e \bmod q, a) \in \mathbb{Z}_q^{n+1}$ 是在密钥 $a \leftarrow \mathbb{Z}_q^n$ 下的 LWE 加密。消息 $m \in \mathbb{Z}_q$ 在 k 个密钥 $s_1, \dots, s_k \in \mathbb{Z}_q^n$ 下的多密钥 LWE 密文具有如下形式: $\sum_{i=1}^k \langle a_i, s_i \rangle + e + m \bmod q$, $a_1, \dots, a_k \in \mathbb{Z}_q^{kn+1}$ 。

定义 4 (决策-RLWE) 对于正整数 n 和 q , 设 R 是维数为 n 的环, χ 是 R 上的误差分布。RLWE $_{n,q,\chi}$ 问题是区分给定样本 $(b, a) \in R_q^2$, 并按下列方式分布的情况: ① 对于 $s \in R_q$ 称为密钥, 抽样 $a \leftarrow R_q$, $e \leftarrow \chi$, 然后输出 $(b = a \cdot s + e \bmod q, a)$; ② 在 R_q^2 上的均匀分布, RLWE $_{n,q,\chi}$ 假设是指在给定合理的计算资源下, 没有有效的算法能够在多项式时间内解决 RLWE $_{n,q,\chi}$ 问题, 即

在计算上是困难的。

非正式地，称 $(a \cdot s + e + m \bmod q, a) \in R_q^2$ 是消息 $m \in R_q$ ，密钥 $s \in R_q$ 下的 RLWE 加密。消息 $m \in R_q$ 在 k 个密钥 $s_1, \dots, s_k \in R_q$ 下的多密钥 RLWE 密文具有如下形式： $\sum_{i=1}^k a_i \cdot s_i + e + m \bmod q, a_1, \dots, a_k \in R_q^{k+1}$ 。

1.2.2 NTRU 问题

通常使用三元密钥来实例化 NTRU 问题。在构造中从 $\{-1, 0, 1\}$ 上的分布生成密钥，使得 0 以 $\frac{1}{2}$ 的概率出现，1 和 -1 以 $\frac{1}{4}$ 的概率出现，这近似于标准差 $\sigma = \frac{1}{\sqrt{2}}$ 。可以定义 NTRU 问题的反循环版本和矩阵版本。每个版本都有计算和决策两个变体。

定义 5 (NTRU) 设 $N > 0$ ， $Q > 1$ 为整数， $R = \frac{\mathbf{Z}[X]}{X^N + 1}$ 。设 $\sigma > 0$ 为实数 g ， $f \leftarrow \chi_\sigma^N$ 并且 f 在 R_Q 可逆。

计算 (N, Q, σ) NTRU 问题：是在给定 $h := g \cdot f^{-1} \bmod Q$ 的情况下恢复 f 和 g 。

决策 (N, Q, σ) NTRU 问题：是区分和从中随机抽取的均匀随机多项式之间的问题。

1.2.3 LWE 加密

LWE 加密：给定安全参数 λ ，维数 n ，模数 q ，明文空间 $t = 2$ ，上限为 $\frac{q}{2t}$ 的噪声分布 χ ，输入明文 $m \in \{0, 1\}$ ，均匀随机选取 $a \in \mathbf{Z}_q^{n+1}$ （从中均匀随机选取元素组成矩阵），向量 $s \in \{0, 1\}^n$ ，噪声 $e \in \chi$ ，输出密文：

$$E_{\text{LWE}}(m) = \left(a, as + e + m \frac{q}{2} \right) \bmod q \in \mathbf{Z}_q^{n+1} \quad (2)$$

其解密函数为：

$$m' = \frac{t(b - as)}{q} \bmod 2 = \frac{m + 2e}{q} \bmod 2 \quad (3)$$

因为 $|e| < \frac{q}{4}$ ，所以 $m' = m \bmod 2$ 满足解密正确性。即在一个加密比特值的 LWE 密文中，只要密文中的噪声上限 $|e| < \frac{q}{4}$ ，即可解密成功。因此，若对于 2 个新鲜的 LWE 密文具有同态评估的需求，只要保证结果密文中的噪声小于上限即可。

可，因此在 LWE 加密中为了保证密文具有可评估性，噪声的选取往往更小。例如，在 FHEW 中，为了适应方案提出的一种新型 NAND 密文评估门，其中的 LWE 加密算法其初始噪声仅为 $\frac{q}{16}$ ，即给定两个新鲜的 LWE 密文 $C_1 = (a_1, b_1 = a_1 s + e_1 + m_1 \frac{q}{4})$ 和 $C_2 = (a_2, b_2 = a_2 s + e_2 + m_2 \frac{q}{4})$ ，进行 NAND 运算：

$$(a, b) = \text{NAND}(C_1, C_2) = \left(-a_1 - a_2, \frac{5q}{8} - b_1 - b_2 \right) \quad (4)$$

该结果密文 (a, b) 满足：

$$\left| b - as - (1 - m_1 m_2) \frac{q}{2} \right| = \left| \pm \frac{q}{8} - (e_1 + e_2) \right| < \frac{q}{8} + \frac{q}{16} + \frac{q}{16} = \frac{q}{4} \quad (5)$$

因此，结果密文 (a, b) 满足解密正确性。

2 基于 NTRU 的多密钥全同态加密方案设计

本节主要对基于 NTRU 自举的 MK-FHE 方案的设计与构造进行介绍和阐述。

2.1 NTRU 加密算法

基于 NTRU 的加密方案包括 4 种 PPT (probabilistic polynomial time) 算法。

1) NTRU.ParamGen(1^λ): 接收安全参数并输出元组 (N, Q, ζ, B, ℓ) ，其中 B 是用于分解密文的基， $\ell := \lceil \log_B(Q) \rceil$ 。

2) NTRU.KeyGen: 采样 $f' \leftarrow \chi_\zeta^N$ ，并设置 $f := 1 + 4 \cdot f'$ 直到 f^{-1} 存在于 R_Q ，输出 $\text{sk} := f$ 。

3) NTRU.EncS(f, m): 给定一个明文多项式 m ，采样 $g \leftarrow \chi$ ，输出密文 $\text{NTRU}_{Q,f}(m) := g/f + m$ 。

4) NTRU.EncG(f, v): 设 B 是一个整数参数，对于密钥 $f \in R$ （即在 R_Q 中是可逆的），向量 $v \in R_Q$ 的 NTRU 加密定义为：

$$\text{NTRU}'_{Q,f}(v) := (g_0/f' + B^0 \cdot v, \dots, g_{d-1}/f' + B^{d-1} \cdot v) \in R_Q^d \quad (6)$$

其中， $f', g_0, \dots, g_{d-1} \in \chi$ 具有小系数，并且 $d = \lceil \log_B Q \rceil$ 。

对于任意的多项式 $a \in R_Q$ ，定义 $\text{BitDecom}_B(a) \in R_B^d$ 将其分解为向量

$(a_0, \dots, a_{d-1}) \in R_B^d$ 满足 $\mathbf{a} = \sum_{i=0}^{d-1} a_i \cdot B^i$ 。因此, 若给定一个 NTRU 密文 $c = \text{NTRU}_{Q_f}(m)$ 和另一个向量型 NTRU 密文 $c' = \text{NTRU}'_{Q_f}(m') \in R_Q^d$, 其外积表示为“ $\odot$ ”, 运算过程为 $\text{BitDecom}_B(c) = (c_0, \dots, c_{d-1}) \in R_B^d$ 和 $c' = (c'_0, \dots, c'_{d-1})$ 之间的数量积, 即

$$c \odot c' = \text{BitDecom}_B(c), c' = c_i c'_i = \sum_{i=0}^{d-1} c_i g_i f' + g f' + m m' \in R_Q \quad (7)$$

显然内积的结果是一个 NTRU 密文, 即 $c \odot c' = \text{NTRU}_{Q_f}(m) \odot \text{NTRU}'_{Q_f}(m') = \text{NTRU}_{Q_f}(m m')$ 。

2.2 多密钥全同态加密方案

2022 年, Bonte 等在 FHEW、TFHE 等自举技术的基础上提出了一种基于 NTRU 的快速自举算法, 该方案的优势之一在于自举过程是 NTRU 密文间的运算, 因此其在存储复杂度和时间复杂度上相较于之前的自举方案具有较大优势。同时, 对于 LWE 密钥 $s_i \in \{-1, 0, 1\}$ 的 LWE 密文, 该方案也能够通过自举技术对相应的 LWE 密文进行自举处理, 这是该方案的另一优势, 该方法实际上是一种选择机制。例如, 当 $s_i = -1$ 时, 该方案对自举密钥的预处理过程为:

$$\text{Evk}_i = \mathbf{g} + (X^{a_i} - 1) \cdot \text{NTRU}'_{Q_f}(0) + (X^{-a_i} - 1) \cdot \text{NTRU}'_{Q_f}(1) \quad (8)$$

其中 $\mathbf{g} = [B^0, B^1, \dots, B^{d-1}]$ 。当 $s_i = -1$ 时, 关于自举密钥 Evk_i 在预处理过程中实际发挥作用的是密文 $\text{NTRU}'_{Q_f}(1)$, 即 Evk_i 最终是关于 X^{-a_i} 的加密, 从而实现了对于三元组 LWE 密文的正确同态解密。

$$\begin{cases} \text{evk}_j = \{ \text{NTRU}'_{Q_f}(1), \text{NTRU}'_{Q_f}(0), \text{NTRU}'_{Q_f}(0) \}, s_i = 1, s_{i+1} = 0 \\ \text{evk}_j = \{ \text{NTRU}'_{Q_f}(0), \text{NTRU}'_{Q_f}(1), \text{NTRU}'_{Q_f}(0) \}, s_i = 0, s_{i+1} = 1 \\ \text{evk}_j = \{ \text{NTRU}'_{Q_f}(0), \text{NTRU}'_{Q_f}(0), \text{NTRU}'_{Q_f}(1) \}, s_i = 1, s_{i+1} = 1 \\ \text{evk}_j = \{ \text{NTRU}'_{Q_f}(0), \text{NTRU}'_{Q_f}(0), \text{NTRU}'_{Q_f}(0) \}, s_i = 0, s_{i+1} = 0 \end{cases} \quad (9)$$

其中, $j \in [n/2]$, $i = 0, 2, 4, \dots, n-2$ 。

2) Acc: 对于给定的多密钥 LWE 密文 $c = (b, a_0, a_1, \dots, a_{nk-1}) \in \mathbb{Z}_q^{nk+1}$, 当通过自举对 LWE 密文进行同态解密时, 首先通过预处理生成同态解密运算时使用的自举密钥, 过程如下:

$$\begin{aligned} \text{evk}_j &= \left(X^{\frac{2N}{q} \cdot a_i} - 1 \right) \cdot \text{evk}_{j,0} + \left(X^{\frac{2N}{q} \cdot a_{i+1}} - 1 \right) \cdot \text{evk}_{j,1} \\ &+ \left(X^{\frac{2N}{q} \cdot (a_i + a_{i+1})} - 1 \right) \cdot \text{evk}_{j,2} + \mathbf{g} \end{aligned} \quad (10)$$

这一选择机制为本文基于自举技术实现快速的多密钥全同态加密方案提供了启发。具体地说, 给定一个噪声接近上限的 LWE 密文 $c = (a, as + e + \frac{q}{2}m)$, 其中 $s \in \{0, 1\}^n$, 自举解密过程就是逐个密钥位地进行 n 次计算, 从而达到同态解密的结果 $b - \sum a_i s_i$ 。直观地, 优化自举效率的一种方式可以从多密钥位同时计算的角度考虑。例如, 如果每次计算可以实现对 2 个密钥位的同时处理, 则同态解密时只进行 $n/2$ 次密文计算, 显然这能有效降低同态自举过程的效率。上述在 Bonte 等方案中的选择机制为这一方法提供了技术支撑, 具体而言, 假设给定 s_0 和 s_1 , 在对对应的自举密钥 evk 做预处理时, 只需要最终的 evk 是关于 X^{a_0} (当 $s_0 = 1, s_1 = 0$)、 X^{a_1} (当 $s_0 = 0, s_1 = 1$)、 $X^{a_0 + a_1}$ (当 $s_0 = 1, s_1 = 1$) 或 X^0 (当 $s_0 = 0, s_1 = 0$) 的加密即可。根据上述对 Bonte 等方案中自举密钥预处理过程的阐述, 在自举密钥预处理过程中根据 s_i 和 s_{i+1} 的值, 利用 $\text{NTRU}'_{Q_f}(1)$ 对相应的组合进行选择, 即可实现一次运算对多密钥位的处理。因此, 本文构造的基于 NTRU 自举的多密钥全同态加密方案如下。

1) BSKGen: 给定 LWE 密钥 $s \in \{0, 1\}^n$, 其中 n 是 LWE 密文的维度, 均匀随机选取 NTRU 密钥 $f \in R$, 选取加密所需的小系数多项式向量 $\mathbf{g} \in R_Q$, 并根据 LWE 密钥 s_i 和 s_{i+1} 的值, 输出 NTRU 密文作为自举密钥 (其中 $j \in [n/2]$), 有如下定义:

其中 $i = 0, 2, 4, \dots, nk-2$, N 是环多项式的深度, q 为 LWE 的模数, N 和 q 均为 2 的幂次方。此外, 设置累加器初始 $\text{Acc} = \lfloor \frac{Q}{8} \rfloor \cdot \sum_{i=0}^{N-1} X^i \cdot X^{\frac{2N}{q} \cdot (b + \frac{q}{4})}$, 随后执行 $nk/2$ 次累加运算, 即

$$\text{Acc} = \text{Acc} \odot \text{evk}_j \quad (11)$$

当关于 LWE 密文的同态解密累加运算完成后, 将结果密文设置为一个 RLWE 密文, 如下:

$$\text{Acc} = \left(\text{Acc} + \left\lfloor \frac{Q}{8} \right\rfloor \cdot \sum_{i=0}^{N-1} X^i, 0, 0, \dots \right) \in R_Q^{k+1} \quad (12)$$

3) HybridProduct: 给定每个参与方的NTRU密钥 f , 每个参与方随机选取 $a \in R_Q^d$, 密钥 $z \in R$, 噪声 $e_0^d \in \chi$, 输出 $b = -z \cdot a + e_0 \in R_Q^d$, 并设置 $b_0 = -a$, 随机选取 $d_1 \in R_Q^d$, $r \in \chi$, 噪声 $e_1^d \in \chi$, 输出 $d_0 = -z \cdot d_1 + r \cdot g + e_1 \in R_Q^d$, $d_2 = r \cdot a + f \cdot g + e_2 \in R_Q^d$ 。因此, 对于所有参与方, 给定 $d_{i,0}$ 、 $d_{i,1}$ 、 $d_{i,2}$ 以及 b_j , 其中 $j \in [k]$, k 表示参与方数量, 计算:

$$\begin{aligned} x_j[l] &= \langle g^{-1}(b_j[l], d_{i,0}) \rangle \\ y_j[l] &= \langle g^{-1}(b_j[l], d_{i,1}) \rangle \end{aligned} \quad (13)$$

其中 $l \in [d]$ 。并输出:

$$D_i = \begin{bmatrix} d_{i,2} + x_0 & 0 & \cdots & y_0 & \cdots \\ x_1 & d_{i,2} & & y_1 & \\ \vdots & & \ddots & & \vdots \\ x_i & 0 & & d_{i,2} + y_i & 0 \\ \vdots & & & & \vdots \\ x_k & 0 & \cdots & y_k & \cdots & d_{i,2} \end{bmatrix} \in R^{l(k+1) \cdot (k+1)} \quad (14)$$

4) 样本提取: 给定一个多密钥RLWE密文 $\hat{c}$, 可以用密钥解密, 同态提取 $\langle \hat{c}, (1, \hat{z}) \rangle$ 的常数多密钥LWE密文。

Extract: 对于输入的多密钥RLWE密文 $\hat{c} = (c_0, c_1, \dots, c_k) \in R_Q^{k+1}$, $c'_i = (c_{i,0}, -c_{i,N-1}, \dots, -c_{i,1}) \in \mathbf{Z}_Q^N$, 其中 $c_{i,j}$ 为多项式 $c_i \in R_Q$ 的第 j 个系数, 并得到一个新的多密钥LWE密文:

$$\bar{c} = (c_0, c'_1, \dots, c'_k) \in \mathbf{Z}_Q^{kN+1} \quad (15)$$

5) 模数转换: 该过程将一个在模数 Q 下的LWE密文转换为在另一个模数 q 下的LWE密文。

ModSwitch: 解析输入的多密钥LWE密文为 $\bar{c} = (c_0, c_1, \dots, c_{kN}) \in \mathbf{Z}_Q^{kN+1}$, 对于 $i = 1, \dots, kN$, 计算:

$$c'_i = \left\lfloor \frac{q \cdot c_i}{Q} \right\rfloor + B \in \mathbf{Z}_q \quad (16)$$

其中 $B \in \{0, 1\}$ 服从伯努利分布, 最终输出:

$$\bar{c}' = (c'_0, \dots, c'_{kN}) \in \mathbf{Z}_q^{kN+1} \quad (17)$$

6) 多密钥转换: 因为上述自举过程输出的LWE密文并非在原始LWE密钥下的加密, 因此, 该过程是将原始LWE密文转换到各参与方密钥

下的加密密文。

KSKGen: 给定密钥 $z = z_1, \dots, z_N \in \mathbf{Z}^N$ 和 $s = s_1, \dots, s_n \in \mathbf{Z}^n$, 采样矩阵 $A_j \leftarrow \mathbf{Z}_q^{d \times n}$ 和 $e_j \leftarrow \chi^d$, 其中 $j = 1, \dots, N$, 计算:

$$b_j = -A_j \cdot s + e_j + z_j \cdot g \in \mathbf{Z}_q^d \quad (18)$$

并输出转换密钥:

$$\text{sk} = \{(b_j, A_j)\}_{1 \leq j \leq N} \quad (19)$$

7) KeySwitch: 将输入的多密钥LWE密文记为 $\bar{c} = (b, a_1, \dots, a_k) \in \mathbf{Z}_q^{kN+1}$ 。对于 $i = 1, \dots, k$, 记 $a_i = (a_{i,0}, \dots, a_{i,N-1})$ 并用 $\text{sk}_i = (b_{i,j}, A_{i,j})$ 来表示各参与方的转换密钥, 计算:

$$\begin{aligned} b'_i &= \sum_{j=1}^N g^{-1}(a_{i,j})^T \cdot b_{i,j} \in \mathbf{Z}_q \\ b' &= b + \sum_{i=1}^k b'_i \end{aligned} \quad (20)$$

以及

$$a'_i = \sum_{j=1}^N g^{-1}(a_{i,j})^T \cdot A_{i,j} \in \mathbf{Z}_q^n \quad (21)$$

最终输出在各参与方联合密钥 $(s_1, \dots, s_k) \in \mathbf{Z}^{nk}$ 下加密的多密钥LWE密文。

$$\bar{c}' = (b', a'_1, \dots, a'_k) \in \mathbf{Z}_q^{kN+1} \quad (22)$$

2.3 加密算法

依据本文所提方案, 多密钥同态加密自举算法如下。

算法 多密钥同态加密自举算法

输入 多密钥LWE密文 $\bar{c} \in \mathbf{Z}_q^{kN+1}$,

自举密钥 $\text{evk}_{i,j,l}, i \in [k], j \in [n/2], l = 0, 1, 2$

输出 多密钥LWE密文 $\bar{c}' \in \mathbf{Z}_q^{kN+1}$

$$1) \bar{c}_{2N} = (b, a_1, \dots, a_{nk}) \leftarrow \frac{2N}{q} \cdot \bar{c} \in \mathbf{Z}_{2N}^{kN+1}$$

$$2) \text{Acc} \leftarrow tv = \left\lfloor \frac{Q}{8} \right\rfloor \cdot X^{b + \frac{N}{2}} \cdot \sum_{i=0}^{N-1} X^i \in R_Q$$

3) for $i = 1, \dots, k$ do

4) for $j = 0, \dots, n/2 - 1$ do

$$5) \text{Acc} \leftarrow \text{Acc} \odot (X^{a_{n \cdot (i-1) + 2j} - 1} \cdot \text{evk}_{i,j,0} + (X^{a_{n \cdot (i-1) + 2j + 1} - 1} \cdot \text{evk}_{i,j,1} + (X^{a_{n \cdot (i-1) + 2j} + a_{n \cdot (i-1) + 2j + 1} - 1} - 1) \cdot \text{evk}_{i,j,2} + g) \in R_Q$$

6) end

7) end

$$8) \text{Acc} \leftarrow \text{Acc} + \left\lfloor \frac{Q}{8} \right\rfloor \cdot \sum_{i=0}^{N-1} X^i \in R_Q$$

$$9) \text{Acc} \leftarrow (\text{Acc}, 0, \dots, 0) \in R_Q^{k+1}$$

$$10) D_i \leftarrow \text{HybridProduct}(f_i) \in R_Q^{d \cdot (k+1) \cdot (k+1)}$$

- 11) for $i = 1, \dots, k$ do
- 12) $\text{Acc} \leftarrow \text{Acc} \odot D_i \in R_Q^{k+1}$
- 13) end
- 14) $\bar{c}''' \leftarrow \text{Extract}(\text{Acc}) \in \mathbf{Z}_Q^{kN+1}$
- 15) $\bar{c}'' \leftarrow \text{ModSwitch}(\bar{c}''') \in \mathbf{Z}_q^{kN+1}$
- 16) $\bar{c}' \leftarrow \text{KeySwitch}(\bar{c}'', \{\text{ksk}_i\}_{1 \leq i \leq k}) \in \mathbf{Z}_q^{kn+1}$

3 方案分析

对于本文所设计的 MK-FHE 方案, 本文给出了正确性分析, 并与其他类似的全同态 MK-FHE 方案进行了比较。

3.1 MK-FHE 算法正确性

自从 2015 年 FHEW 的自举算法被提出后, 后续的大多数工作如 TFHE 等自举方法均遵循这一设计。具体地, 假设给定一个 LWE 密文 $E_{\text{LWE}}(m) = (a, b = as + e + \frac{mq}{2})$, $|e| < \frac{q}{4}$, 其中, $m \in \{0, 1\}$, 那么在该 LWE 密文 $E_{\text{LWE}}(m)$ 中存在一个矢量关系, 即

$$u(m) = b + \frac{q}{4} - as = \frac{mq}{2} + \frac{q}{4} + e \quad (23)$$

因为 $|e| < \frac{q}{4}$, 所以:

$$\begin{aligned} \{0 < u(m) < \frac{q}{2}\} & m = 0 \\ \{\frac{q}{2} \leq u(m) < q\} & m = 1 \end{aligned} \quad (24)$$

回到本文在上述内容中提到的分圆多项式由单位根构成的循环群 $\{1, X^1, X^2, \dots, X^{N-1}, -1, \dots, X^{N-1}\}$, 可以很明显地发现这一循环群是对称的, 并且系数为 ± 1 。因此, 如果设置单项式 $Y = X^{\frac{2N}{q}}$, 那么 $Y^{u(m)}$ 一定符合如下关系:

$$\begin{aligned} Y^{u(m)} & \in \{1, X^1, X^2, \dots, X^{N-1}\} \quad m = 0 \\ Y^{u(m)} & \in \{-1, -X^1, -X^2, \dots, -X^{N-1}\} \quad m = 1 \end{aligned} \quad (25)$$

通过上述公式可以发现, $m = 0$ 和 1 分别代表着将单项式 $Y^{u(m)}$ 处于正系数和负系数的 2 个单项式集合中。回到本文在算法中将初始多项式设置为 $\text{Acc} = \lfloor \frac{Q}{8} \rfloor \cdot Y^{b + \frac{q}{4}} \cdot \sum_{i=0}^{N-1} X^i$, 最终目的是得到 $\text{Acc} = \lfloor \frac{Q}{8} \rfloor \cdot Y^{u(m)} \cdot \sum_{i=0}^{N-1} X^i$, 可以发现如果 $m = 0$, 那么 $Y^{u(m)}$ 会使得 Acc 的常数项系数为 $-\lfloor \frac{Q}{8} \rfloor$, 反之则为 $\lfloor \frac{Q}{8} \rfloor$ 。假设本文在算法第 3)~7) 行

的过程是正确的, 即能够得到关于 $\text{Acc} = \lfloor \frac{Q}{8} \rfloor \cdot Y^{u(m)} \cdot \sum_{i=0}^{N-1} X^i$ 的加密密文, 随后在算法第 8) 行的处理 $\text{Acc} = \text{Acc} + \lfloor \frac{Q}{8} \rfloor \cdot \sum_{i=0}^{N-1} X^i \in R_Q$, 则能够使得密文 Acc 中的常数项系数变为 0 ($m = 0$ 时) 或 $\lfloor \frac{Q}{4} \rfloor$ ($m = 1$ 时)。常数项系数的变化正是对应 FHEW 类型自举技术输出结果密文中的明文信息, 即给定一个噪声达到上限的 LWE 密文 $c = (a, b = as + e + \frac{mq}{2})$, 通过自举输出 $c' = (a', b' = as' + e' + \frac{q}{4}m)$, 其中 $|e'| < \frac{q}{16}$ 。

因此, 通过上述对 FHEW 类型自举技术的阐述, 首先需要分析本文算法第 3)~7) 行的正确性。假设给定单项式 X^m , 同时给定 NTRU 密文 $\text{NTRU}'_{Q_f}(m'), m' \in \{0, 1\}$, 计算

$$(X^m - 1) \cdot \text{NTRU}'_{Q_f}(m') + g \quad (26)$$

如果 $m' = 0$, 则上述公式的计算结果为一个关于 X^0 的 NTRU 加密; 如果 $m' = 1$, 则其结果为关于 X^m 的 NTRU 加密。显然, m' 的值决定了结果密文是关于 X^0 还是 X^m 的加密。所以在算法 Acc 中总是能得到关于单项式 $X^{a_i \cdot s_i + a_{i+1} \cdot s_{i+1}}$ 的加密。因此, 给定多密钥 LWE 密文 $c = (a_0, \dots, a_{n-1}, \dots, a_{nk-1}, b)$, 在算法第 3)~7) 行经过 $nk/2$ 次循环内积运算后, 根据在上文中提到的 NTRU 密文内积运算特性, 能够得到关于 $\lfloor \frac{Q}{8} \rfloor \cdot$

$Y^{b + \frac{q}{4} - \sum a_i \cdot s_i} \cdot \sum_{i=0}^{N-1} X^i$ 的 NTRU 加密。在明文层面, 本文算法是正确的, 但是还需要探讨多密钥 NTRU 密文间的运算, 才能进行后续的正确性分析。假设给定在密钥 f_i 下加密的 NTRU 密文 $\text{NTRU}_{Q_{f_i}}(m)$, 以及在密钥 f_{i+1} 下加密的向量型 NTRU 密文 $\text{NTRU}'_{Q_{f_i}}(m')$, 其内积运算结果

$$\text{NTRU}_{Q_{f_i}}(m) \odot \text{NTRU}'_{Q_{f_{i+1}}}(m') = \frac{g_{i+1}}{f_{i+1}} + \frac{g_i}{f_i} + mm' \quad (27)$$

因此, 对于算法第 3)~7) 行的输出结果密文为

$$\text{Acc} = \frac{g_1}{f_1} + \dots + \frac{g_k}{f_k} + \lfloor \frac{Q}{8} \rfloor \cdot Y^{u(m)} \cdot \sum_{i=0}^{N-1} X^i \quad (28)$$

上述结果密文中的明文是符合期望结果的,

满足正确性要求。同时，对于密文内积运算，假设 $\mathbf{g}^{-1}(\text{NTRU}_{Qf_i}(m))$ 的分解结果为 $(h_0, \dots, h_{d-1})$ ，其中元素 h_i 的系数属于 $\{-1, 0, 1\}$ ，因此，对于结果密文 Acc 中的 g_i ，其系数变化等同于 $\sum_{j=0}^{n/2-1} \sum_{i=0}^{d-1} h_{j,i} \cdot g_{j,i}$ 的变化结果，这一结果与实际 g_i 在于单项式 X^m 的差别，但是单项式并不会影响结果多项式的范数，因为这一结果涉及最终噪声的计算，因此本文使用了这一方式来量化噪声，假设在自举密钥 evk 中 g_i 的系数上限为 B ，则在过程 g'_i 的系数上限为 $B' = \frac{n}{2} dNB$ 。接下来，根据算法过程，需要分析 HybridProduct 算法的正确性。

首先，在 HybridProduct 算法中每个参与方都会使用一个多项式密钥 z_j ，将 $\mathbf{z} = (z_1, \dots, z_k) \in R^{k+1}$ 表示为各参与方的联合密钥，那么 HybridProduct 算法输出的结果 D_i 可以看作在密钥 $\mathbf{z}$ 下对各参与方 NTRU 密钥 f_i 的加密，因为关于 D_i 的运算满足

$$D_i \cdot \mathbf{z} \approx f_i \cdot \mathbf{g}_{k+1} \cdot \mathbf{z} \in R_Q^{d(k+1)} \quad (29)$$

因此，若给定一个在密钥 $\mathbf{z}$ 下加密的 RLWE 密文 c ，其与 D_i 进行内积运算的解密结果满足

$$c \odot D_i \cdot \mathbf{z} = \mathbf{g}_{k+1}^{-1}(c) \cdot D_i \cdot \mathbf{z} = f_i \cdot \langle c, \mathbf{z} \rangle \quad (30)$$

因为在本文算法第9)行将 Acc 设置为一个在密钥 $\mathbf{z}$ 下加密的 RLWE 密文，而经过算法第8)行的处理，此时的 $\text{Acc}_0 = \frac{g_1}{f_1} + \dots + \frac{g_k}{f_k} + \lfloor \frac{Q}{4} \rfloor \cdot Y^{u(m)} \cdot \sum_{i=0}^{N-1} X^i$ ，因此经过 k 次内积运算后， Acc 实际上是关于 $\lfloor \frac{Q}{4} \rfloor \cdot Y^{u(m)} \cdot \sum_{i=0}^{N-1} X^i \cdot \prod f_i$ ，因为本文方案设置的 NTRU 密钥为 $f = 4f' + 1$ ，因此，常数项结果为 $\frac{Q}{4} m$ ，即 Acc 为一个在密钥 $\mathbf{z}$ 下关于 $\frac{Q}{4} m$ 的加密。因此，HybridProduct 算法也是满足正确性的。

此外，这一过程也会引起密文中噪声的变化，从对矩阵 D_i 的解密结果分析，对于 $D_i \cdot \mathbf{z}$ ，噪声项为 $e = r_i \cdot e_j + r_i \cdot e'_j + z_i \cdot e_{i,1} + M_j \cdot e_{i,2}$ ，其中， $M_j \in R^{d \times d}$ 是一个第 l 行为 $\mathbf{g}^{-1}(b_j[l])$ 的矩阵， e'_j 为一个分解噪声，其系数属于 $\{0, 1\}$ ，假设

$e_j, e_{i,1}, e_{i,2}$ 的系数上限也为 B ，对于解密结果中的噪声上限为 $B'' = (d+2)NB + N$ ，而在本文算法第11)~13)行，经过 k 次运算后，其噪声项为 $\pm 1 \prod_{i \in [k]} f_i + \prod_{i \in [k]} (g'_i \prod f_i) + \prod_{i \in [k]} (e \prod f_i)$ ，噪声上限为 $kN + kB' + kB''$ 。因此，关于 HybridProduct 算法及其相关计算也是满足正确性的。

最后，关于明文提取、模数切换以及密钥切换算法，这一系列算法在各自举方案中，包括 FHEW、TFHE、NTRU 自举等^[23]均为通用算法，其主要过程就是首先将一个 RLWE 密文根据环多项式反循环矩阵的性质，将其系数提取为一个在模数 Q 下的 LWE 密文，随后通过模数转换算法将模数 Q 转换为原始 LWE 密文的模数 q ，再通过密钥切换算法将在联合密钥 $\mathbf{z} = (z_0, \dots, z_{n-1}, \dots, z_{nk-1})$ 下加密的 LWE 密文切换为在各参与方原始 LWE 密钥 $\mathbf{s} = (s_0, \dots, s_{n-1}, \dots, s_{nk-1})$ 下加密的 LWE 密文，因此本文对其正确性不再进行阐述。

通过上述对本文所设计的 MK-FHE 中主要算法的正确性分析，本文所设计的 MK-FHE 方案能够正确、有效地实现对不同密钥下加密的 LWE 密文转换到同一密钥下加密的 LWE 密文。综上所述，本文是正确的。

3.2 MK-FHE 算法安全性

在第1.2节中描述的 RLWE 假设和 NTRU 假设下，提出的 MKFHE 方案在语义 (indistinguishability under chosen-plaintext attack, IND-CPA) 上是安全的，这是一个标准的混合论证。具体来说，该方案的语义安全性依赖于以下4种类型的实例在计算上不可区分于均匀分布的特性，非正式地保证加密不会向被动对手透露加密消息。

1) 密文 c ：是维数为 n ，模数为 q ，噪声分布为 χ ，基于均匀二进制密钥分布的 LWE 加密。

2) 多密钥切换密钥 ksk ：是维数为 n ，模数为 q ，噪声分布为 χ^d ，基于均匀二进制密钥分布的 LWE 加密。

3) 自举密钥 evk ：是维数为 n ，密钥 $f \in R$ ，多项式向量 $\mathbf{g} \in R_Q$ ，基于三元密钥分布的 NTRU 加密。

4) HybridProduct: 是模数为 Q , 噪声分布为 χ , 基于三元密钥分布的 NTRU 加密。

公认地, LWE 和 RLWE 从最坏情况下的困难假设中获得了强有力的安全保证。NTRU 变体的安全性由 Stehlé 等^[24]在假设 RLWE 问题难解的基础上进行了证明, 但要求 f 和 g 必须从足够大标准差 $\text{poly}(N) \sqrt{Q}$ 的离散高斯分布中采样 (N 是 NTRU 的环维数, Q 是模数)。然而, 基于 NTRU 的全同态加密系统的具体安全性更为复杂, 因为应用文献^[24]结果所需的标准差通常过大。具有大模数的“过度扩展”的 NTRU 实例在实践中很容易被破解^[25-27]。Kirchner 等^[27]表明可以利用 NTRU 格中存在的稠密子格进行攻击, 由于参数的选择, 攻击是可行的。对于随机三元密钥, 模数 Q 小至 $N^{2.783 + o(1)}$ 时就被认为是过度扩展。Ducas 等^[28]的研究为该“疲劳点”得出更紧密的值, 即 $Q = N^{2.484 + o(1)}$ 。分析模数 Q 在何种情况下会使得稠密子格发现攻击比密钥恢复更有效来确定这一点。具体来说, 疲劳点被估计在 $Q \approx 0.004 \cdot N^{2.484 + o(1)}$, 适用于 $N > 100$ 。尽管 Ducas 等的分析集中在环 $\mathbf{Z}_Q[X]/(X^N - 1)$ 上的循环 NTRU, 而本文提出的方案在 $\mathbf{Z}_Q[X]/(X^N + 1)$ 上实现, 显然, 反循环版 NTRU 的安全性不会比循环版本弱。

由于自举密钥和多密钥切换密钥分别是基本方案和混合乘积密钥的加密, 需要假设该方案是循环安全的。目前尚不清楚是否可以在已知此类加密的情况下获得可证明的安全性 (在标准假设

下), 或者是否可以利用这些加密来攻击 FHE 方案。截至目前, 所有不受限制的 FHE 方案 (在单密钥和多密钥设置中) 都需要此假设。

3.3 方案分析与对比

下面对本文提出的基于 NTRU 自举的 MK-FHE 方案与其他类似 FHEH 的 MK-FHE、批处理 MK-FHE 和全动态 MK-FHE 方案进行比较, 其结果如表 1 所示。表 1 中, k 是与密文相关的密钥的实际数量, K 表示 k 的设计上限, L 表示同态评估的布尔电路的最大深度 (无引导), n 是用于安全性的底层 LWE 问题的维度。 $\tilde{O}$ 符号隐藏了某些多项式函数的形式为 $\log \text{poly}(n, k, l)$ 的因子。 $|\text{pk}|$ 和 $|\text{CT}|$ 分别表示 pk 和密文的大小, 其中所有大小均以位为单位。CRM 表示方案中是否需要公共参考矩阵。

本文在 2022 年开源的代码 NTRUFatigue 基础上, 对所提方案进行了实现, 并计算了密文扩展时间。实验初始环境如下: Intel Core i5-7500 CPU @ 3.40GHz 3.40 GHz、32.0 GB RAM、64 位操作系统、VS2010 C++ 编译环境。初始参数如下: LWE 维度 $n = 500$ 、模数 $q = 2^9$ 、多项式深度 $N = 2^{10}$ 、分解基数 $B = 2^{11}$ 、多项式模数 Q 为 2 的幂次方, 实验中设置 $Q = 2^{32}$ 。此外, 实验设置了 3 个参与方 P_0 、 P_1 和 P_2 分别对应密钥 t_0 、密钥 t_1 、密钥 t_2 , 其中 t_i 的元素从二元组中选取, 给定 P_i 加密的 LWE 密文 $c_i = (a_i, a_i \cdot t_i + e_i + m_i q/2)$, 其中 $|e_i| < \frac{q}{16}$ 。首先将 c_0 和 c_1 扩展为在

表 1 多密钥同态加密方案对比

Table 1 Comparison of Multi-key FHE schemes

方案	$ \text{pk} $	$ \text{CT} $	CRM	动态	假设	自举
Clear 等 ^[12] 方案	$\tilde{O}(nL^2)$	$\tilde{O}(n^2 k^2 L^2)$	Yes	No	LWE	No
Brakerski 等 ^[29] 方案	$\tilde{O}(n^3)$	$\tilde{O}(nk)$	Yes	Yes	LWE&Circular security	Yes
Mukherjee 等 ^[13] 方案	$\tilde{O}(nL^2)$	$\tilde{O}(n^2 k^2 L^2)$	Yes	No	LWE	Yes
Peikert 等#1 ^[30] 方案	$\tilde{O}(n(K+L)^2)$	$\tilde{O}(n^3 k(K+L)^4)$	Yes	Yes	LWE	No
Peikert 等#2 ^[31] 方案	$\tilde{O}(n^4(K+L)^4)$	$\tilde{O}(n^2 k^2(K+L)^2)$	Yes	Yes	LWE&Circular security	No
Chen 等 ^[14] 方案	$\tilde{O}(n^2 k^2)$	$\tilde{O}(nk)$	Yes	No	RLWE&Circular security	Yes
Kim 等 ^[23] 方案	$\tilde{O}(nd^2)$	$\tilde{O}(n^2 k^2 d^2)$	No	No	LWE	Yes
Chen 等 ^[32] 方案	$\tilde{O}(n^3(K+L)^2)$	$\tilde{O}(n^2 k^2(K+L)^2)$	Yes	Yes	LWE	No
本文的方案	$\tilde{O}(Kd(n+q))$	$\tilde{O}(nk)$	No	Yes	RLWE	Yes

密钥 $t = (t_0, t_1)$ 这一级联密钥下的加密密文 c'_0 和 c'_1 ，并进行同态与非运算得到密文 $c_{0\bar{A}1}$ ，随后通过本文所提出的算法对结果密文进行多密钥自举得到噪声刷新的LWE密文 $c'_{0\bar{A}1}$ ，其解密结果为 $m_0 \bar{\wedge} m_1$ ，多密钥自举过程总体耗时约为 0.11 s，而在本文所提出的算法第3)~7)行同态解密过程耗时约为 0.08 s。随后，本文方案继续将密文 $c'_{0\bar{A}1}$ 和密文 c_2 分别设置为在联合密钥 $t = (t_0, t_1, t_2)$ 下的LWE加密 $c''_{0\bar{A}1}, c'_2$ 并执行同态加法运算 $c''_{0\bar{A}1} + c'_2$ ，随后通过本文算法刷新噪声并对结果密文解密，其解密结果为 $m_0 \wedge m_1 + m_2$ ，多密钥自举过程总体耗时约为 0.17 s，而在算法第3)~7)行同态解密过程花费时间约为 0.12 s，上述耗时满足所需快速傅里叶变换次数的比例，如当参与方为2方时，算法3)~7)行所需快速傅里叶变换次数为 $2n(1+d) + (1+d) = 4004$ ，当参与方数量为3方时，算法3)~7)行所需快速傅里叶变换次数为 $3n(1+d) + (1+d) = 6004$ ，因此对一个比特密文的密文扩展时间结果与理论预估时间大致吻合。此外，随着参与方的增加，本文方案对密文进行多密钥扩展的时间是呈线性增加的。

4 应用场景

本节进一步探索了该方案在各个行业中的潜在应用及可行性。本文提出的基于NTRU自举的多密钥全同态加密技术能够在各行业中解决零售行业中多源销售数据监管存在的数据隐私安全流通问题中提供支持，从而有效地保护各行业核心数据。

在多行业多源销售数据监管场景下，以零售税费计算需求为例，公共税务部门计算不同行业的多源数据税收时，需要收集统计所有参与方的销售数据，以实现全面的税务核算和审计。但各行业、各参与方等数据属于商业机密和个人隐私，尤其是销售数量，直接反映了企业的市场表现、竞争力、库存管理及其对市场需求的响应能力。这些数据泄露可能导致竞争对手获取企业的战略信息，甚至影响企业的运营和市场份额。因此，各参与方无法直接将这些敏感信息提供给公共税务部门，税务部门作为税务监管方无法直接获取商品的销售金额等数据来对相关税收进行查

验。在此背景下，多密钥同态加密方案成为一个较为理想的解决方法，其不仅能够保护不同参与方的订货、销售等机密数据，同时还能够应用于各行业不同来源销售数据的聚合密态处理，并能够在税务计算、税务监管等方面中起到重要作用。多密钥同态加密在销售数据跨部门监管应用场景如图1所示。

各行业参与计算的参与方将不同类型的商品销售单价、数量通过密钥将加密数据提供给政务云服务提供方。政务云服务提供方通过多密钥全同态加密方案中的相关算法将密文扩展为新的密文后，通过电路将扩展后的密文与公共税务部门提供的税率计算函数进行同态加密计算得到多密钥隐私计算的结果。公共税务部门通过联合解密算法将多密钥隐私计算的结果进行解密从而获取到其所需要查验的数据。具体流程如下。

现有计算参与方 $S_1, S_2, S_3 \dots$ 提供 $A, B, C \dots$ 不同类型商品销售数量， $p_A, p_B, p_C \dots$ 表示各商品类型的销售单价， $n_A, n_B, n_C \dots$ 表示各类商品的销售数量。首先各个销售网点运行算法进行参数的初始化并分别生成密钥 $k_1, k_2, k_3 \dots$ 。将其不同种类的商品销售数据分别加密为 $C_{n_{A,S_1}}^{k_1}, C_{n_{B,S_1}}^{k_1}, C_{n_{C,S_1}}^{k_1} \dots$ 并提供给政务云服务提供方进行处理。政务云服务提供方把不同参与方 $S_1, S_2, S_3 \dots$ 加密后的各类商品销售数据密文 $C_{n_{A,S_1}}^{k_1}, C_{n_{B,S_1}}^{k_1}, C_{n_{C,S_1}}^{k_1} \dots$ 通过多密钥同态加密算法将其扩展为：

$$\begin{aligned} C_{n_{A,S_1}}^{k_1} &\rightarrow C_{n_{A,S_1}}^{k_1, k_2, k_3 \dots}, C_{n_{B,S_1}}^{k_1} \rightarrow C_{n_{B,S_1}}^{k_1, k_2, k_3 \dots}, \dots \\ C_{n_{A,S_2}}^{k_2} &\rightarrow C_{n_{A,S_2}}^{k_1, k_2, k_3 \dots}, C_{n_{B,S_2}}^{k_2} \rightarrow C_{n_{B,S_2}}^{k_1, k_2, k_3 \dots}, \dots \\ C_{n_{A,S_3}}^{k_3} &\rightarrow C_{n_{A,S_3}}^{k_1, k_2, k_3 \dots}, C_{n_{B,S_3}}^{k_3} \rightarrow C_{n_{B,S_3}}^{k_1, k_2, k_3 \dots}, \dots \end{aligned} \quad (31)$$

再通过已有运算电路

$$\begin{aligned} &(n_{A,S_1} + n_{A,S_2} + n_{A,S_3} + \dots) \cdot p_A + \\ &(n_{B,S_1} + n_{B,S_2} + n_{B,S_3} + \dots) \cdot p_B + \dots \end{aligned} \quad (32)$$

对扩展后的密文进行同态运算，公共税务部门提供的税率计算函数在政务云服务提供方的计算电路中被转化为一个评估函数 f ，该函数将扩展后的加密销售数据与税率相结合，从而进行计算：

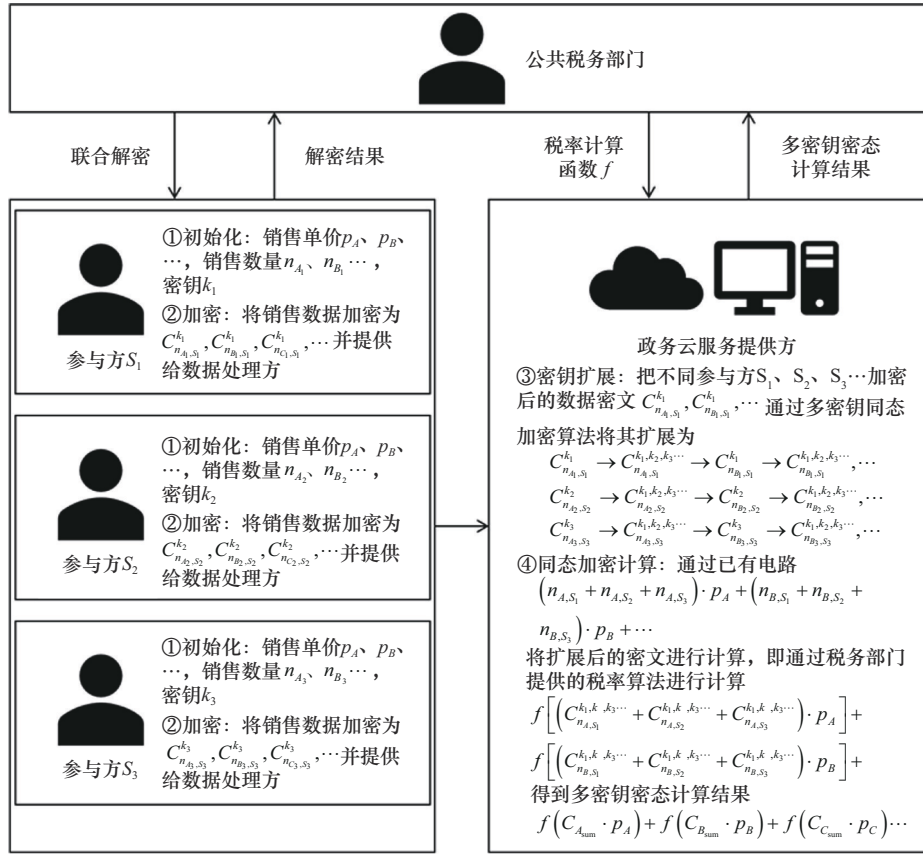


图1 多密钥同态加密在销售数据跨部门监管应用

Figure 1 Multi-key homomorphic encryption in cross-departmental supervision of sales data

$$f\left[\left(C_{n_{A, S_1}}^{k_1, k_2, k_3, \dots} + C_{n_{A, S_2}}^{k_1, k_2, k_3, \dots} + C_{n_{A, S_3}}^{k_1, k_2, k_3, \dots}\right) \cdot p_A\right] +$$

$$f\left[\left(C_{n_{B, S_1}}^{k_1, k_2, k_3, \dots} + C_{n_{B, S_2}}^{k_1, k_2, k_3, \dots} + C_{n_{B, S_3}}^{k_1, k_2, k_3, \dots}\right) \cdot p_B\right] \dots \quad (33)$$

得到多密钥隐私计算结果 $f(C_{A_{\text{sum}}} \cdot p_A) + f(C_{B_{\text{sum}}} \cdot p_B) + f(C_{C_{\text{sum}}} \cdot p_C) \dots$ 并发送给公共税务部门。公共税务部门通过对多密钥隐私计算后的密文进行联合解密, 从而得到所有计算参与方销售数据聚合后的结果。该方案使得在处理大规模多源数据时, 可以通过频繁而高效的自举运算, 保证密文深度不会随着多次加密运算而累积增长, 从而显著提高运算效率并保持结果精确度。特别是在税收核算计算过程中, NTRU 自举技术的引入能够在不影响密文数据安全性的情况下, 优化加密数据的计算链路, 不仅保护了各计算参与方的个人隐私数据, 同时公共税务部门能够收集到所需的整体税务数据来查验是否存在不合法合规的情况, 从而解

决了多行业多源销售数据跨部门监管存在的数据隐私安全流通这一问题, 能够更好地实现各行业的数字化转型和健康发展。

5 结束语

本文基于 NTRU 自举技术构造了一种多密钥全同态加密方案, 相较于传统的 NTRU 自举技术, 在保证安全性的同时具有更高的计算效率和更小的公钥长度, 在综合效率上有了一定的提升, 同时, 讨论了将方案结合到多行业多源销售数据聚合与税务协同计算场景中, 用于解决多源数据跨部门监管中存在的数据隐私安全流通问题。然而, 本文为了提高同态解密效率, 在自举密钥生成时相较于原有的方案需要生成 1.5 倍的密钥数量, 即本文方案的自举密钥长度是原有方案的 1.5 倍。在未来的工作中, 会继续完善方案并在自举密钥空间复杂度持平的情况下实现同态解密过程的效率提高。

参考文献:

- [1] 杨德春, 冉彬, 孔令虎, 等. 以数据为核心的烟草制造行业数字化转型[J]. 智能制造, 2021, (1): 106-109.
YANG D C, RAN B, KONG L H, et al. Digital transformation of tobacco manufacturing industry with data as the core[J]. Intelligent Manufacturing, 2021, (1): 106-109.
- [2] 李凤华, 李晖, 贾焰, 俞能海, 等. 隐私计算研究范畴及发展趋势[J]. 通信学报, 2016, 37(4): 4.
LI F H, LI H, JIA Y, YU N H, et al. Privacy computing: concept, connotation and its research trend[J]. Journal on Communications, 2016, 37(4): 4.
- [3] YAO A C. Protocols for secure computations[C]//23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). IEEE, 1982: 160-164.
- [4] YANG Q, LIU Y, CHEN T, et al. Federated machine learning: concept and applications[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2019, 10(2): 1-19.
- [5] 杨帆, 孙奕, 陈性元, 等. 基于同态代理重认证的可验证联邦聚合方法[J]. 网络与信息安全学报, 2024, 10(3): 91-106.
YANG F, SUN Y, CHEN X Y, et al. Verifiable federated aggregation method based on homomorphic proxy re-authentication[J]. Chinese Journal of Network and Information Security, 2024, 10(3): 91-106.
- [6] SABT M, ACHEMLAL M, BOUABDALLAH A. Trusted execution environment: what it is, and what it is not [C] // 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015(1): 57-64.
- [7] 张晓均, 张经伟, 黄超, 等. 可验证医疗密态数据聚合与统计分析方案[J]. 软件学报, 2022, 33(11): 4285-4304.
ZHANG X J, ZHANG J W, CHEN Y X, et al. Verifiable encrypted medical data aggregation and statistical analysis scheme[J]. Journal of Software, 2022, 33(11): 4285-4304.
- [8] 任艳丽, 余凌赞, 何港, 等. 一种隐私保护的卷积神经网络预测方案[J]. 计算机学报, 2023, 46(8): 1606-1619.
REN Y L, YU L Z, HE G, et al. A scheme of privacy-preserving convolutional neural network prediction[J]. Chinese Journal of Computers, 2023, 46(8): 1606-1619.
- [9] 李宇溪, 周福才, 徐紫枫. 支持K-近邻搜索的移动社交网络隐私保护方案[J]. 计算机学报, 2021, 44(7): 1481-1500.
LI Y X, ZHOU F C, XU Z F. Privacy-preserving k-nearest-neighbor search over mobile social network[J]. Chinese Journal of Computers, 2021, 44(7): 1481-1500.
- [10] 肖文乾, 杨高波, 王德望, 等. 基于加法同态加密与多高位嵌入的加密域图像可逆信息隐藏[J]. 网络与信息安全学报, 2023, 9(4): 121-133.
XIAO W Q, YANG G B, WANG D W, et al. Reversible data hiding in encrypted images based on additive homomorphic encryption and multi-MSB embedding[J]. Chinese Journal of Network and Information Security, 2023, 9(4): 121-133.
- [11] LÓPEZ-ALT A, TROMER E, VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]//Proceedings of the 44th Annual ACM Symposium on Theory of Computing. 2012: 1219-1234.
- [12] CLEAR M, MCGOLDRICK C. Multi-identity and multi-key leveled FHE from learning with errors[C]//Advances in Cryptology--CRYPTO 2015: 35th Annual Cryptology Conference. 2015: 630-656.
- [13] MUKHERJEE P, WICHS D. Two round multiparty computation via multi-key FHE[C]//Advances in Cryptology - EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2016: 735-763.
- [14] CHEN H, CHILLOTTI I, SONG Y. Multi-key homomorphic encryption from TFHE[C]//Advances in Cryptology - ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security. 2019: 446-472.
- [15] XU K, TAN B H M, WANG L P, et al. Multi-key fully homomorphic encryption from NTRU and (R) LWE with faster bootstrapping[J]. Theoretical Computer Science, 2023, 968: 114026.
- [16] BONTE C, ILIASHENKO I, PARK J, et al. FINAL: faster FHE instantiated with NTRU and LWE[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2022: 188-215.
- [17] KLUCZNIAK K. NTRU-v-um: secure fully homomorphic encryption from NTRU with small modulus[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 1783-1797.
- [18] XIANG B, ZHANG J, DENG Y, et al. Fast blind rotation for bootstrapping FHEs[C]//Annual International Cryptology Conference. 2023: 3-36.
- [19] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.
- [20] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[C]//Proc Int Algorithmic Number Theory Symp. 1998: 267-288.
- [21] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//STOC, ACM, 2005: 84-93.
- [22] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C]//Advances in Cryptology-EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2010: 1-23.
- [23] KIM E, LEE H S, PARK J. Towards round-optimal secure multiparty computations: multikey FHE without a CRS[C]//Information Security and Privacy, ACISP 2018, 2018: 101-113.
- [24] STEHLÉ D, STEINFELD R. Making NTRU as secure as worst-case problems over ideal lattices[C]//Advances in Cryptology - EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2011: 27-47.
- [25] ALBRECHT M R, BAI S, DUCAS L. A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes[C]//CRYPTO, Lecture Notes in Computer Science. 2016: 153-178.
- [26] CHEON J H, JEONG J, LEE C. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero[J]. LMS Journal of Computation and Mathematics, 2016, 19: 255-266.
- [27] KIRCHNER P, FOUQUE P. Revisiting lattice attacks on overstretched NTRU parameters[C]//EUROCRYPT, Lecture Notes in

- Computer Science, 2017: 3-26.
- [28] DUCAS L, VAN-WOERDEN W P J. NTRU fatigue: how stretched is overstretched[C]//ASIACRYPT, Lecture Notes in Computer Science. 2021,: 3-32.
- [29] BRAKERSKI Z, PERLMAN R. Lattice-based fully dynamic multi-key FHE with short ciphertexts[C]//Annual International Cryptology Conference. 2016: 190-213.
- [30] PEIKERT C. Public-key cryptosystems from the worst-case shortest vector problem[C]//Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. 2009: 333-342.
- [31] PEIKERT C, SHIEH I. Multi-key FHE from LWE, revisited[C]//Theory of Cryptography Conference. 2016: 217-238.
- [32] CHEN Y, DONG S, LI T, et al. Dynamic multi-key FHE in asymmetric key setting from LWE[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 5239-5249.

[作者简介]



郑俊华 (1978-), 男, 浙江金华人, 中国烟草总公司广东省公司信息中心工程师, 主要研究方向为计算机软件与信息安全。



江宏伟 (1980-), 男, 河南信阳人, 中国烟草总公司广东省公司信息中心高级工程师, 主要研究方向为网络和数据安全防护。



刘荣 (1982-), 男, 广东省韶关人, 中国烟草总公司广东省公司信息中心高级工程师, 主要研究方向为云平台、大数据。



李沂修 (2000-), 男, 河北邯郸人, 暨南大学硕士生, 主要研究方向为密码学与信息安全。



李闻 (1981-), 男, 江西鄱阳人, 中国烟草总公司广东省公司信息中心高级工程师, 主任科员, 主要研究方向为计算机应用技术。



翁健 (1976-), 男, 广东茂名人, 暨南大学教授、博士生导师, 主要研究方向为密码学、云计算安全、区块链与信息安全。