

同态加密专栏

全同态加密研究*

李增鹏¹, 马春光^{1,2}, 周红生³

1. 哈尔滨工程大学 计算机科学与技术学院, 哈尔滨 150001
2. 中国科学院信息工程研究所 信息安全部国家重点实验室, 北京 100093
3. 弗吉尼亚联邦大学 工程学院计算机系, 里士满 23284-3019

通讯作者: 马春光, E-mail: machunguang@hrbeu.edu.cn

摘要: 随着云计算模式的普及应用, 数据存储和计算服务的外包已经成为必然趋势, 由此带来的数据安全和隐私保护问题愈加受到业界和学界的关注。全同态加密 (fully homomorphic encryption, FHE) 体制, 可在不泄露敏感信息的前提下完成对密文的处理任务, 有着与生俱来的保护用户数据安全和隐私的特性。此外, 由于格密码具有可抵抗量子攻击和同态运算的特性, 这使得基于格的全同态加密研究备受关注, 成为近年密码学界研究的热点问题。当前, 对全同态加密的研究主要集中在两方面, 一方面是方案的设计及性能的提升, 另一方面则是其潜在应用的探索。因此, 本文从全同态加密所经历的三个阶段、基于格的全同态加密体制设计和全同态加密面临的问题及发展趋势等方面, 较为全面地介绍了自 Gentry (STOC 2009) 提出首个全同态加密体制后, 近几年来的重要研究成果。

关键词: 云计算; 格密码体制; 全同态加密体制

中图分类号: TP309.7 **文献标识码:** A **DOI:** 10.13868/j.cnki.jcr.000208

中文引用格式: 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.

英文引用格式: LI Z P, MA C G, ZHOU H S. Overview on fully homomorphic encryption[J]. Journal of Cryptologic Research, 2017, 4(6): 561–578.

Overview on Fully Homomorphic Encryption

LI Zeng-Peng¹, MA Chun-Guang^{1,2}, ZHOU Hong-Sheng³

1. College of Computer Science and Technology, Harbin Engineering University, Harbin 15001, China
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
3. Department of Computer Science, School of Engineering, Virginia Commonwealth University, Richmond, VA23284-3019, U.S.A.

Corresponding author: MA Chun-Guang, E-mail: machunguang@hrbeu.edu.cn

Abstract: With the popularization of cloud computing model, the outsourcing of data storage and computing services has become an inevitable trend, and the issues of data security and privacy protection have attracted more and more attention from the industry and academia. Fully homomorphic

* 基金项目: 国家自然科学基金项目 (61472097)

收稿日期: 2017-06-20 定稿日期: 2017-08-31

encryption (FHE) cryptosystems, which can complete the processing tasks on ciphertexts without leakage of sensitive information, have the inherent characteristics of protecting users' data security and privacy. Moreover, since the lattice cipher has the property of resisting quantum attack and homomorphism operation, it makes the study of lattice-based FHE under the spotlight. Currently, the research of fully homomorphic encryption mainly focuses on two aspects: improving the design and performance of the schemes, and exploring the potential applications. This paper overviews the following: the three phases of fully homomorphic encryptions, lattice-based design of homomorphic encryption systems, and the problems which the fully homomorphic encryptions are facing with. This paper presents a comprehensive review on the important research results in this field since the first fully homomorphic encryption scheme proposed by Gentry (at STOC 2009).

Key words: cloud computing; lattice-based cryptography; fully homomorphic encryption (FHE)

1 前言

云计算是一种基于互联网的计算方式,为我们提供了一个巨大的信息处理平台,通过这种方式,共享的软硬件资源和信息可以按需提供给计算机和其他设备。云计算在提供经济性、可靠性的同时,也对数据安全带来了巨大的挑战。个人数据一旦上传到网上,便失去了对数据的控制,如何保证云端数据的私密性、完整性,成为云计算到来前需解决的首要问题。其次,在云计算和大数据的背景下,各种信息存储于网络、传输于网络、处理于网络,人们对数据安全和隐私保护的要求越来越高。因此,如何在保护数据安全和用户隐私的前提下完成安全计算,是云计算亟待解决的一个实际问题。

全同态加密 (fully homomorphic encryption, FHE) 的诞生,为云计算安全提供了理论上的解决方案,可在不泄露敏感信息的前提下完成对密文的处理任务,有着与生俱来的保护用户数据安全和隐私的特性,在很大程度上解决云计算上的数据安全问题。简单来说,用户可以将数据加密后以密态的形式保存在云端。除非获得加密者的私钥,否则无人可以获得明文。但用户又可以对云端的密文进行有意义的操作。全同态加密允许合理利用此类密态数据,同时又不影响用户的隐私。

事实上,同态密码的概念最初是由 Rivest, Adleman 和 Dertouzos^[1]三人于 1978 年提出的隐私同态 (privacy homomorphic) 概念。他们给出一个“保密数据库 (private data banks)”的应用场景: 用户将个人敏感数据加密后存储在一个不可信的服务器中,并给出正确的查询应答。因此,从某种角度讲,“保密数据库”的思想已经基本完整涵盖了数据存储与数据处理过程,完全可以将其视作当今流行的安全云存储与安全云计算融合的一种概念性雏形^[2,3]。许多密码学家都将全同态加密思想置于与公钥加密思想比肩齐名的重要地位^[4-11],他们认为,“公钥加密方案开辟了密码学的新方向,而实用的全同态加密方案则将催生新型分布式计算模式”。全同态加密概念自提出后近 30 年来,一直被密码学界誉为“密码学圣杯”。

我们所熟知的经典密码学算法,如 RSA^[12], ElGamal^[6]乘法同态方案, Paillier^[9]加法同态方案也被称为同态密码方案,但这些方案仅能算作部分同态加密 (partly homomorphic encryption) 方案,即仅支持一种同态运算,要么是加密运算,要么是乘法运算。而随着量子计算机的发展,上述密码体制由于无法抵抗量子攻击而面临着被淘汰的潜在风险。同时,可抗量子攻击的格密码体制成为后量子密码研究中最为核心的研究领域,其与生俱来可抗量子攻击和支持同态运算的特性,为基于格的全同态加密体制诞生奠定了基础。在同态加密的概念出现 30 年后,第一个真正意义上的全同态加密算法出现。在 2009 年的 STOC 国际会议上, Graig Gentry^[13]给出了第一个基于理想格的全同态加密解决方案,从理论上解决了这一公开问题。学术界和产业界一致对这一创新工作给予了高度评价,深信该“圣杯真实的存在”,相信存在若干全同态加密的构造方案有待发掘,并认为这一重大技术突破将有助于改变或消除公众对云计算应用安全问题(特别是隐私保护问题)的普遍担忧,并极有可能会催生一些新型安全应用的出现。自此,设计出实用化的全同态加密方案成为密码学界和业界孜孜以求的共同目标。而全同态加密也成为密码学基础理论研究中的一个热门课题,近几年来,在三大密码会议及 TCC 等密码学顶级会议中,全同态加密及其应用的研究都占据了相当的比重^[14-31]。

在近 9 年的全同态加密发展过程中,大致可以划分为三个阶段,第一阶段是 Gentry 在 2009 年的突破

性工作^[13]. 第二阶段是 Brakerski 和 Vaikuntanathan 首次利用容错学习 (learning with errors, LWE) 假设实现了 FHE^[16] 并在 Ring-LWE 假设下实现了 FHE^[15]. 第三阶段则是 Gentry 等人^[32] 首次利用近似特征向量的方法实现了 FHE, 该方案就是当前最为经典的 Gentry-Sahai-Waters (GSW) 方案, 在同态运算时不再依赖于计算公钥. 接下来, 本文从 (基于整数和基于格) 全同态加密所经历的三个阶段, 基于格的全同态加密体制设计和全同态加密面临的问题及发展趋势等方面, 来概述全同态加密的发展现状. 在此之前, 我们首先给出全同态加密的定义.

1.1 全同态加密的定义

定义 1 (层级全同态加密) 令 $L = L(\lambda)$ 为一个固定的函数. 为深度为 L 的一类电路 $\{C_\lambda\}_{\lambda \in \mathbb{N}}$ 构造一个 L -层级全同态加密 (leveled FHE) 方案, 该方案包括四个概率多项式时间 (probabilistic polynomial time, PPT) 算法 (KeyGen , Enc , Dec , Eval) 如下:

- 密钥生成算法 KeyGen 是一个随机化算法, 它以安全参数 1^λ 作为输入, 并输出一个公钥 pk 和私钥 sk .
- 加密算法 Enc 是一个随机化算法, 它以一个公钥 pk 和一个消息 $m \in \{0, 1\}$ 为输入, 并输出一个密文 c .
- 解密算法 Dec 是一个确定性算法, 它以一个私钥 sk 和一个密文 c 为输入, 并输出一个消息 $m \in \{0, 1\}$.
- 同态运算算法 Eval 输入一个公钥 pk , 一个运算电路 $C \in \mathcal{C}_\lambda$, 和一个密文列表 $c_1, \dots, c_{\ell(\lambda)}$, 并输出一个密文 c^* .

并要求下述性质成立:

- **正确性.**

- 对于任意 λ , 任意 $m \in \{0, 1\}$, 和由 $\text{KeyGen}(1^\lambda)$ 输出的任意 (pk, sk) , 我们有

$$m = \text{Dec}(\text{sk}, (\text{Enc}(\text{pk}, m)))$$

- 对于任意 λ , 任意 m_1, \dots, m_ℓ , 和任意 $C \in \mathcal{C}_\lambda$, 我们有

$$C(m_1, \dots, m_\ell) = \text{Dec}(\text{sk}, (\text{Eval}(\text{pk}, C, \text{Enc}(\text{pk}, m_1), \dots, \text{Enc}(\text{pk}, m_\ell))))$$

- **紧致性 (Compactness).** 令 $c := \text{Eval}(C, (c_1, \text{pk}_1, \text{evk}_1), \dots, (c_\ell, \text{pk}_\ell, \text{evk}_\ell))$, 那么存在一个多项式 P 满足 $|c| \leq P(\kappa, N)$. 换句话说, 密文 c 的大小与 ℓ 和 $|C|$ 无关. 然而, 允许依据密钥的个数 N 来计算密文.
- **安全性.** 使用选择明文攻击 (chosen plaintext attacks, CPA) 安全性的标准概念来定义安全性. 如果对于任意多项式时间敌手 \mathcal{A} 来说, 下面的公式在 λ 上是可忽略的, 那么我们说一个同态加密方案是不可区分选择明文攻击安全的 (也称为 IND-CPA 安全的):

$$|\Pr[\mathcal{A}(\text{pk}, \text{Enc}(\text{pk}, 0)) = 1] - \Pr[\mathcal{A}(\text{pk}, \text{Enc}(\text{pk}, 1)) = 1]| = \text{negl}(\lambda)$$

其中 $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(1^\lambda)$.

2 全同态加密研究现状

通过对现有文献的分析可以看出, 目前用来构造 FHE 的困难假设, 主要有两种, 一种是格上基于 Regev 的 LWE 问题^[33], 另外一种则是整数上基于 Howgrave-Graham^[34] 的近似最大公约数 (approximate greatest common divisor, AGCD) 问题. 其中, 基于格的构造, 又可进一步分为基于理想

格以 Gentry 方案为蓝图的 FHE 构造; 基于 LWE 假设, 利用密钥交换等技术来实现 FHE 的构造; 基于 LWE 假设, 利用近似特征向量构造的 FHE 方案; 以及基于 NTRU, 利用密钥交换等技术来实现 FHE 的构造. 经典全同态加密方案的构造方法和继承关系如图1所示.

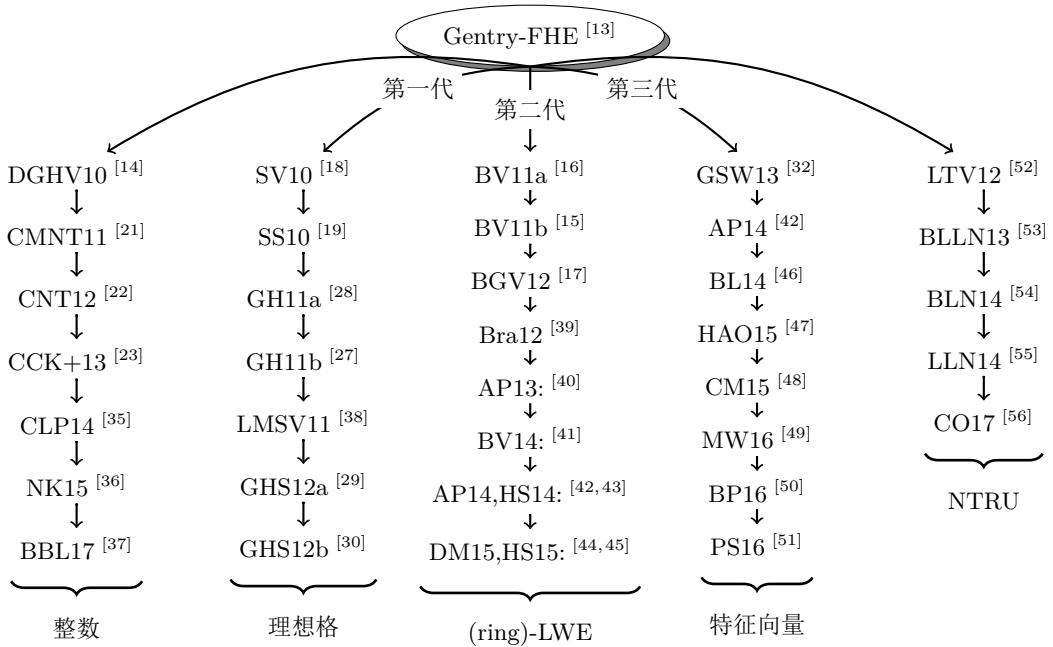


图 1 全同态加密发展概况
Figure 1 Brief history of fully homomorphic encryption

如图1所示, 第 1 列是基于整数上 AGCD 假设的部分 FHE 经典方案, 第 2~4 列则分别是基于格上 LWE 假设的第一、二、三代部分经典的 FHE 方案, 第 5 列则是基于 NTRU 格的部分 FHE 经典方案. 下文着重总结基于格上 LWE 假设的 FHE 方案.

2.1 基于格基的全同态加密研究现状

2.1.1 基于理想格的(第一代)全同态加密研究

Gentry 的 FHE 体制的设计是基于理想格 (ideal lattice) 上的有界编码问题 (bounded distance decoding problem, BDDP) 和稀疏子集和问题 (sparse subset sum problem, SSSP), 其构造过程分为两步: 首先, 设计一个具备有限次密文运算的同态加法和同态乘法的近似同态 (somewhat homomorphic encryption, SWHE) 加密体制, 其运算能力是借助于格上的噪声向量实现. 随着密文运算次数的增加, 噪声逐步增大, 当其超出某一阀值时, 就会出现解密错误. 为此, 引入 “Bootstrapping” 程序, 利用重加密的方法对密文进行更新, 以此控制噪声膨胀, 保证解密正确性, 从而实现任意次的密文同态运算. 尽管该方法可以实现全同态加密所希望的任意次密文运算, 但 Bootstrapping 的过程需将私钥加密后作为公共参数予以公开. 因此, 利用 Bootstrapping 实现的全同态加密体制无法抵抗选择密文攻击 (CCA), 只能达到选择明文攻击 (CPA) 安全. 随后, 文献 [28, 29] 则分别对 Bootstrapping 程序进行改进, 利用主理想格的代数结构取代 Gentry [13] 的理想格, 目的是减少私钥尺寸, 提高解密算法的计算效率, 但缺陷是将私钥由 n 维向量约减到 1 维向量上, 从而增加了方案遭受 Key Recovery 攻击的概率. 此外, Smart 和 Vercauteren 在 Gentry 方案 [13] 的基础上, 提出具有相对小的密钥和密文尺寸的 FHE 方案 [18], 在效率上有所提高. 而 Stehlé 和 Steinfel 利用 “可忽略概率解密错误” 这一弱化条件, 对 Gentry 方案 [13] 进行优化, 提出了较快速的 FHE 方案 [19], 允许降低比特计算复杂度. 但由于 SSSP 假设研究尚不成熟且安全性不充分, 为了使 FHE 方案不再依赖于 SSSP 假设, Brakerski 和 Vaikuntanathan [15, 16] 等人于 2011 年提出基于

LWE 假设的(层级)FHE 方案, 该方法不再依赖于压缩解密电路构造可自举(Bootstrapping)的 FHE 方案, 即不再依赖于 SSSP 假设。以此, 标志着第二代 FHE 方案的诞生。

2.1.2 基于 LWE 的(第二、三代)全同态加密算法构造研究现状

正如上所述, 第二代 FHE 首次利用 LWE 假设来实现。而 LWE 问题自 Regev^[33] 提出以来便引起广泛关注, 可抵抗量子攻击和可简单快速实现的特点, 为格基公钥密码学引入新的发展动力, 已是当前密码学领域一个重要的计算困难问题。格公钥密码系统的主要特点是一般情形下(average-case)解决 LWE 问题并不比在最坏情形下(worst-case)解决一些著名格近似问题简单。简单来说, LWE 问题是给定一个 $m \times n$ 的矩阵 \mathbf{A} 和向量 $\mathbf{b} = \mathbf{As} + \mathbf{e} \pmod{q}$, 去计算 $\mathbf{s} \in \mathbb{Z}_q^n$, 这里 $\mathbf{e} \in \mathbb{Z}_q^m$ 是一个“短”错误向量。2011 年, Brakerski 和 Vaikuntanathan^[15] 在 CRYPTO 上发表了一个基于 Ring-LWE 假设的便于描述和分析的 SWHE 方案, 其安全性规约到理想格上的最坏情形困难问题, 且利用 Gentry 的压缩范式(squashing)和 Bootstrapping 程序将 SWHE 转化为真正的 FHE 方案。同年, Brakerski 和 Vaikuntanathan^[16] 在 FOCS 上发表的 FHE 方案则是完全基于(标准)LWE 假设。方案的安全性依赖于任意格上的最坏情况下短向量问题(short vector problem)的困难性。此外, 与之前的方案相比, BV 方案的主要改进有两点: ① 使用 Relinearization 技术, 将基于 LWE 假设的 Regev 方案^[33] 转换为 SWHE 方案; ② 提出一种新的 Dimension-Modulus Reduction 技术来实现 Bootstrapping 程序, 而不再使用 Gentry 的压缩范式^[13]。该方法能有效缩短密文、降低解密电路的复杂性而无须引入额外假设, 但仍需 Gentry 的 Bootstrapping 程序来实现真正的 FHE 方案。自此, FHE 的研究进入了第二阶段, 即基于(ring)-LWE 假设^[25] 的 FHE 阶段。隔年, Brakerski 等人^[17](即 BGV 方案)在 ITCS 上发表了不再依赖 Gentry 的 Bootstrapping 程序来获得“层级”FHE 方案, 突破 Gentry 构建全同态加密框架, 且分别讨论了在 Ring-LWE 和 LWE 两种假设下的构造。随后, Brakerski^[39] 利用张量乘积技术构造了一个标量不变(scale-invariant)的 FHE 方案, 即, 模 q 与初始化噪声 B 的比例保持不变¹, 从而无需再利用复杂的模交换(modulus switching)技术来控制噪声的增长。此后, 为进一步提升 FHE 方案的计算效率, 若干优化方案也随之提出, 如文献[57]。

2013 年, Gentry 等人^[32] 在 CRYPTO 上发表利用近似特征向量方法来构建 FHE 方案的论文, 即当前经典的 Gentry-Sahai-Waters(GSW) 方案, 标志着 FHE 的研究进入第三阶段。该方案的同态加法和同态乘法都只是通过做简单的矩阵加法和乘法来实现, 从而使得 GSW-FHE 方案相对简单、快速, 容易理解。并且, 实施同态运算时不再像第一、二代同态加密方案一样需要使用计算公钥, 而只需借助用户的公钥即可实现。此外, 他们首次实现了基于身份的 FHE 方案和基于属性的 FHE 方案。但仍需借助 Bootstrapping 程序来实现任意次的同态操作。2014 年, Brakerski 和 Vaikuntanathan^[41] 在 ITCS 上给出一种利用 GSW 方案和 Barrington 定理^[58] 的方法来改进 Bootstrapping 程序的方案, 即利用 Branching Program 来实现同态运算。然而, 同年, Alperin-Sherif 和 Peikert^[42] 则指出利用 Barrington 定理的转化方法是非常低效的并给出了一种运行时间更短且错误增长更小的 Bootstrapping 程序。此外, 他们利用 Micciancio 和 Peikert^[59] 的工具矩阵(gadget matrix) $\mathbf{G} = \mathbf{I} \otimes (2^0, 2^1, \dots, 2^{\lceil \log q \rceil})$, 给出了一种更简单的 FHE 形式。随后的研究多采用该形式, 且提出各种各样的改进方案。

2.2 基于整数的全同态加密算法构造研究现状

在本节中, 我们简单讨论基于整数的 FHE 方案。基于整数的 FHE 方案完全遵循 Gentry 的构造蓝图^[13], 只是在 AGCD 困难假设下的实现。具体来说, 沿着 Gentry 的思路^[13], 2010 年, Dijk 等人^[14] 提出一个完全基于整数运算的 FHE 方案^[14], 以下简称 DGHV 方案。其目的在于简化概念, 即通过在整数上 FHE 的例子去说明即使像 FHE 这样复杂的事情, 也可以通过简单的技术去实现。他们将 SWHE 方案安全性规约到一个困难问题“AGCD 问题”。随后, Coron 等人从 Dijk 等人^[14] 的 DGHV 方案入手, 对 DGHV 方案采用公钥压缩、模交换等技术手段, 来优化整数上的 FHE 方案^[21–23]。具体来说, 2011 年, Coron 等人^[21] 借助于 Gentry-Halevi 对 Gentry 加密方案的实现思想, 将公钥元素中的二次形式替换成线性形式(公钥规模由 $O(\lambda^{10})$ 约减至 $O(\lambda^7)$), 使用简单的算术操作实现了整数上的 FHE 方案。2012 年, Coron 等人^[22] 引入公钥压缩技术将公钥规模从 $O(\lambda^7)$ 约减至 $O(\lambda^5)$ 。2013 年, Cheon 等人^[23] 引入批量密码(batch cryptography)技术, 使其可以加密和同态处理明文向量。2014 年, Coron 等人^[35], 基于

¹方案中的计算过程使用相同的模而不是像“模交换(modulus-switching)”技术中使用的模的阶梯

Brakerski 的 Scale-Invariant FHE 方案^[39], 构造整数上的 Scale-Invariant FHE 方案。2015 年, Nuida 和 Kurosawa^[36] 改进了 Cheon 等人^[23] 的方案, 使消息空间由任意素数 Q 转变为 \mathbb{Z}_Q , 使其解密电路的深度有较大改进。

2.3 比较分析

由上述分析, 我们可以看出。当前的三代 FHE, 尽管在效率方面已有较大提升, 但仍未脱离 Gentry 所提出的利用 Bootstrapping 程序获得满足任意次同态操作的 FHE 方案的原则。在本届中, 我们着重对比分析基于格的三代经典 FHE 方案。在第一代基于理想格的 FHE 方案中, Gentry^[13] 是利用重加密算法来刷新密文降低噪声的规模, 从而实现 Bootstrapping 程序的。以 Brakerski 和 Vaikuntanathan 方案为代表的第二代 FHE 方案^[15, 16], 利用 Key-Switching 技术将维度膨胀的密文约减回原始维度, 利用 Modual-Switching 技术来控制密文噪声的膨胀。其主要优点在于获得层级的 FHE 不再依赖于 Bootstrapping 程序。但若需实现满足任意次同态操作的 FHE, 仍需借助 Bootstrapping 程序。然而, 效率的提升带来了存储开销的加大, 因为 Key-Switching 的实现是借助比特分解算法 BitDecomp(\cdot) 和 2 的幂算法 PowerofTwo(\cdot) 来实现, 而这两个算法则导致密钥尺寸膨胀 $\ell = \text{ceillog } q$ 倍。Gentry, Sahai 和 Waters 三人^[32] 则利用近似特征向量的方法, 即私钥即为密文矩阵的特征向量, 引入工具矩阵 \mathbf{G} , 给出了更加简洁的构造, 从而避免了复杂的 Key-Switching 和 Modual-Switching 技术。更重要的是, 同态运算不会引起密文的膨胀, 因为密文矩阵的维度与工具矩阵 \mathbf{G} 保持一致。但与第二代 FHE 一样, 若要实现满足任意次同态操作的 FHE, 仍需借助 Bootstrapping 程序。此外, 对于 Bootstrapping 程序的优化已有若干显著成果, 我们将在后文中详细的介绍。

3 基于格的全同态加密方案分析

3.1 格公钥密码学概述

王和刘两人^[60] 曾对格密码学做了详细的概述。在传统密码学研究领域, 格仅仅作为分析密码方案的工具, 之前对格的研究主要集中在格基规约研究。1982 年, Lenstra 等人^[61] 提出的 LLL (Lenstra-Lenstra-Lovász) 算法, 已被用于攻击诸多公钥密码方案, 经过几十年的发展, 格基规约算法已经成功地成为攻击各种公钥 Miami 系统最常用的工具之一。1996 年, Ajtai 和 Dwork^[62] 合作提出了第一个基于格困难问题的 AD 加密方案, 尽管当格的维数很高时, AD 加密方案的效率极低, 且没有安全性分析, 但却拉开了基于格设计密码学原语的序幕。目前, 大部分格密码方案都是基于最小整数解 (short integer solution, SIS) 问题和容错学习 (learning with errors, LWE) 问题。这两个问题都可以规约到求解最坏情形下的格困难问题。在保证安全 (即保证足够难度) 的前提条件下, 提高规约的紧致性对格密码方案效率的提高至关重要: 规约越紧, 参数选的越小, 存储量和计算量的效率也就越高。一般地, 基于格上困难问题的公钥密码方案具有以下几个显著优势: ①格问题的计算复杂性: 格上任意随机实例的安全度都相同。这一性质也是格公钥密码学与其他公钥密码学的最主要的区别。Ajtai 早已证明, 格上困难问题在随机实例下的困难度等价于最坏实例下的困难度, 因此格上的公钥密码方案可以选取随机实例, 便于格公钥密码算法的使用和普及。②格基密码计算高效性: 格公钥密码算法涉及的运算通常都是矩阵以及向量间的乘法运算、线性求和运算以及模运算, 相比基于大数分解和离散对数问题所设计的公钥密码方案, 格公钥密码算法计算简单、高效。③格密码安全性: 量子计算机的出现, 迫使必须寻找新的困难问题, 现有研究成果对若干格的困难问题还不存在有效量子算法。因此在格上建立新的公钥密码方案不但打破传统公钥密码垄断局面, 而且更有安全保障, 为公钥密码的设计提供新的思路。此外, 格密码方案所基于的安全问题的平均难度与最大难度相当, 这种新的安全特性增强了人们对使用格密码的信心。

3.2 容错学习 (Learning with Errors, LWE)

格公钥密码系统的主要特点是一般情形下 (average-case) 解决 LWE 问题并不比在最坏情形下 (worst-case) 解决一些著名格近似问题简单。当前, 第二、三阶段的 FHE 构造多基于 LWE 困难问题, 简单来说, LWE 问题是给定一个 $m \times n$ 的矩阵 \mathbf{A} 和向量 $\mathbf{b} = \mathbf{As} + \mathbf{e} \pmod{q}$, 去计算 $\mathbf{s} \in \mathbb{Z}_q^n$, 这里 $\mathbf{e} \in \mathbb{Z}_q^m$ 是一个“短”错误向量。具体来说:

定义 2 (LWE 分布) 对于一个秘密向量 $\mathbf{s} \in \mathbb{Z}_q^n$, 通过均匀随机地选择向量 $\mathbf{a} \in \mathbb{Z}_q^n$, 选取 $e \leftarrow \chi$, 并输出 $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e \pmod{q})$, 来选取 $\mathbb{Z}_q^n \times \mathbb{Z}_q$ 上的 LWE 分布 $\mathcal{A}_{\mathbf{s}, \chi}$.

LWE 问题有两个主要的版本: 搜索 (search) 版本, 是已知 LWE 样本来寻找秘密向量, 判定 (decision) 版本, 是用来区分 LWE 实例和均匀随机样本.

定义 3 (Search-LWE_{n,q,χ,m}) 对于一个均匀随机的 $\mathbf{s} \in \mathbb{Z}_q^n$ (对于所有抽样来说是固定的), 给定了从 $\mathcal{A}_{\mathbf{s}, \chi}$ 中选取的 m 个独立抽样 $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, 从而找到 \mathbf{s} .

定义 4 (Decision-LWE_{n,q,χ,m}) 给定 m 个独立样本 $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, 其中每个抽样取自如下两个分布: (1). $\mathcal{A}_{\mathbf{s}, \chi}$, 其中 $\mathbf{s} \in \mathbb{Z}_q^n$ 是一个均匀随机的秘密向量 (对所有的抽样来说是固定的) 或者 (2). 均匀分布. 即 (以不可忽略的优势) 区分以上两个分布.

Regev^[33] 及其文献 [49, 63] 证明了, 对于恰当的参数, LWE 问题与格的近似最短向量 (shortest vector problem, SVP) 问题同样困难.

3.3 Gentry-Sahai-Waters 方案概述

在本节中, 我们介绍 Gentry-Sahai-Waters (GSW) 全同态加密方案^[32].

令 k 为一个安全参数, L 为 Leveled FHE 方案的层级数. 以下, 我们给出 GSW^[32] 方案的简要描述. 该方案最初是根据函数 BitDecomp, BitDecomp⁻¹ 和 Flatten 来定义的, 但是本来采用 Alperin-Sheriff 和 Peikert 所用的简化方式^[42, 49], 即, 使用工具矩阵 \mathbf{G} .

- 初始化算法 GSW.Setup($1^k, 1^L$):

1. 选择 $\kappa = \kappa(k, L)$ 比特的一个模 q , 参数 $n = n(k, L) \in \mathbb{N}$, $m = m(k, L) = O(n \log(q))$ 和 \mathbb{Z} 上的错误分布 $\chi = \chi(k, L)$.
2. 输出: $\text{params} = (n, q, \chi, m)$. 注意, 令 $\ell = \lfloor \log(q) \rfloor + 1$ 且 $N = (n + 1) \cdot \ell$.

- 密钥生成算法 GSW.KeyGen(params):

1. 均匀选取 $\mathbf{t} = (t_1, \dots, t_n)^T \leftarrow \mathbb{Z}_q^n$ 并计算 $\mathbf{s} \leftarrow (1, -\mathbf{t}^T)^T = (1, -t_1, \dots, -t_n)^T \in \mathbb{Z}_q^{(n+1) \times 1}$;
2. 均匀选取随机公共矩阵 $\mathbf{B} \leftarrow \mathbb{Z}_q^{m \times n}$ 和一个错误向量 $\mathbf{e} \leftarrow \chi^m$;
3. 计算向量 $\mathbf{b} = \mathbf{B}\mathbf{t} + \mathbf{e} \in \mathbb{Z}_q^m$ 并构造矩阵 $\mathbf{A} = (\mathbf{b} | \mathbf{B}) \in \mathbb{Z}_q^{m \times (n+1)}$, 特别的, 这里有,

$$\mathbf{As} = (\mathbf{b} | \mathbf{B})\mathbf{s} = (\mathbf{B}\mathbf{t} + \mathbf{e} | \mathbf{B}) \begin{pmatrix} 1 \\ -\mathbf{t} \end{pmatrix} = \mathbf{B}\mathbf{t} + \mathbf{e} - \mathbf{B}\mathbf{t} = \mathbf{e}$$

4. 返回私钥 $\text{sk} \leftarrow \mathbf{s}$ 和公钥 $\text{pk} \leftarrow \mathbf{A}$.

- 加密算法 $\mathbf{C} \leftarrow \text{GSW.Enc}(\text{params}, \text{pk}, \mu)$: 加密单比特信息 $\mu \in \{0, 1\}$,

1. 令 \mathbf{G} 为如上 $(n + 1) \times N$ 维的工具矩阵, 并均匀选取一个随机矩阵 $\mathbf{R} \leftarrow \{0, 1\}^{m \times N}$;
2. 计算并生成密文 $\mathbf{C} = \mu\mathbf{G} + \mathbf{A}^T\mathbf{R} \pmod{q} \in \mathbb{Z}_q^{(n+1) \times N}$.

这里需要注意的是, 在原始的 GSW 方案中, 加密算法使用 $\text{Flatten}(\mu\mathbf{I} + \text{BitDecomp}(\mathbf{RA})) \in \{0, 1\}^{N \times N}$, 其中 \mathbf{I} 为单位矩阵.

- 解密算法 $\mu' \leftarrow \text{GSW.Dec}(\text{params}, \text{sk}, \mathbf{C})$:

1. 输入私钥 $\text{sk} = \mathbf{s} \in \mathbb{Z}_q^{n+1}$, 令 I 满足 $q/4 < 2^{I-1} \leq q/2$. 令 \mathbf{C}_I 为 \mathbf{C} 的第 I 列;

2. 在 $(-q/2, q/2]$ 范围内计算 $x \leftarrow \langle \mathbf{C}_I, \mathbf{s} \rangle \pmod{q}$; 请注意 $\langle \mathbf{C}_I, \mathbf{s} \rangle = \mathbf{C}_I^T \mathbf{s}$ 并且有

$$\begin{aligned}\mathbf{C}^T \mathbf{s} &= \mu \mathbf{G}^T \mathbf{s} + \mathbf{R}^T \mathbf{A} \mathbf{s} \\ &= \mu(1, 2, 4, \dots)^T + \mathbf{R}^T \mathbf{e} \pmod{q}\end{aligned}$$

选择 \mathbf{C} 的第 I 列对应于选择该向量的第 I 个坐标, 即 $\mu 2^{I-1} + \mathbf{R}_I^T \mathbf{e}$.

3. 输出 $\mu' = \lfloor |x|/2^{I-1} \rfloor$. 因此, 如果 $|x| < 2^{I-2} \leq q/4$ 则返回 0, 如果 $|x| > 2^{I-2}$ 则返回 1.

- 运算算法 GSW.Eval(params, $\mathbf{C}_1, \dots, \mathbf{C}_l$):

- 同态加法运算 GSW.Add($\mathbf{C}_1, \mathbf{C}_2$): 输出

$$\mathbf{C}_1 + \mathbf{C}_2 = (\mu_1 + \mu_2) \mathbf{G} + \mathbf{A}^T (\mathbf{R}_1 + \mathbf{R}_2) \in \mathbb{Z}_q^{(n+1) \times N}$$

- 同态乘法运算 GSW.Mult($\mathbf{C}_1, \mathbf{C}_2$): 计算 $\mathbf{G}^{-1}(\mathbf{C}_2) \in \{0, 1\}^{N \times N}$ 并输出 $\mathbf{C}_1 \mathbf{G}^{-1}(\mathbf{C}_2)$. 即,

$$\begin{aligned}\mathbf{C}_1 \mathbf{G}^{-1}(\mathbf{C}_2) &= (\mu_1 \mathbf{G} + \mathbf{A}^T \mathbf{R}_1) \mathbf{G}^{-1}(\mathbf{C}_2) \\ &= \mu_1 \mathbf{C}_2 + \mathbf{A}^T \mathbf{R}_1 \mathbf{G}^{-1}(\mathbf{C}_2) \\ &= \mu_1 \mu_2 \mathbf{G} + \mathbf{A}^T \mathbf{R}_1 \mathbf{G}^{-1}(\mathbf{C}_2) + \mu_1 \mathbf{A}^T \mathbf{R}_2 \\ &= \mu_1 \mu_2 \mathbf{G} + \mathbf{A}^T (\mathbf{R}_1 \mathbf{G}^{-1}(\mathbf{C}_2) + \mu_1 \mathbf{R}_2) \in \mathbb{Z}_q^{(n+1) \times N}\end{aligned}$$

此外, 也可以通过输出 $\mathbf{G} - \mathbf{C}_1 \mathbf{G}^{-1}(\mathbf{C}_2)$ 来计算一个同态 NAND 门.

注 1 这里, Mukherjee 等 [49] 方案中的解密算法公式是为了选择一个特定的向量 $\mathbf{w} = (0, \dots, 0 | \lceil \frac{q}{2} \rceil)$ 来计算 $\mathbf{s} \mathbf{C} \mathbf{G}^{-1}(\mathbf{w})^T$, 但相比原 GSW 方案的解密算法效率要低得多 (无论是计算时间还是噪声项的大小). 因此, 本文, 我们仍将采用原 GSW 方案的解密算法. 此外, 当 q 为 2 的幂时, 还存在另外一种方式来处理 \mathbb{Z}_q 上的信息. 具体细节参见文献 [32].

3.4 安全性

定理 1 对于参数 $m = O(n \log(q))$, 令参数 (m, n, q, χ) 使得 $\text{LWE}_{(m, n, q, \chi)}$ 困难假设成立, 那么该 GSW 方案是 IND-CPA 安全的.

该证明中的主要步骤是证明 $(\mathbf{A}, \mathbf{RA})$ 与均匀分布是计算不可区分的. 定理的简要证明在文献 [32] 中给出, 本文不再赘述.

4 存在问题及发展趋势

自 Gentry [13] 提出第一个 FHE 方案至今, 全同态加密取得了长足的发展, 但仍存在诸多的不足, 特别是在计算效率、安全性以及全同态加密的应用等方面. 本节中, 将针对 FHE 发展的如下几个方面展开分析, 并进一步探讨下一步的发展趋势.

4.1 全同态加密的性能研究

4.1.1 全同态加密的多比特加密研究

所谓多比特加密技术, 亦可称之为消息封装, 向量 (矩阵) 加密, 批量密码技术. 其实质是一次加密多个比特消息. 然而, 现有 FHE 方案普遍专注于研究单比特的 FHE 方案, 因为一旦获得单比特的 FHE 方案, 通过迭代或者拼接的方式即可获得多比特加密, 但利用这种直接简单的方式, 在 FHE 本身就计算效率低的情形下, 会引起密钥尺寸更长, 计算开销更大, 加密噪声更膨胀等诸多问题. 导致方案的实用价值低, 不足以投入实际应用中. 针对第一代 FHE 方案, 2010 年, Smart 和 Vercauteren 二人 [64] 提出利用中国剩余定理来构造支持单指令多数据 (single instruction multiple data, SIMD) 的同态操作. 随后, 针

对第二代 FHE 方案, 2013 年, Brakerski 等人^[31] 在 PKC 上, 发表了第一个基于 LWE 的密文封装同态加密方案, 他们利用 Peikert 等人^[65] 将多个明文比特封装到一个 Regev 加密方案密文中的方法, 首先将多个比特消息封装, 利用 Regev 加密方案对该封装消息进行加密, 进而对获得的该封装密文进行 Smart-Vercauteren 的 SIMD 同态操作^[64]. 针对第三代 FHE 方案, Hiromasa 等人^[47] 构造了第一个矩阵加密的层级 FHE 方案, 下称 HAO (Hiromasa-Abe-Okamoto) 方案, 该方案支持同态矩阵的加法和乘法运算, 并优化 Alperin-Sheriff 和 Peikert 的 Bootstrapping 程序, 使格的近似因子从 $\tilde{O}(\lambda^3)$ 约减到 $\tilde{O}(\lambda^{2.5})$, 从而利用优化的 Bootstrapping 程序获得可以处理任意次同态操作的 FHE 方案. 然而, 该方案只能逐比特解密而无法实现一次解密, Li 等人^[66] 则基于 dual-Regev 方案 (即 Gentry-Peikert-Vaikuntanathan^[67]) 构造了一种可支持一次解密的多比特 FHE 加密方案. 但因基于 dual-Regev 方案, 使得 Li 等人的方案的密钥及密文尺寸规模增大为 $O(m \log q)$ 而不再是 $O(n \log q)$, 导致其计算开销增大. 随后, Li 等人^[68] 又基于 Regev 方案^[33] 构造了一种支持一次解密的可抗泄漏多比特 FHE 方案.

4.1.2 全同态加密的计算效率提升及实现

FHE 方案的计算效率问题, 是另一个广受关注的问题. 当前的格基 FHE 方案的构造中, 分析其效率低的原因, 有以下两点:

- 自举技术. 即 Bootstrapping 技术, Bootstrapping 是将 SWHE 方案转变为可支持任意次同态操作的 FHE 方案的关键技术, 也是当前可以在固定长度的密钥和密文条件下对任何可以有效操作的函数进行同态运算的唯一途径. 但同时也是制约着 FHE 方案效率的根源. 在 Bootstrapping 程序中, 每个门电路都需同态调用解密电路, 这使得以此为基础的 FHE 方案效率很低.
- 密文膨胀. 现有的 FHE 方案, 在进行同态操作过程中, 密文、密钥及密钥交换矩阵 (第二代 FHE) 的维度急剧膨胀. 特别地, 在基于 LWE 的 FHE 中, 密文、噪声都会以某种规模增长. 例如, 采用重线性化技术的方案, 噪声会成平方增长, $\text{Error} \rightarrow \text{Error}^2$; 采用模交换技术的方案, $\text{Error} \rightarrow O(\|\mathbf{s}\|_1) \cdot \text{Error}$; 采用近似特征值技术的方案, 噪声增长依赖于密文的 1-范数 $\|\mathbf{c}\|_1$.

如何在保证基本安全的前提下, 设计出计算复杂度和空间复杂度可接受的 FHE 方案, 一直是密码学界和业界高度关注的问题. 由于 Bootstrapping 技术需要较大的计算开销, 近年来, 若干工作在逐步提高 Bootstrapping 程序的效率. 如, Alperin-Sheriff 和 Peikert 两人在 2013 年 CRYPTO 年会上提出一个实际的拟线性 (Quasilinear) 时间的 Bootstrapping 技术. 他们的工作本质上是优化了 Gentry^[26] 等人 (SCN2012) 的 “Ring-Switching” 程序. 次年, Brakerski 和 Vaikuntanathan^[41] 利用 Branching Program 来实现同态运算, 并使 Bootstrapping 程序基于多项式近似因子的 LWE 假设, 但也导致了运行时间变大. Alperin-Sherif 和 Peikert^[42] 则给出了一种运行时间更短且错误增长更小的 Bootstrapping 程序. 随后, Halevi 和 Shoup 两人^[43] 开发了同态数据库 Helib, 并实现了 Brakerski-Gentry-Vaikuntanathan (BGV) 方案^[17], 但仅支持有限次的同态操作, 即只实现 SWHE 方案. 次年, Halevi 和 Shoup 两人^[45] 则将 Helib 扩展至支持重加密²操作, 以此来实现 Bootstrapping 程序. 同年, Ducas 和 Micciancio(DM) 两人^[44] 则给出一种基于 Regev 密文形式的 Bootstrapping 程序, 其重加密速度相比^[45] 更快, 但他们的方案仅支持处理单比特密文. 之后, Chillotti 等人^[69] 以外积 (external product) 的形式来表示 DM 方案^[44] 的密文, 由此使得 Bootstrapping 过程所需时间减少至 0.1 秒, 少于 DM 方案的 1 秒.

4.2 全同态加密的安全性研究

FHE 除了上面提到的计算效率或性能面临诸多挑战外, 其自身的安全性也广受质疑. 究其原因, 现代密码学是以可证明安全为基石, 而可证明安全是将密码体制安全的强弱根据攻击者能力不同划分为三类, 分别是较弱的选择明文攻击安全性 (CPA 安全)、非适应性选择密文攻击安全性 (CCA1 安全) 以及最强的适应性选择密文攻击下安全性 (CCA2 安全). 然而, 由于 FHE 具备密文同态运算的属性, 同态特性意味着延展性 (malleability), 因此 FHE 体制不可能抵抗适应性选择密文攻击, 即达到 CCA2 安全.

在安全性研究方面, 只要相应的 FHE 方案的加密算法是非确定性的, 那么 FHE 方案可以达到 CPA 安全. 现阶段, 大部分的工作都只给出了 CPA 的安全性证明. 2010 年, Loftus 等人^[38] 研究 Gentry 基于

²重加密是 bootstrapping 程序的重要组件, 用来刷新密文以获得噪声更小的新鲜密文.

理想格的 FHE 方案^[13](及其变体^[18])在自适应攻击下私钥的安全性。他们证明了 Gentry-Halevi 的方案^[27]不是 CCA1 安全的，并证明如果敌手能够访问解密预言机，就能确定私钥。此外，Loftus 等人给出 Smart-Vercauteren(SV) 密码系统的一个变体^[18]，在该方案中，即使敌手有一个解密预言机，私钥似乎仍旧安全。该结果是基于“有效密文”的概念，由解密算法所保证，并且其安全性依赖于一个非常强的知识假设。随后，由于构造 Smart-Vercauteren 密码系统所依赖的计算假设(即，short principal ideal problem，短主理想问题)被攻破^[70-72]，因此该方案不再被认为是安全的。在这期间若干工作在尝试构造 CCA1 安全的 FHE 方案，直到 2017 年，Cannitte 等人^[73]提出了第一个真正意义上的 CCA1 安全 FHE，但他们并没有完全解决密文长度仍然依赖于电路输入长度的问题。因此 CCA1 层级全同态加密问题仍旧没有得到完全解决。

另一方面，针对现有 FHE 方案的攻击此消彼长。利用密钥恢复攻击(key recovery attacks)方法对 FHE 的攻击就是一种最具代表性的攻击方法。具体来说，Zhang 等人^[74]利用密钥恢复攻击实现了对 Dijk 等人^[14]方案的攻击。随后，Chenal 和 Tang 两人^[75]同样利用密钥恢复攻击方法，除对 Dijk 等人^[14]方案采取更有效的攻击外，还对经典的第二代 FHE 方案(如，Brakerski 和 Vaikuntanathan 的两个方案^[15,16]，Brakerski 等人的文献[17]方案和 Brakerski 的文献[39]方案)以及第三代 Gentry 等人^[32]的 FHE 方案进行了攻击。随后，Dahab 等人^[76]则利用密钥恢复攻击方法对 Bos 等人^[53]基于 NTRU 的 FHE 方案实现了攻击。与此同时，Chenal 和 Tang 两人^[77]利用密钥恢复攻击方法对 López-Alt 等人^[52]和 Bos 等人^[53]的基于 NTRU 的 FHE 方案实现了攻击。为了阻止密钥恢复攻击，Li 等人^[78]提出一种多私钥的方法，来阻止对 GSW 方案^[32]的密钥恢复攻击。但 Stehlé^[79]则指出，该方案不能阻止利用噪声知识来对 GSW 方案的密钥恢复攻击，随后，Li 等人^[80]又提出一种对偶的多密钥 GSW 方案来阻止密钥恢复攻击。

此外，旁路攻击是另外一种对 FHE 方案安全性造成威胁的攻击方式。因此，抗泄漏(leakage resilient)的 FHE 方案应运而生。Berkoff 和 Liu 两人^[46]则针对第三代 FHE 的 GSW 方案提出一种抗泄漏的 FHE 方案，但该方案仅针对单比特加密。随后，Li 等人^[68]则利用 Hiromasa 等人^[47]的 HAO 多比特 FHE 方案，构造了一种抗泄漏的 HAO 方案，此外，同文中，Li 等人进一步优化了多比特 FHE 构造，使其可以容忍更多比特信息的泄漏。但目前，如何构造抗泄漏的第二代 FHE 方案仍是一个公开问题。

4.3 全同态加密的应用研究

以往的数据加密体制存在一个共同的问题，即数据在加密之后，若要对数据进行操作，就必须先解密，这增加了数据的不安全因素。在云存储和大数据广泛应用的今天，加密文档需求日益增长，为了便于云存储服务商对用户数据进行管理，提高系统处理和服务效率，云存储服务商必须能对用户加密数据进行诸如排序、检索等操作，显然以往传统的加密机制无法达到这一目的。

4.3.1 基于全同态加密的安全多方计算

安全多方计算(multiparty computation, MPC)从 1980 年起，就一直是当前隐私安全的研究热点问题，当前依然强势。事实上，最近研究结果表明，安全多方计算越来越接近实用，已逐渐从理论密码学的研究领域转变为应用密码学研究范畴。以两方计算为例，Alice 和 Bob 要计算一个函数 f ，首先构造一个电路 C 用于计算输入分别为 x 和 y 的函数 f ，然后执行 MPC 协议并计算 $f(x, y)$ 。这里的安全指的是 Alice 不会学习任何有关 y 的信息，Bob 也不会学习任何有关 x 的信息。传统的安全 MPC 协议通常是基于(抽象)电路来实现，如利用 RAM 计算模型，通信双方首先构造一个他们需要计算函数的电路，然后采用不同的技术手段来共同计算他们的联合输入电路。电路的规模反映了函数的计算复杂度，即相对于“复杂”的函数，通信双方需要交换大量的数据或交互大量的时间。同态加密技术是安全多方计算的核心技术之一，而使用 FHE 技术，这些限制不再存在，使得融合 FHE 技术可以设计高效的 MPC 协议。而基于 FHE 的 MPC 协议仅需很少的通信复杂度和更少的通信轮数。

现阶段，基于 FHE 来设计 MPC 协议，目前存在两种方式，一种是基于门限的 FHE(threshold-FHE)方案来设计 MPC 协议。另外一种是基于多密钥的 FHE(multikey-FHE)方案来设计 MPC 协议。

基于 Threshold-FHE 的 MPC 协议。遵循 Cramer 等人^[3]的门限同态加密方案，Asharov 等人^[81]首次提出 Threshold-FHE 的概念。他们利用 Threshold-FHE 方案，在 CRS(common reference string) 模型下，基于 LWE 假设，构造了一个抵抗半恶意(semi-malicious)敌手的 3-轮 MPC 协议，并

利用非交互零知识 (non-interactive zero-knowledge) 证明获得一个抵抗恶意 (fully-malicious) 敌手的 4-轮 MPC 协议。随后, Garg 等人^[82] 利用不可区分性混淆 (indistinguishability obfuscation, iO) 和 NIZK 构造了一个在 CRS 模型下, 抵抗静态恶意敌手的 2-轮公平 (fairness) 的 MPC 协议。Gordon 等人^[83] 指出, 在 Standalone 模型下, 2-轮公平的 MPC 协议是不可能实现的。同时, Gordon 等人实现了在 CRS 模型下 3-轮公平 MPC 协议且无需增加通信的轮次, 最后利用 Asharov 等人^[81] 的编译器, 获得一个在 CRS 模型下, 抵抗恶意敌手的 4-轮公平的 MPC 协议。下面, 我们简要概述在 CRS 模型下基于 Threshold-FHE 的 3-轮 MPC 协议。

1. 各参与方协作获得一个 FHE 方案的通用公钥 pk 。随后, 各参与方对各自的私钥 sk 进行秘密共享。
2. 各参与方利用通用公钥 pk 来加密各自的输入 x_i , 并将密文广播出去。
3. 各参与方接收到各个密文后, 本地执行并完成同态运算。各参与方利用收到的所有私钥份额来对同态运算后的密文解密, 最后, 利用拉格朗日插值多项式恢复出同态运算后的结果。

基于 Multikey-FHE 的 MPC 协议。 Lopez-Alt 等人^[52] 首次提出 Multikey-FHE 的概念, 并利用 Multikey-FHE 方案, 在 CRS (common reference string) 模型下, 基于 NTRU 的第二代 FHE 方案, 构造了一个抵抗半恶意敌手的 3-轮 MPC 协议。2016 年, Mukherjee 和 Wichs 两人^[49] 利用 Clear 和 McGoldrick 两人^[48] 所构造的 GSW 方案的 Multikey-FHE 方案, 构造了一个在 CRS 模型下, 抗半恶意敌手的 2-轮 MPC 协议。下面, 我们简要概述在 CRS 模型下基于 Multikey-FHE 的 2-轮 MPC 协议。

1. 各参与方执行密钥生成算法获得公钥 pk 和私钥 sk , 并在各自的公钥下加密各自的输入, 将获得的密文广播出去。
2. 各参与方接收到各个密文后, 本地执行并完成同态运算后, 利用各自私钥来获得部分解密结果, 之后利用所有收到的部分解密结果来获得最终的同态运算结果。

由上述描述可以发现, 基于 Mukherjee-Wichs 的 FHE 方案^[49] 仅支持单跳 (single-hop) 的同态运算。协议开始之前, 需将各参与方确定。而 Brakerski 和 Perlman 两人^[50] 则构造一种完全动态的 Multikey-FHE 方案, 允许参与方随意加入与退出协议, 同时支持多跳 (multi-hop) 的同态运算。但 Brakerski-Perlman 方案^[50] 却不能支持灵活的单跳同态运算。同年, Peikert 和 Shiehian 两人^[51] 也提出两种 MultiKey-FHE 的方案, 但该方案的密文尺寸 $O(N^2)$ 大于 Brakerski 和 Perlman 的密文尺寸 $O(N)$ 。此外, 上述 MultiKey-FHE 方案只能获得最终的运算结果, 即 $y = f(x_1, \dots, x_n)$ 。然而却不能获得对应的各自输入的运算结果, 即 $y_i = f(x_i)$ 。Dodis 等人^[84] 则利用函数秘密共享 (function secret sharing, FSS) 的方法构造了一种 Spooky 加密, 并基于该加密方案和 piO (probabilistic indistinguishability obfuscation), 设计一个 2-轮的 MPC 协议。

4.3.2 基于全同态加密的密文处理

FHE 能在很大程度上解决云计算上的数据安全问题。用户可以将加密后的数据以密态数据的形式保留在云端。除非获得加密者的私钥, 否则无人可以获得明文。但是, 用户可以对云端的密文进行有意义的操作。FHE 合理利用此类密态数据, 同时又不影响用户的隐私。此外, 利用 FHE 的各种密文处理技术也得到了进一步的发展。如私有信息检索 (private information retrieval, PIR)^[85-92], 隐私保护数据挖掘 (privacy-preserving data mining, PPDM) 和加密数据检索 (searching on encrypted data) 等方面。值得注意的是, 可搜索加密 (searchable encryption, SE) 作为加密数据检索的一种特例, 与 PIR 检索最主要区别在于, PIR 系统主要用于保护用户的查询隐私, 而加密数据检索方案则用于保护被查询文件的安全。

以下针对各方面, 分别概述具有代表性的几个工作。① 1998 年, Chor 等人^[85] 首次提出 PIR 的概念后, 各种各样的 PIR 系统及利用 PIR 保护隐私的应用被提出^[86]。2011 年, Brakerski 和 Vaikuntanathan 两人^[16] 在利用 LWE 构造第二代 FHE 的同文中, 结合 FHE 技术, 设计了首个基于 LWE 假设的 PIR 系统。随后, Yi 等人^[87] 则将 Brakerski 和 Vaikuntanathan 两人的结果推广至整数上, 并设计了基于整数 FHE 的单一服务器 PIR 系统。在 2014 年同态密码及加密计算的研讨会上,³ Sunar 等人^[88] 则利用

³Workshop on Applied Homomorphic Cryptography and Encrypted Computing, WAHC

基于 NTRU 的 FHE 方案^[52] 设计了一个高效的 PIR 系统。次年, Dai 等人^[89] 则利用 GPU⁴ 来优化 Sunar 等人^[88] 的 PIR 系统。而 Li 等人^[92] 则将 Brakerski 和 Vaikuntanathan 两人的结果推广至更高效的多比特检索的 PIR 系统。^② 在加密数据检索方面, Boneh 等人^[93] 则利用 SWHE 方案⁵ 来检索加密数据。解决了数据检索只能处理析取 (disjunction) 查询而无法处理合取 (conjunction) 查询的问题, 但该方案只允许对密态数据的检索。Cheon 等人^[94] 利用 Brakerski 等人^[17] 的 FHE 方案, 提出一种密文处理框架, 不但可以检索密态数据, 同时也可以同态计算密态数据。随后, Cheon 等人^[95] 进一步优化了该框架。^③ 对于隐私保护数据挖掘方面, 特别是在基因序列分析的同时保护用户的隐私是一个重要的研究课题^[96]。Cheon 等人^[97] 考虑到基因序列分析中潜在的隐私泄露风险问题, 利用 DGHV 整数 FHE 方案^[14], 实现对加密基因数据的编辑距离 (edit distance) 的同态运算。此外, Kim 和 Lauter 两人^[98] 则分别利用基于 LWE 的 BGV-FHE 方案^[17] 和基于 NTRU 的 YASHE 方案^[53], 实现了加密基因数据的安全外包和计算比较。此外, 微软的研究人员, Dowlin 等人^[99] 则利用神经网络来实现对密态数据的分析。

随着当前 FHE 技术的发展, 结合 FHE 技术, 若干隐私保护及密文处理技术得到进一步的发展。如不经意随机存取 (oblivious random access memo, ORAM) 技术^[100–104], 委托计算 (delegate computation)^[105], 混淆 (obfuscation)^[106–108] 等等。

4.3.3 结合全同态加密的其他密码学原语

随着 Gentry 等人的第三代 FHE 方案的提出^[32], 各种各样的密码学原语通过使用 FHE 作为基础密码学组件来丰富其自身的功能。譬如, 基于身份的加密 (identity-based encryption, IBE)^[109–112], 基于属性的加密 (attribution-based encryption)^[113–116], 函数加密 (functional encryption)^[117], 水印密码学 (watermarking cryptographic)^[118–120], 某一类的混淆 (obfuscation)^[121–125] 以及各类伪随机函数 (pseudorandom function)^[126–130] 等等。结合 FHE 技术, 丰富各类密码学原语的功能是当前密码学领域的前沿课题。但均超出本文讨论的范畴, 故不再过多赘述。

5 总结

由于量子计算机的发展, 可抗量子攻击的格密码体制成为后量子密码研究中最核心的研究领域, 其与生俱来的同态运算特性, 对于设计基于格的全同态加密体制具有得天独厚的优势。自 2009 年, Gentry 在基于理想格的全同态加密体制构造方面取得突破性进展后, 过去几年来该领域受到学界及业界的广泛关注并取得了丰富的研究成果。因此, 本文从全同态加密所经历的三个阶段, 基于格的第三代全同态加密体制 (GSW 方案) 设计和全同态加密面临的问题及发展趋势等方面, 着重对基于格的全同态加密技术进行了较为详细的总结。全同态加密的研究是一项复杂的系统工程, 交叉着复杂的数学问题, 密码问题和工程实践问题, 且其自身的理论和高效实用的构造还待于进一步完善与发展。同时, 全同态加密在密文检索, 隐私保护数据挖掘以及加密数据处理等方面的广泛应用前景已逐步得到证实。此外, 利用全同态加密作为一个密码学组件来设计其他的密码学原语, 具有很大的理论价值和实际意义。

References

- [1] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169–180.
- [2] BRICKELL E F. On privacy homomorphism[C]. In: Advances in Cryptology—EUROCRYPT 1987. Springer Berlin Heidelberg, 1988: 117–125.
- [3] CRAMER R, DAMGÅRD I, NIELSEN J. Multiparty computation from threshold homomorphic encryption[C]. In: Advances in Cryptology—EUROCRYPT 2001. Springer Berlin Heidelberg, 2001: 280–300.
- [4] DAMGÅRD I, NIELSEN J. Universally composable efficient multiparty computation from threshold homomorphic encryption[C]. In: Advances in Cryptology—CRYPTO 2003. Springer Berlin Heidelberg, 2003: 247–264.
- [5] GOLDWASSER S, MICALI S. Probabilistic encryption[J]. Journal of Computer and System Sciences, 1984, 28(2): 270–299.
- [6] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[C]. In: Advances in Cryptology—CRYPTO 1984. Springer Berlin Heidelberg, 1985: 10–18.

⁴Graphics Processing Units

⁵实质为 Paillier 加法同态方案。

- [7] OKAMOTO T, UCHIYAMA S. A new public-key cryptosystem as secure as factoring[C]. In: Advances in Cryptology—EUROCRYPT 1998. Springer Berlin Heidelberg, 1998: 308–318.
- [8] NACCACHE D, STERN J. A new public key cryptosystem based on higher residues[C]. In: Proceedings of the 5th ACM Conference on Computer and Communications Security. ACM, 1998: 59–66.
- [9] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. In: Advances in Cryptology—EUROCRYPT 1999. Springer Berlin Heidelberg, 1999: 223–238.
- [10] DAMGARD I, JURIK M. A generalisation, a simplification and some applications of Paillier’s probabilistic public-key system[C]. In: Public Key Cryptography—PKC 2001. Springer Berlin Heidelberg, 2001: 119–136.
- [11] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[C]. In: Theory of Cryptography Conference—TCC 2005. Springer Berlin Heidelberg, 2005: 325–341.
- [12] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120–126.
- [13] GENTRY C. Fully homomorphic encryption using ideal lattices[C]. In: Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing—STOC 2009. ACM, 2009: 169–169.
- [14] VAN DIJK M, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers[C]. In: Advances in Cryptology—EUROCRYPT 2010. Springer Berlin Heidelberg, 2010: 24–43.
- [15] BRAKERSKI Z, VAIKUNTANATHAN V. Fully homomorphic encryption from ring-LWE and security for key dependent messages[C]. In: Advances in Cryptology—CRYPTO 2011. Springer Berlin Heidelberg, 2011: 505–524.
- [16] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[C]. In: IEEE 52nd Annual Symposium on Foundations of Computer Science—FOCS 2011. IEEE, 2011: 97–106.
- [17] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping[C]. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. ACM, 2012: 309–325.
- [18] SMART N P, VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[C]. In: Public Key Cryptography—PKC 2010. Springer Berlin Heidelberg, 2010: 420–443.
- [19] STEHLÉ D, STEINFELD R. Faster fully homomorphic encryption[C]. In: Advances in Cryptology—ASIACRYPT 2010. Springer Berlin Heidelberg, 2010: 377–394.
- [20] CHEN Y, NGUYEN P Q. Faster algorithms for approximate common divisors: breaking fully-homomorphic-encryption challenges over the integers[C]. In: Advances in Cryptology—EUROCRYPT, 2012. Springer Berlin Heidelberg, 2012: 502–519.
- [21] CORON J S, MANDAL A, NACCACHE D, et al. Fully homomorphic encryption over the integers with shorter public keys[C]. In: Advances in Cryptology—CRYPTO, 2011. Springer Berlin Heidelberg, 2012: 487–504.
- [22] CORON J S, NACCACHE D, TIBOUCHI M. Public key compression and modulus switching for fully homomorphic encryption over the integers[C]. In: Advances in Cryptology—EUROCRYPT, 2012. Springer Berlin Heidelberg, 2012: 446–464.
- [23] CHEON J H, CORON J S, KIM J, et al. Batch fully homomorphic encryption over the integers[C]. In: Advances in Cryptology—EUROCRYPT 2013. Springer Berlin Heidelberg, 2013: 315–335.
- [24] FAN J, VERCAUTEREN F. Somewhat practical fully homomorphic encryption[J]. IACR Cryptology ePrint Archive, 2012, 2012: 144.
- [25] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM (JACM), 2013, 60(6): 43.
- [26] GENTRY C, HALEVI S, PEIKERT C, et al. Ring switching in BGV-style homomorphic encryption[C]. In: Security and Cryptography for Networks—SCN 2012. Springer Berlin Heidelberg, 2012: 19–37.
- [27] GENTRY C, HALEVI S. Implementing Gentry’s fully-homomorphic encryption scheme[C]. In: Advances in Cryptology—EUROCRYPT 2011. Springer Berlin Heidelberg, 2011: 129–148.
- [28] GENTRY C, HALEVI S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits[C]. In: IEEE 52nd Annual Symposium on Foundations of Computer Science—FOCS, 2011. IEEE, 2011: 107–109.
- [29] GENTRY C, HALEVI S, SMART N P. Better bootstrapping in fully homomorphic encryption[C]. In: Public Key Cryptography—PKC. Springer Berlin Heidelberg, 2012: 1–16.
- [30] GENTRY C, HALEVI S, SMART N P. Fully homomorphic encryption with polylog overhead[C]. In: Advances in Cryptology—EUROCRYPT. Springer Berlin Heidelberg, 2012: 465–482.
- [31] BRAKERSKI Z, GENTRY C, HALEVI S. Packed ciphertexts in LWE-based homomorphic encryption[C]. In: Public Key Cryptography—PKC, 2013. Springer Berlin Heidelberg, 2013: 1–13.
- [32] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]. In: Advances in Cryptology—CRYPTO 2013. Springer Berlin Heidelberg, 2013: 1–13.

- berg, 2013: 75–92.
- [33] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing. ACM, 2005: 84–93.
 - [34] HOWGRAVE-GRAHAM N. Approximate Integer Common Divisors[C]. In: International Conference on Cryptography and Lattices. Springer Berlin Heidelberg, 2001: 51–66.
 - [35] CORON J S, LEPOINT T, TIBOUCHI M. Scale-invariant fully homomorphic encryption over the integers[C]. In: Public Key Cryptography—PKC 2014. Springer Berlin Heidelberg, 2014: 311–328.
 - [36] NUIDA K, KUROSAWA K. (Batch) fully homomorphic encryption over integers for non-binary message spaces[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 537–555.
 - [37] BENARROCH D, BRAKERSKI Z, LEPOINT T. FHE over the integers: Decomposed and batched in the post-quantum regime[C]. In: Public Key Cryptography—PKC 2017. Springer Berlin Heidelberg, 2017: 271–301.
 - [38] LOFTUS J, MAY A, SMART N P, et al. On CCA-secure somewhat homomorphic encryption[C]. In: Selected Areas in Cryptography—SAC 2011. Springer Berlin Heidelberg, 2011: 55–72.
 - [39] BRAKERSKI Z. Fully homomorphic encryption without modulus switching from classical GapSVP[C]. In: Advances in Cryptology—CRYPTO 2012. Springer Berlin Heidelberg, 2012: 868–886.
 - [40] ALPERIN-SHERIFF J, PEIKERT C. Practical bootstrapping in quasilinear time[C]. In: Advances in Cryptology—CRYPTO 2013. Springer Berlin Heidelberg, 2013: 1–20.
 - [41] BRAKERSKI Z, VAIKUNTANATHAN V. Lattice-based FHE as secure as PKE[C]. In: Proceedings of the 5th Conference on Innovations in Theoretical Computer Science. ACM, 2014: 1–12.
 - [42] ALPERIN-SHERIFF J, PEIKERT C. Faster bootstrapping with polynomial error[C]. In: Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2014: 297–314.
 - [43] HALEVI S, SHOUP V. Algorithms in HElib[C]. In: Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2014: 554–571.
 - [44] DUCAS L, MICCIANCIO D. FHEW: Bootstrapping homomorphic encryption in less than a second[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 617–640.
 - [45] HALEVI S, SHOUP V. Bootstrapping for HElib[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 641–670.
 - [46] BERKOFF A, LIU F H. Leakage resilient fully homomorphic encryption[C]. In: Theory of Cryptography Conference—TCC 2014. Springer Berlin Heidelberg, 2014: 515–539.
 - [47] HIROMASA R, ABE M, OKAMOTO T. Packing messages and optimizing bootstrapping in GSW-FHE[C]. In: Public Key Cryptography—PKC 2015. Springer Berlin Heidelberg, 2015: 699–715.
 - [48] CLEAR M, MCGOLDRICK C. Multi-identity and multi-key leveled FHE from learning with errors[C]. In: Advances in Cryptology—CRYPTO 2015. Springer Berlin Heidelberg, 2015: 630–656.
 - [49] MUKHERJEE P, WICHES D. Two round multiparty computation via multi-key FHE[C]. In: Advances in Cryptology—EUROCRYPT 2016. Springer Berlin Heidelberg, 2016: 735–763.
 - [50] BRAKERSKI Z, PERLMAN R. Lattice-based fully dynamic multi-key FHE with short ciphertexts[C]. In: Advances in Cryptology—CRYPTO 2016. Springer Berlin Heidelberg, 2016: 190–213.
 - [51] PEIKERT C, SHIEHIAN S. Multi-key FHE from LWE, revisited[C]. In: Theory of Cryptography Conference—TCC 2016. Springer Berlin Heidelberg, 2016: 217–238.
 - [52] LÓPEZ-ALT A, TROMER E, VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]. In: Proceedings of the 44th Annual ACM Symposium on Theory of Computing. ACM, 2012: 1219–1234.
 - [53] BOS J W, LAUTER K E, LOFTUS J, et al. Improved security for a ring-based fully homomorphic encryption scheme[C]. In: 14th IMA International Conference on Cryptography and Coding 2013. Springer Berlin Heidelberg, 2013: 45–64.
 - [54] BOS J W, LAUTER K, NAEHRIG M. Private predictive analysis on encrypted medical data[J]. Journal of Biomedical Informatics, 2014, 50: 234–243.
 - [55] LAUTER K, LÓPEZ-ALT A, NAEHRIG M. Private computation on encrypted genomic data[C]. In: International Conference on Cryptology and Information Security in Latin America. Springer Berlin Heidelberg, 2014: 3–27.
 - [56] CHONGCHITMATE W, OSTROVSKY R. Circuit-private multi-key FHE[C]. In: IACR International Workshop on Public Key Cryptography—PKC 2017. Springer Berlin Heidelberg, 2017: 241–270.
 - [57] LI Z, MA C, DU G, et al. Dual LWE-based fully homomorphic encryption with errorless key switching[C]. In: 2016 IEEE 22nd International Conference on Parallel and Distributed Systems—ICPADS. IEEE, 2016: 1169–1174.
 - [58] BARRINGTON D A. Bounded-width polynomial-size branching programs recognize exactly those languages in

- NC^1 [J]. Journal of Computer and System Sciences, 1989, 38(1): 150–164.
- [59] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: Simpler, tighter, faster, smaller[C]. In: Advances in Cryptology—EUROCRYPT 2012. Springer Berlin Heidelberg, 2012: 700–718.
- [60] WANG X Y, LIU M J. Survey of lattice-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 13–27.
王小云, 刘明洁. 格密码学研究 [J]. 密码学报, 2014, 1(1): 13–27.
- [61] LENSTRA A K, LENSTRA H W, LOVÁSZ L. Factoring polynomials with rational coefficients[J]. Mathematische Annalen, 1982, 261(4): 515–534.
- [62] AJTAI M, DWORCK C. A public-key cryptosystem with worst-case/average-case equivalence[C]. In: Proceedings of the 29th Annual ACM Symposium on Theory of Computing—STOC 1997. ACM, 1997: 284–293.
- [63] PEIKERT C. Public-key cryptosystems from the worst-case shortest vector problem[C]. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing—STOC. ACM, 2009: 333–342.
- [64] SMART N P, VERCAUTEREN F. Fully homomorphic SIMD operations[J]. Designs, Codes and Cryptography, 2014, 1(71): 57–81.
- [65] PEIKERT C, VAIKUNTANATHAN V, WATERS B. A framework for efficient and composable oblivious transfer[C]. In: Advances in Cryptology—CRYPTO 2008. Springer Berlin Heidelberg, 2008: 554–571.
- [66] LI Z P, MA C G, MORAIS E, et al. Multi-bit leveled homomorphic encryption via dual-LWE-based[C]. In: Information Security and Cryptology—INSCRYPT 2016. Springer Berlin Heidelberg, 2017: 221–242.
- [67] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing—STOC 2008. ACM, 2008: 197–206.
- [68] LIN Y R, TONG H, TANG J, et al. Guest editorial: Big scholar data discovery and collaboration[J]. IEEE Transactions on Big Data, 2017, 3(1): 1–2.
- [69] CHILLOTTI I, GAMA N, GEORGIEVA M, et al. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds[C]. In: Advances in Cryptology—ASIACRYPT 2016. Springer Berlin Heidelberg, 2016: 3–33.
- [70] BIASSE J F, FIEKER C. Subexponential class group and unit group computation in large degree number fields[J]. LMS Journal of Computation and Mathematics, 2014, 17(A): 385–403.
- [71] BIASSE J F, SONG F. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields[C]. In: Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms. ACM, 2016: 893–902.
- [72] CRAMER R, DUCAS L, PEIKERT C, et al. Recovering short generators of principal ideals in cyclotomic rings[C]. In: Advances in Cryptology—EUROCRYPT 2016. Springer Berlin Heidelberg, 2016: 559–585.
- [73] CANETTI R, RAGHURAMAN S, RICHELSON S, et al. Chosen-ciphertext secure fully homomorphic encryption[C]. In: Public Key Cryptography—PKC 2017. Springer Berlin Heidelberg, 2017: 213–240.
- [74] ZHANG Z, PLANTARD T, SUSILO W. On the CCA-1 security of somewhat homomorphic encryption over the integers[C]. In: International Conference on Information Security Practice and Experience—ISPEC 2012. Springer Berlin Heidelberg, 2012: 353–368.
- [75] CHENAL M, TANG Q. On key recovery attacks against existing somewhat homomorphic encryption schemes[C]. In: International Conference on Cryptology and Information Security in Latin America 2014. Springer Berlin Heidelberg, 2014: 239–258.
- [76] DAHAB R, GALBRAITH S, MORAIS E. Adaptive key recovery attacks on NTRU-based somewhat homomorphic encryption schemes[C]. In: 8th International Conference on Information Theoretic Security—ICITS 2015. Springer Berlin Heidelberg, 2015: 283–296.
- [77] CHENAL M, TANG Q. Key recovery attacks against NTRU-based somewhat homomorphic encryption schemes[C]. In: International Information Security Conference. Springer Berlin Heidelberg, 2015: 397–418.
- [78] LI Z P, GALBRAITH S D, MA C G. Preventing adaptive key recovery attacks on the GSW levelled homomorphic encryption scheme[C]. In: International Conference on Provable Security. Springer International Publishing, 2016: 373–383.
- [79] Damien Stehlé and Steven Galbraith. Personal communications. September, 2016.
- [80] LI Z, GALBRAITH S D, MA C. Preventing adaptive key recovery attacks on the GSW levelled homomorphic encryption scheme[J]. IACR Cryptology ePrint Archive, 2016, 2016: 1146.
- [81] ASHAROV G, JAIN A, LÓPEZ-ALT A, et al. Multiparty computation with low communication, computation and interaction via threshold FHE[C]. In: Advances in Cryptology—EUROCRYPT 2012, 2012: 483–501.
- [82] GARG S, GENTRY C, HALEVI S, et al. Two-round secure MPC from indistinguishability obfuscation[C]. In: Theory of Cryptography Conference—TCC 2014. Springer Berlin Heidelberg, 2014: 74–94.

- [83] GORDON S D, LIU F H, SHI E. Constant-round MPC with fairness and guarantee of output delivery[C]. In: Advances in Cryptology—CRYPTO 2015. Springer Berlin Heidelberg, 2015: 63–82.
- [84] DODIS Y, HALEVI S, ROTHBLUM R D, et al. Spooky encryption and its applications[C]. In: Advances in Cryptology—CRYPTO 2016. Springer Berlin Heidelberg, 2016: 93–122.
- [85] CHOR B, GOLDREICH O, KUSHILEVITZ E, et al. Private information retrieval[C]. In: 36th Annual Symposium on Foundations of Computer Science—FOCS 1995. IEEE, 1995: 41–50.
- [86] GERTNER Y, ISHAI Y, KUSHILEVITZ E, et al. Protecting data privacy in private information retrieval schemes[J]. Journal of Computer and System Sciences, 2000, 60(3): 592–629.
- [87] YI X, KAOSAR M G, PAULET R, et al. Single-database private information retrieval from fully homomorphic encryption[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(5): 1125–1134.
- [88] DORÖZ Y, SUNAR B, HAMMOURI G. Bandwidth efficient PIR from NTRU[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014: 195–207.
- [89] DAI W, DORÖZ Y, SUNAR B. Accelerating SWHE based PIRs using GPUS[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015: 160–171.
- [90] LEPOINT T, TIBOUCHI M. Cryptanalysis of a (somewhat) additively homomorphic encryption scheme used in PIR[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015: 184–193.
- [91] KHEDR A, GULAK G, VAIKUNTANATHAN V. SHIELD: Scalable homomorphic implementation of encrypted data-classifiers[J]. IEEE Transactions on Computers, 2016, 65(9): 2848–2858.
- [92] LI Z P, MA C G, WANG D, et al. Toward single-server private information retrieval protocol via learning with errors[J]. Journal of Information Security and Applications, 2017, 34: 280–284.
- [93] BONEH D, GENTRY C, HALEVI S, et al. Private database queries using somewhat homomorphic encryption[C]. In: International Conference on Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2013: 102–118.
- [94] CHEON J H, KIM M, KIM M. Search-and-compute on encrypted data[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015: 142–159.
- [95] CHEON J H, KIM M, KIM M. Optimized search-and-compute circuits and their application to query evaluation on encrypted data[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(1): 188–199.
- [96] DOWLIN N, RAN G B, LAINE K, et al. Manual for using homomorphic encryption for bioinformatics[R]. Technical Report, November 2015.
- [97] CHEON J H, KIM M, LAUTER K. Homomorphic computation of edit distance[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015: 194–212.
- [98] KIM M, LAUTER K. Private genome analysis through homomorphic encryption[J]. BMC Medical Informatics and Decision Making, 2015, 15(5): S3.
- [99] GILAD-BACHRACH R, DOWLIN N, LAINE K, et al. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy[C]. In: International Conference on Machine Learning. 2016: 201–210.
- [100] GOLDREICH O, OSTROVSKY R. Software protection and simulation on oblivious RAMs[J]. Journal of the ACM (JACM), 1996, 43(3): 431–473.
- [101] GENTRY C, GOLDMAN K A, HALEVI S, et al. Optimizing ORAM and using it efficiently for secure computation[C]. In: International Symposium on Privacy Enhancing Technologies Symposium. Springer Berlin Heidelberg, 2013: 1–18.
- [102] GENTRY C, HALEVI S, RAYKOVA M, et al. Outsourcing private RAM computation[C]. In: 2014 IEEE 55th Annual Symposium on Foundations of Computer Science—FOCS 2014. IEEE, 2014: 404–413.
- [103] GENTRY C, HALEVI S, JUTLA C, et al. Private database access with he-over-oram architecture[C]. In: International Conference on Applied Cryptography and Network Security—ACNS 2015. Springer Berlin Heidelberg, 2015: 172–191.
- [104] DEVADAS S, VAN DIJK M, FLETCHER C W, et al. Onion ORAM: A constant bandwidth blowup oblivious RAM[C]. In: Theory of Cryptography Conference—TCC 2016. Springer Berlin Heidelberg, 2016: 145–174.
- [105] CHUNG K M, KALAI Y T, VADHAN S P. Improved delegation of computation using fully homomorphic encryption[C]. In: Advances in Cryptology—CRYPTO 2010. Springer Berlin Heidelberg, 2010: 483–501.
- [106] BARAK B, GOLDREICH O, IMPAGLIAZZO R, et al. On the (im)possibility of obfuscating programs[C]. In: Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001: 1–18.
- [107] GARG S, GENTRY C, HALEVI S, et al. On the implausibility of differing-inputs obfuscation and extractable witness encryption with auxiliary input[C]. Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2014: 518–535.

- [108] GENTRY C, LEWKO A B, SAHAI A, et al. Indistinguishability obfuscation from the multilinear subgroup elimination assumption[C]. In: 2015 IEEE 56th Annual Symposium on Foundations of Computer Science—FOCS 2015. IEEE, 2015: 151–170.
- [109] YAMADA S. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters[C]. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2016: 32–62.
- [110] KATSUMATA S, YAMADA S. Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps[C]. In: Advances in Cryptology—ASIACRYPT 2016. Springer Berlin Heidelberg, 2016: 682–712.
- [111] BOYEN X, LI Q Y. Towards tightly secure lattice short signature and id-based encryption[C]. In: Advances in Cryptology—ASIACRYPT 2016. Springer Berlin Heidelberg, 2016: 404–434.
- [112] YAMADA S. Asymptotically compact adaptively secure lattice ibes and verifiable random functions via generalized partitioning techniques[J]. IACR Cryptology ePrint Archive, 2017, 2017: 96.
- [113] BONEH D, GENTRY C, GORBUNOV S, et al. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits[C]. In: Advances in Cryptology—EUROCRYPT 2014. Springer Berlin Heidelberg, 2014: 533–556.
- [114] GORBUNOV S, VINAYAGAMURTHY D. Riding on asymmetry: Efficient ABE for branching programs[C]. In: Advances in Cryptology—ASIACRYPT 2015. Springer Berlin Heidelberg, 2015: 550–574.
- [115] BRAKERSKI Z, VAIKUNTANATHAN V. Circuit-ABE from LWE: Unbounded attributes and semi-adaptive security[C]. In: Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2016: 363–384.
- [116] BRAKERSKI Z, CASH D, TSABARY R, et al. Targeted homomorphic attribute-based encryption[C]. In: Theory of Cryptography Conference—TCC 2016. Springer Berlin Heidelberg, 2016: 330–360.
- [117] APON D, FAN X, LIU F H. Deniable attribute based encryption for branching programs from LWE[C]. In: Theory of Cryptography Conference—TCC 2016. Springer Berlin Heidelberg, 2016: 299–329.
- [118] NISHIMAKI R. How to watermark cryptographic functions[C]. In: Advances in Cryptology—EUROCRYPT 2013. Springer Berlin Heidelberg, 2013: 111–125.
- [119] COHEN A, HOLMGREN J, NISHIMAKI R, et al. Watermarking cryptographic capabilities[C]. In: Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing—STOC 2016. ACM, 2016: 1115–1127.
- [120] KIM S, WU D J. Watermarking cryptographic functionalities from standard lattice assumptions[J]. IACR Cryptology ePrint Archive, 2017, 2017: 380.
- [121] CANETTI R, LIN H, TESSARO S, et al. Obfuscation of probabilistic circuits and applications[C]. In: Theory of Cryptography Conference—TCC 2015. Springer Berlin Heidelberg, 2015: 468–497.
- [122] BRAKERSKI Z, VAIKUNTANATHAN V, WEE H, et al. Obfuscating conjunctions under entropic ring LWE[C]. In: Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science—ITCS 2016. ACM, 2016: 147–156.
- [123] GOYAL R, KOPPULA V, WATERS B. Separating semantic and circular security for symmetric-key bit encryption from the learning with errors assumption[C]. In: Advances in Cryptology—EUROCRYPT. Springer Cham, 2017: 528–557.
- [124] GOYAL R, KOPPULA V, WATERS B. Lockable obfuscation[J]. IACR Cryptology ePrint Archive, 2017, 2017: 274.
- [125] WICHES D, ZIRDELIS G. Obfuscating compute-and-compare programs under LWE[J]. IACR Cryptology ePrint Archive, 2017, 2017: 276.
- [126] BRAKERSKI Z, VAIKUNTANATHAN V. Constrained key-homomorphic PRFs from standard lattice assumptions[C]. In: Theory of Cryptography Conference—TCC 2015. Springer Berlin Heidelberg, 2015: 1–30.
- [127] HOHENBERGER S, KOPPULA V, WATERS B. Adaptively secure puncturable pseudorandom functions in the standard model[C]. In: Advances in Cryptology—ASIACRYPT 2015. Springer Berlin Heidelberg, 2015: 79–102.
- [128] BONEH D, LEWI K, WU D J. Constraining pseudorandom functions privately[C]. In: IACR International Workshop on Public Key Cryptography—PKC 2017. Springer Berlin Heidelberg, 2017: 494–524.
- [129] CANETTI R, CHEN Y. Constraint-hiding constrained PRFs for NC^1 from LWE[C]. In: Advances in Cryptology—EUROCRYPT 2017. Springer Cham, 2017: 446–476.
- [130] BONEH D, KIM S, MONTGOMERY H. Private puncturable PRFs from standard lattice assumptions[C]. In: Advances in Cryptology—EUROCRYPT 2017. Springer Cham, 2017: 415–445.

作者信息



李增鹏(1989-), 山东青岛人,
博士生在读. 主要研究领域为
格公钥密码学和安全协议.
E-mail: lizengpeng@
hrbeu.edu.cn



马春光(1974-), 黑龙江双鸭山
人, 教授. 主要研究领域为公钥
密码学和隐私保护.
E-mail: machunguang@
hrbeu.edu.cn



周红生(1976-), 副研究员. 主
要研究领域为公钥密码学和安
全协议.
E-mail: hszhou@vcu.edu