基于同态加密的多方数据共享安全机制研究

李猛
杭州安恒信息安全技术有限公司　浙江杭州　310000

【摘　要】数字化时代里，多方数据共享成为各领域创新发展的关键驱动力。但数据隐私和安全问题也相伴而生，限制着数据共享的程度。同态加密技术的诞生，给解决这些难题带来新思路。文章着眼于基于同态加密的多方数据共享安全机制展开探究，阐释同态加密原理以及其于数据共享中的长处，深入探讨该安全机制的设计架构、关键技术的落地实现和实际应用场景，同时对其性能状况和面临的挑战予以评估剖析，给出应对办法，目的是为构建安全且高效的多方数据共享环境，提供理论与实践层面的支撑。

【关键词】同态加密；多方数据共享；安全机制；数据隐私；加密技术

Research on secure mechanism of multi-party data sharing based on homomorphic encryption

Li Meng
Hangzhou Anheng Information Security Technology Co.，LTD. Zhejiang Hangzhou　310000

【Abstract】In the digital age，multi-party data sharing has become a key driver for innovation and development across various fields. However，issues of data privacy and security have emerged，limiting the extent of data sharing. The emergence of homomorphic encryption technology offers new solutions to these challenges. This article focuses on exploring secure mechanisms for multi-party data sharing based on homomorphic encryption，explaining the principles of homomorphic encryption and its advantages in data sharing. It delves into the design architecture，implementation of key technologies，and practical application scenarios of this security mechanism. Additionally，it evaluates the performance status and challenges faced by the system，providing strategies to address them. The aim is to support the construction of a secure and efficient multi-party data sharing environment from both theoretical and practical perspectives.

【Key words】homomorphic encryption；multi-party data sharing；security mechanism；data privacy；encryption technology

引言

大数据与人工智能蓬勃时，多方数据共享于金融、医疗、科研等领域日趋重要。整合各异源数据，能挖掘高价值信息以促进行业创新。于医疗领域可助力探寻疾病规律，在金融领域利于评估信用风险。但数据共享存在显著安全隐患，数据含敏感内容，传统加密在共享时先解密，易引发泄露。同态加密技术可对加密数据运算，结果与明文运算等同，为数据共享提供新安全途径。研究基于此技术的安全机制，对保障数据安全、推进共享意义非凡。

一、同态加密技术基础与数据共享优势

（一）同态加密原理剖析

同态加密时，借特定加密算法把明文数据转为密文。拿基于数学难题的同态加密算法来讲，运用由一对大整数构成的公钥加密明文，经繁杂数学运算，让明文与公钥结合产生密文。解密要用对应的私钥，对密文做反向运算，从而还原出明文。此过程中，加密、解密算法设计依托特定数学难题，像整数分解、离散对数等问题，以此保证在不知私钥时，很难从密文推出明文。同态加密关键特性在于支持同态计算，能对加密数据做特定运算。比如加法同态加密，可对两个密文相加，解密后的结果和相应明文相加结果一样；乘法同态加密支持密文相乘，解密后也能得到正确的明文相乘结果。有了这特性，数据在加密状态下就能处理、分析，规避了数据解密引发的安全风险。

（二）同态加密在数据共享中的独特优势

多方数据共享时，数据所有者能够先加密数据再共享。因同态加密支持在密文上运算，数据使用者没有私钥，无法知晓数据真实内容，仅能按授权对加密数据操作，有力保护了数据隐私。像医疗数据共享方面，患者病历经同态加密后提供给研究机构，研究机构可对加密数据做统计分析，比如算某种疾病发病率，却无法得知患者具体身份及详细病情[1]。传统数据共享在处理数据时通常要解密，这无疑增加了数据

泄露风险。同态加密让数据在共享与处理全程都维持加密，仅在最终要用数据结果时才解密，极大降低数据泄露几率。就算数据传输或存储时泄露，攻击者得到的也是加密数据，很难从中获取有用信息。

二、基于同态加密的多方数据共享安全机制设计

（一）安全机制架构设计

数据所有者处于数据源头，掌控着数据所有权与控制权。他们承担对自身掌握数据的加密任务，这意味着数据所有者得熟知数据敏感程度及应用场景，挑选合适的同态加密算法与加密参数，以此保障加密后数据的安全性与可用性。在基因数据共享项目里，科研人员身为数据所有者，要对采集的大量基因数据加密。鉴于基因数据关乎个人遗传隐私，一旦泄露后果严重，科研人员会采用安全性高、适配复杂数据结构处理的同态加密算法，把基因数据转变为密文。加密完成，数据所有者将加密数据分享给数据使用者，同时明晰数据使用目的、范围和期限等授权信息，确保数据共享合规。

数据使用者肩负挖掘数据价值之责，在数据所有者授权范畴内，对加密数据开展计算和分析。这需要他们具备相应技术能力与业务知识，熟练运用同态加密技术的计算特性，从加密数据里提取有价值信息。于金融领域，金融机构作为数据使用者，获客户授权后，会借助加密的交易数据训练风险评估模型。运用同态加密计算功能，在不触及客户交易细节的情况下，对加密数据进行统计分析与模型运算，为客户生成精准风险评估报告，提升金融服务质量与效率。复杂数据共享场景里，可信第三方起着关键的桥梁和监管作用。他们主要承担密钥管理与访问控制等重要工作，以此保障数据共享安全合法。在一些跨机构科研合作项目中，科研管理机构作为可信第三方，采用先进密钥管理系统，对参与项目各方的密钥集中管理。经严格的密钥生成、存储和分发流程，确保密钥安全且唯一。同时，科研管理机构根据项目研究需求及各方角色，制定详尽访问控制策略，监督数据使用，防范数据滥用或非法获取，维护数据共享环境的公平与安全。

数据所有者按自身需求选合适同态加密算法加密数据，兼顾数据类型、规模与后续计算需求。像医疗费用统计这类结构化数值数据，加法同态性好的算法适配；医学影像这类含大量浮点数的图像数据，支持近似同态计算的算法更佳。加密后，数据所有者可将加密数据传至专业数据共享平台（平台有强存储和传输能力保障数据安全高效），也能直接给数据使用者。数据使用者接收加密数据，本地利用同态加密计算特性，依授权范围和规则，用专业工具算法处理。医疗研究中，研究人员获加密病历数据后，用专门软件在加密状态下统计分析，如算疾病发病率、治愈率等指标，无需解密患者具体信息。

（二）关键技术实现

Paillier 算法凭借优良加法同态性，在加密数据需做加法运算处大显身手，像统计求和、算平均值等场景。以电商平台销售数据统计为例，商家可用 Paillier 算法加密每日销售额。平台对加密数据求和得总销售额，却无需知晓具体数值，从而守护了商家商业机密[2]。研究人员为提升 Paillier 算法性能，从参数设置优化入手，选更适配的大整数参数，提升计算效率；还改进计算流程，删减不必要步骤，增强算法安全性。CKKS 算法在处理浮点数领域优势突出，因其支持近似同态计算，很契合机器学习里的数据处理场景。就拿图像识别的机器学习模型训练来说，图像数据含大量浮点数像素值。经 CKKS 算法加密后，模型能在加密数据上开展卷积运算、池化操作等训练。研究人员通过改进 CKKS 算法量化策略，降低量化误差，提升模型训练精度；还对算法计算复杂度加以优化，加快模型训练速度。

基于身份的密钥管理系统堪称有效之法，其依据参与方身份信息生成密钥。在跨国科研合作项目里，各参与机构都有独一无二的身份标识，系统据此为各机构生成相应密钥。这般操作确保密钥唯一且安全，毕竟各机构密钥与其身份紧密相连，大大降低密钥遭冒用风险。借助诸如 Diffie – Hellman 密钥交换协议这类安全的密钥分发协议，在参与方间安全分发密钥。这份协议依托数学难题搭建而成，就算网络环境欠佳，参与各方依旧能够安全地进行密钥信息的交互。在实际投入应用的过程中，参与的各方借助 Diffie – Hellman 协议来共同确定共享密钥，随后依据该共享密钥分别生成各自的公钥和私钥，以此确保密钥分发的整个过程都处于安全状态，能够有效地抵御密钥出现泄露的风险。

三、基于同态加密的多方数据共享安全机制应用场景

（一）医疗数据共享场景

医学研究开展疾病探究、药物研发等工作，离不开大量患者医疗数据。医院、医疗机构这些数据所有者，运用基于同态加密的多方数据共享安全机制，加密患者医疗数据后分享给医学研究机构[3]。研究机构能对加密数据做统计分析，比如计算不同年龄段、性别中某种疾病发病率，探究疾病与遗传因素关联等。因数据全程加密，患者隐私得以有效保护。远程医疗场景下，患者医疗数据要在患者、医生及医疗机构间共享。基于同态加密技术，患者医疗数据加密后传送给医生，医生可对加密数据开展诊断操作，像查看患者生命体征、

影像数据等，进而给出诊断建议。诊断建议同样加密后反馈给患者或医疗机构，保证数据在传输与处理时的安全性。

（二）金融数据共享场景

金融机构做信贷评估之际，得把多个数据源信息整合起来，像个人信用档案、资产状况、消费习惯等。借由同态加密手段，不同金融机构能将自身掌握的数据加密，而后分享至联合信贷评估平台。该平台可对加密数据展开运算，比如综合考量客户信用风险并给出信用评分。因数据加密，客户敏感信息得以守护，金融机构也能收获更精准的信用评估成果。在金融市场剖析方面，金融机构可将自家交易数据、市场行情数据等加密后，分享给专业数据分析机构。数据分析机构能够针对加密数据实施复杂剖析，像是预估市场走向、分析投资组合风险之类。加密技术保障了金融机构数据安全，也为金融市场平稳发展给予了有力支撑。

四、安全机制性能评估与挑战应对

（一）性能评估指标与结果分析

计算效率属于衡量同态加密安全机制性能的关键指标。测试不同规模数据在同态加密运算与明文运算所花时间，以此评判同态加密对计算效率的影响。实验显示，相较明文计算，同态加密计算效率会有一定下滑，处理大规模数据时更为明显[4]。不过伴随技术持续进步、算法不断优化，计算效率正逐步提升。采用更高效同态加密算法，搭配硬件加速技术，能够有效缩短计算耗时。安全性是同态加密安全机制的核心所在。分析同态加密算法抵御各类攻击的能力，像密码分析攻击、侧信道攻击等，进而评估其安全性。当下，多数同态加密算法理论上安全性颇高，然而实际应用中，密钥管理、算法实现等环节的安全隐患仍需留意。比如强化密钥防护，防范密钥泄露；优化算法实现，规避安全漏洞，借此提升系统整体安全性。

（二）面临的挑战与应对策略

面临复杂计算任务，同态加密的计算性能仍旧是个棘手问题。要攻克这一难题，能够采用硬件加速的办法，比如借助图形处理器（GPU）或者现场可编程门阵列（FPGA），来加快同态加密的计算进程。进一步优化同态加密算法，降低计算复杂程度，提升计算效率，比如钻研新的同态加密算法架构，采用更高效的计算办法。多方数据共享里，密钥管理颇为繁杂，涵盖密钥生成、分发、存储以及更新等流程。要简化密钥管理，能够采用集中式密钥管理系统，由可信第三方统一负责密钥管理[5]。同时凭借区块链技术去中心化、不可篡改的特性，增强密钥管理的安全性与可追溯性，像把密钥生成和分发记录存于区块链上，保证密钥管理的透明、安全。

当下同态加密技术欠缺统一标准，各类算法以及实现方式彼此间存在兼容性难题。想要解决此问题，就得推进同态加密技术标准化工作，拟定统一的技术标准与接口规范。还要强化不同系统间兼容性测试，保证同态加密安全机制在各异平台与环境中都能正常运作，比如搭建同态加密技术标准化测试平台，针对不同算法及实现开展兼容性测试。

结语

同态加密构建的多方数据共享安全机制，为数据共享安全难题给出有效解法。经探究同态加密技术原理与长处，设计恰当安全机制架构，落实关键技术，在医疗、金融等领域应用，证实此安全机制在守护数据隐私、降低泄露风险、提升数据共享灵活性上作用显著。虽说当前这些安全机制在计算性能、密钥管理、标准兼容性方面存有挑战，不过采取对应办法，像硬件加速、优化算法、推进标准化等，能逐步攻克这些难关。随着技术持续进步，基于同态加密的多方数据共享安全机制会日益完善，给各领域数据共享提供更可靠安全保障，助力数字化时代数据驱动的创新发展。

参考文献

[1]彭鑫才.工业物联网中基于同态加密的轻量级隐私保护技术研究[D].电子科技大学，2024.DOI：10.27005/d.cnki.gdzku.2024.002153.

[2]魏啸磊，林苏，潘越，等.支持多数据源安全共享的分布式大数据协作系统研究[J].计算机时代，2022，(06)：10-13.

[3]林英杰.基于同态加密智能合约的电力数据安全共享方案研究与实现[D].哈尔滨工业大学，2022.DOI：10.27061/d.cnki.ghgdu.2022.000925.

[4]马英.一种基于隐私计算的数据共享模型研究[J].信息安全研究，2022，8(02)：122-128.

[5]刘婷婷.基于同态加密的聚类算法及其在精准营销中的应用研究[D].南京邮电大学，2021.DOI：10.27251/d.cnki.gnjdc.2021.000823.