第 3 卷◆第 3 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

浅析同态加密技术发展及应用

金世皓
厦门大学马来西亚分校
DOI:10.12238/acair.v3i3.15582

[摘　要] 随着数据安全和用户隐私泄露事件频发,同态加密技术的重要性日益凸显。本文追溯了同态加密技术的发展历程,阐释了其中的基本原理和技术特点,综述了最新研究进展,介绍了该技术在多个领域中的典型应用,并分析了应用中面临的主要挑战及应对策略。本文对同态加密技术的深入研究和实践应用具有一定的参考价值。
[关键词] 同态加密；数据安全；隐私保护；云计算
中图分类号：G623.58　文献标识码：A

A Brief Analysis of the Development and Application of Homomorphic Encryption Technology

Shihao Jin
Xiamen University Malaysia

[Abstract] With the frequent occurrence of data security and user privacy breaches, the importance of homomorphic encryption technology is becoming increasingly prominent. This article traces the development history of homomorphic encryption technology, explains its basic principles and technical characteristics, summarizes the latest research progress, introduces the typical applications of this technology in multiple fields, and analyzes the challenges and countermeasures faced in the process of technology application. This article has certain reference value for in-depth research and practical application of homomorphic encryption technology.
[Key words] homomorphic encryption; Data security; Privacy protection; Cloud Computing

引言

随着云计算和大数据的迅猛发展和广泛应用,数据安全和用户隐私保护问题日益凸显。在云端存储和处理数据的过程中,确保数据的机密性、完整性和可用性至关重要。同态加密作为一种前沿加密技术,支持在不解密的情况下直接对密文执行计算,具备“数据可算不可见”的独特优势,为数据应用过程的数据安全与隐私保护提供了有效保障[1]。因此深入研究同态加密技术,对解决当今社会面临的数据安全和隐私保护挑战具有重要意义。

1 同态加密技术概述

1.1同态加密技术发展历程

同态加密技术自20世纪70年代起发展至今,其演进过程可以分为四个阶段,各阶段均体现了理论突破和实践应用的深度融合：

1.1.1前期探索阶段(1978-2005)

1978年,Rivest等三位学者首次提出了隐私同态加密的概念,突破了传统加密技术的功能限制,引发了学术界的关注与可计算加密机制研究的初步探索。在此后二十余年间,具有部分同态特性的算法体系逐步建立：1985年提出的ElGamal公钥加密算法；1999年Paillier提出了基于复合剩余类问题的加法同态加密算法；2005年提出了Boneh-Goh-Nissim方案[1]。

1.1.2理论突破阶段(2009)

2009年Craig Gentry首次构建了第一个全同态加密方案,这是同态加密领域的一个重要里程碑[2],该方案基于数学概念——理想格,支持在加密数据上执行任意次数的加乘计算,从此开启了全同态加密研究的新篇章。

1.1.3工程优化与算法迭代阶段(2011-2016)

随着bootstrapping技术(2011)与BGV方案的AES电路实现(2012)等工程突破,同态加密开始走向实际应用。在此期间,具有代际特征的多类方案相继涌现：以BGV/BFV方案为代表的第二代FHE着重优化多项式环上的模约简运算；基于近似数算术的CKKS方案(2017)和GSW方案组成的第三代FHE,则拓展了浮点数运算与容错计算能力[2]。技术生态层面,IBM推出的HElib开源库通过密文打包等技术大幅提升了BGV方案的工程可行性。

1.1.4标准化推进阶段(2017-至今)

2017年HomomorphicEncryption.org联盟的成立标志着技术发展进入规范制定期。该组织发布的安全标准、API标准和应用白皮书,为算法实现、参数选取及行业应用建立了系统化框

架。参与标准制定的成员单位已经涵盖Microsoft、Intel等科技企业以及麻省理工、斯坦福等知名学府,这种产学研协同机制有效推进了技术标准与产业需求的精准对接。

综上所述,同态加密经历了四代演进发展,已经从纯粹理论模型发展成为具有实用价值的密码学研究分支。当前研究热点正朝着安全性增强、硬件加速架构设计、多维数据协同计算等方向持续发展。

1.2同态加密技术基本原理

同态加密作为一种特殊的加密方法,其核心特性在于支持对加密数据执行特定计算,且所得计算结果与对明文执行相同运算的结果一致。下面以经典的同态加密Paillier算法[3]为例,阐述其密钥生成、加密、解密、同态运算过程。

1.2.1密钥生成

首先选择两个大素数 p 和 q，$\gcd(pq,(p-1)(q-1))=1$ 且满足 p，q 长度相等。$\gcd$ 为最大公约数；

计算 $n=pq$ 和 $\lambda=\mathrm{lcm}(p-1,q-1)$，$\mathrm{lcm}$ 为最小公倍数；

定义 $L(x)=\dfrac{x-1}{n}$；$L(x)$ 为一个函数；

然后选择一个随机数 g 满足 $g<n*n$,

$$u=(L(g^{\lambda} \bmod n^2))^{-1} \bmod n$$

最后生成公钥 (n,g) 和私钥（λ，u）。

1.2.2加密过程

给定明文 m 和公钥 (n,g)，加密过程选择一个随机数 r，满足0<r<n和0<r<n,计算密文

$$c=g^m r^n \bmod n^2$$

1.2.3解密过程

给定密文c和私钥（λ，u),解密过程计算

$$m=L(c^{\lambda} \bmod n^2)*u$$

1.2.4同态运算

Paillier算法具有加法同态性,即Paillier加密的两个密文消息相乘的结果解密后得到两个消息相加的结果。

对于两个密文 $c_1=g^{m1}\bullet r_1{}^n \bmod n^2$ 和

$$c_2=g^{m2}\bullet r_2{}^n \bmod n^2$$

$$c_1*c_2=g^{m1}\bullet g^{m2}\bullet r_1^n\bullet r_2^n \bmod n^2$$

$$c_1*c_2=g^{(m1+m2)}\bullet(r_1\bullet r_2)^n \bmod n^2$$

所以 c_1*c_2 可以看作是 $m=m1+m2$ 加密的密文，c_1*c_2 的解密结果为 m 。

1.3同态加密方式分类

同态加密技术可依据计算能力、代数构造和目标函数三个维度进行系统性分类。

(1)按照同态加密的计算能力分类,可以分为完全同态加密、部分同态加密及近似同态加密三种类型[4]。①完全同态加密是指在数据不解密的情况下,可以对其进行任意的加法、乘法计算操作;②部分同态加密则是指仅支持特定类型的计算操作,效率极高；③近似同态加密支持对数据进行有限乘法和加法计算操作,通过重缩放恢复出可接受误差范围内的近似结果。

(2)按照代数结构分类,同态加密方式包括基于理想格的同态加密、基于编码的同态加密、基于整数的同态加密[4]。①理想格基方案：基于环LWE问题,安全性依赖格难题；②整数环基方案：基于近似最大公约数问题,运算简洁；③编码基方案：基于纠错码LWE问题,具有量子抗性潜力。

(3)按目标函数类型分类,同态加密方式包括多项式同态加密、矩阵同态加密、布尔同态加密；①多项式同态加密专注于高效计算多项式函数；②矩阵同态加密常用于优化矩阵运算；③布尔同态加密常用于优化布尔电路计算[6]。

1.4同态加密的技术特点

同态加密具备以下几个核心技术特点与约束：

(1)数据可算不可见。同态加密技术的核心优势在于支持对加密数据进行直接计算,全过程无需解密,从根本上避免了服务端或第三方平台的数据泄漏风险。这种特性使得在云计算环境中,用户能够在保护数据隐私的前提下进行安全的数据处理和分析。

(2)化解数据共享与隐私矛盾。同态加密技术支持在密文上执行计算操作。通过“数据不动模型动,模型不动数据动”的隐私计算方式,能够有效化解跨域数据共享与隐私保护之间的矛盾,消除“信息孤岛”。

(3)强化安全性保障。同态加密技术基于严格的数学证明,具有抵御已知攻击手段的能力。为金融服务、医疗保健等高敏感领域中的数据安全处理与传输应用提供了可靠支撑[3]。

(4)效率与性能局限。当前的全同态加密存在显著性能瓶颈,乘法运算开销巨大,远超明文计算,难以满足实时交互需求；而且密钥体积庞大,达到GB量级,且密文体量随计算复杂度呈指数增长,导致密文传输延迟过高。这些因素限制了全同态加密技术的应用场景范围。

2 同态加密技术的最新进展

近年来涌现了一系列创新同态加密方案,在计算效率上取

得了显著提升,在密钥管理和安全性上取得了一些突破性进展。

2.1新型同态加密方案的提出

麻省理工学院的研究团队在2025年提出了融合两种加密工具的部分同态加密方案,适用于私有数据库查询和统计分析等场景。基于MLWE-1024的同态加密方案在数据隐私保护领域取得突破,将密文膨胀率从传统方案的1:33000压缩至1:48,而且保持了相同的安全性[9],为基因组数据安全共享提供了新范式。

2.2门限全同态加密的效率提升

东南大学李松泽团队(2025,USENIX Security)会议上提出了基于BFV加密的门限全同态加密方案,创新性采用“加密份额”设计,解决了计算效率与容错性无法兼顾的长期挑战。实验显示,当参与方数量为1000时,新方案实现了3.83-15.4倍加速[10]。

2.3多密钥同态加密的进展

CCS19方案将TFHE框架与MKFHE融合,支持多用户以独立密钥对加密数据执行联合密文计算。BGV型MKFHE方案通过密钥切换和密文扩展优化,进一步降低了公钥尺寸和计算复杂度,为跨机构的多方安全计算提供了支撑[2]。

2.4抗量子同态加密的落地

基于格密码学的同态加密方案已证明具有抗量子攻击能力。NIST标准化的Kyber算法为同态加密提供了后量子安全基础,Mind Network等项目将相关技术集成到区块链基础设施,确保长期数据安全。

2.5应用领域拓展

同态加密技术已经拓展应用到了云计算、金融、医疗保健、物联网、智能制造等领域。随着大数据规模扩展、物联网终端数量增多、区块链应用深化、硬件芯片算力跃升,同态加密技术将获得更加广阔的应用前景。

2.6与人工智能技术结合

同态加密正深度融入机器学习等人工智能技术,这种融合不仅打破了数据隐私保护与模型训练的固有矛盾,而且为人工智能技术的发展注入了新的活力,共同推动数据安全与隐私保护领域的发展。

3 同态加密技术的典型应用

凭着“数据可算不可见”的独特优势,同态加密技术在多领域中展现出广泛的应用前景。

3.1云计算领域

云计算服务普及背景下,云端数据的安全性是用户关注的焦点问题。同态加密支持在不解密数据的情况下对数据进行计算,可以有效保护数据的隐私和安全,特别适合在线数据分析、协同计算等需要保护用户隐私的云计算应用场景[3]。

3.2医疗保健领域

医疗机构处理大量的敏感患者数据时,保护患者隐私成为行业难点。同态加密技术能保障医疗机构在不解密数据的情况下,对患者隐私数据进行统计分析,进而有助于改进医疗服务质量,并提高医疗效率[3]。

3.3金融服务领域

金融交易中防止交易数据泄露和非法访问至关重要。蚂蚁集团的“摩斯安全计算平台”基于同态加密技术,支持金融机构在密文环境下进行联合建模,已服务超过200家银行。同态加密技术支持在加密状态下对交易数据进行验证和处理,能够阻止未经授权的访问,降低篡改交易风险,进而提高金融交易的安全性。

3.4区块链领域

区块链技术中交易数据是公开透明的,可能会暴露用户隐私数据。引入同态加密技术,在保护用户数据隐私的同时,可以保证区块链的公开性和不可篡改性[11],实现交易数据的验证和记录,进而有效解决用户隐私保护难题。

3.5电子投票领域

电子投票时需要确保投票的匿名性、正确性和可验证性。通过同态加密,选民本地加密选票后提交,计票中心直接对密文进行求和(计票)操作,最终公布解密结果[13],实现了“选票保密性”和“计票正确性”的统一。

4 同态加密面临的主要挑战与应对策略

同态加密技术在数据安全和隐私保护领域展现出了巨大潜力,但在实际应用中仍然面临着诸多技术挑战,其具体内容和应对策略分别如下：

4.1计算效率优化

计算效率提升是优化同态加密技术的首要瓶颈。由于同态加密涉及模幂运算、多项式乘法等复杂数学运算,导致加解密计算耗时剧增。大规模数据处理的效率问题尤为突出,严重制约了同态加密技术的实用性和普及程度[5]。

我们通过算法改进和硬件升级两个方面来提高计算效率。首先,优化算法中的数学运算、降低算法复杂度,减少不必要的循环计算,能提升同态加密的计算效率[7]。同时升级使用专用硬件加速器来提高计算性能,在GPU、专用芯片等硬件上实现高效的并行计算和数据处理[12]。

4.2密钥管理改进

密钥管理复杂度随着计算规模指数级增长。密钥管理需同时满足密文计算支持与安全防护需求,其生成、分发及维护过程存在着系统性挑战。

在密钥管理时可以采用分层密钥结构、密钥协商协议以及安全的密钥存储和访问机制,以便保障密钥在全生命周期中的安全性、可用性和可追溯性[8],以此降低密钥泄露的风险,提高加密系统的稳健性。

4.3安全性增强

同态加密能够提供强大的数据隐私保护能力,但现有技术方案在实际应用中仍然可能受到侧信道攻击、代数攻击等威胁。

为了增强安全性,需要不断深入研究同态加密的安全性理论,识别潜在安全漏洞并设计针对性的防御措施。同时,还可以构建同态加密安全评估模型,通过攻击实验来验证在各种攻击威胁下的安全防护强度[4]。

4.4标准化与生态建设

同态加密发展虽然已有一些标准,但与现有云计算、大数据架构的深度融合仍缺乏统一接口和开发框架,安全性与效率的平衡调优也较为复杂,导致应用落地成本高,难以部署应用[2]。

为了促进同态加密技术的标准化与生态建设,需要优先制定行业标准,定义密钥管理API、密文计算协议等接口规范。同时,行业协会应争取获得开源工具与社区支持,推动开源低代码开发平台,降低应用门槛。此外,政企合作共建测试床也有助于加速在医疗、金融等领域的落地验证。

5 结语

本文围绕同态加密的技术演进、应用图谱、挑战与对策等三个维度展开了系统性研究,对其典型应用场景进行了具体分析,并针对同态加密技术面临的主要技术挑战分别提出了应对策略。同态加密技术将在多个领域获得长足的发展,尤其是在算法优化、动态密钥管理与轻量化协议设计、隐私计算与AI深度融合、硬件芯片级加速架构应用等研究方向将发挥重要作用。通过技术迭代和不断探索创新,同态加密技术有望成为数据要素安全流通的核心使能技术,为数字经济的蓬勃发展提供可信支撑。

[参考文献]

[1]刘钦菊,路献辉,李杰,等.全同态加密自举技术的研究现状及发展趋势[J].密码学报,2021,8(05):795-807.

[2]祁正华,何菲菲,张海桃,等.多密钥全同态加密的研究现状与发展趋势[J].南京邮电大学学报(自然科学版),2023,43(04):72-82.

[3]李宗育,桂小林,顾迎捷,等.同态加密技术及其在云计算隐私保护中的应用[J].软件学报,2018,29(7):1830-1851.

[4]秦宏春.同态加密技术在大数据安全中的应用研究[J].无线互联科技,2023,20(14):97-99.

[5]李浪,余孝忠,杨娅琼,等.同态加密研究进展综述[J].计算机应用研究,2015,32(11):3209-3214.

[6]魏本强,路献辉,王睿达,等.全同态加密应用的编码技术综述[J].密码学报,2024,11(03):521-544.

[7]高丽红,韩少卿,郑涛,等.基于同态加密技术的新型电力系统网络信息检索方法[J].河北电力技术,2025,44(01):59-65.

[8]郑志勇,张艺,朱豆豆,等.同态加密技术在联邦学习中的应用[J].河南科学,2023,41(07):938-945.

[9]Alexandra Henzinger,Ellen Swallow Richards,Yael Kalai. Security scheme could protect sensitive data during cloud computation[J].MIT Security and Cryptography.2025.

[10]常益嘉,李松泽,Arbitrary-Threshold Fully Homomorphic Encryption with Lower Complexity[C],The 34th USENIX Security Symposium2025.

[11]段嘉俊,柳毅,陈家辉.基于区块链的电子医疗数据安全共享方案[J].计算机应用与软件,2024,41(10):116-121.

[12]秦智翔,杨洪伟,郝萌.隐私计算环境下深度学习的GPU加速技术综述[J].信息安全研究,2024,10(7):586-593.

[13]杨亚涛,赵阳,张奇林.基于SEAL库的同态加权电子投票系统[J].计算机学报,2020,43(4):711-723.

作者简介：

金世皓(2006--),男,河南新乡人,厦门大学马来西亚分校,研究方向：软件工程。