基于复制中位数聚合的拜占庭容错安全分布式矩阵乘法

刘怀远[1*]，刘懿中[1,2]，刘建伟[1,2]
（1. 北京航空航天大学网络空间安全学院，北京 100191；
2. 北京航空航天大学杭州创新研究院，杭州 310051）

摘要：安全分布式矩阵乘法（secure distributed matrix multiplication, SDMM）是解决大规模分布式计算中数据隐私泄露与节点滞后问题的关键技术。然而，现有安全分布式矩阵计算（secure distributed matrix computation, SDMC）的多项式编码框架多基于半诚实安全模型，面对篡改计算结果的拜占庭恶意攻击时，缺乏轻量化的节点识别机制。针对该问题，本文提出一种面向主动结果篡改场景的拜占庭容错验证扩展方案。该方案在依托传统多项式掩码技术实现隐私保护的基础上，引入冗余复制计算策略，结合逐元素中位数鲁棒聚合机制，可有效抵御数据投毒攻击。同时，部署轻量化统计验证层，通过弗罗贝尼乌斯范数偏差评分实现恶意节点的检测与隔离。理论分析证明，在恶意节点数量满足诚实多数阈值约束的条件下，本方案可实现矩阵乘积结果的精准重建。实验结果表明，当矩阵维度由 32 提升至 512 时，该方案表现出良好的可扩展性，运行开销比由 4.86 降至 1.06。该方案无需依托复杂的密码学证明机制，可为去中心化云环境下的矩阵乘法运算提供一种高可扩展、可验证的具备拜占庭容错能力的解决方案。

关键词：安全分布式矩阵乘法；拜占庭容错；中位数聚合；弗罗贝尼乌斯范数；冗余复制
中图分类号：TP309 **文献标志码：**A
DOI: 10.20172/j.issn.2097-3136.260620

Byzantine-resilient secure distributed matrix multiplication based on replicated median aggregation

Liu Huaiyuan[1*], Liu Yizhong[1,2], Liu Jianwei[1,2]
（1. School of Cyber Science and Technology, Beihang University, Beijing 100191, China;
2. Hangzhou Innovation Institute, Beihang University, Hangzhou 310051, China）

Abstract: Secure distributed matrix multiplication (SDMM) is a core technique to solve data privacy leakage and node straggler problems in large-scale distributed computation. Most existing polynomial coding frameworks of secure distributed matrix computation (SDMC) are based on the semi-honest security model and lack lightweight mechanisms to identify Byzantine malicious nodes that tamper with calculation results. To solve this problem, this paper proposes a Byzantine fault-tolerant verification extension scheme for active result tampering scenarios. While retaining the privacy protection capability of the traditional polynomial masking scheme, the proposed scheme introduces a redundant replication strategy and combines it with element-wise robust median aggregation to effectively mitigate data poisoning attacks. Furthermore, it deploys a lightweight statistical verification layer, which detects and isolates malicious nodes through Frobenius norm deviation scores. Theoretical analysis demonstrates that the scheme can realize the accurate reconstruction of matrix products when the number of malicious nodes meets the honest majority threshold condition. Experimental results show that the proposed scheme has excellent scalability when the matrix dimension increases from 32 to 512, and its runtime overhead ratio drops significantly from 4.86 to 1.06. Independent of complex cryptographic proof mechanisms, the proposed scheme provides a highly

* **通信作者：**E-mail: intouchables@buaa.edu.cn
基金项目：国家自然科学基金（U21B2021, 62472015, 62202027）

引用格式：刘怀远，刘懿中，刘建伟. 基于复制中位数聚合的拜占庭容错安全分布式矩阵乘法 [J]. 网络空间安全科学学报，2026，4（3）：53 - 63.

Citation Format: Liu H Y, Liu Y Z, Liu J W. Byzantine-resilient secure distributed matrix multiplication based on replicated median aggregation[J]. Journal of Cybersecurity，2026，4（3）：53 - 63.

scalable, verifiable and Byzantine fault-tolerant solution for matrix multiplication operations in decentralized cloud environments.

Keywords: secure distributed matrix multiplication; Byzantine fault tolerance; median aggregation; Frobenius norm; redundant replication

0 引言

矩阵乘法是现代计算范式的数学基石，在工程应用、数据分析及人工智能领域中，属于高计算复杂度、高资源消耗的核心运算。随着数据维度呈指数级增长，受时延与内存资源的严格限制，单台本地设备已无法高效完成大规模矩阵乘法运算。因此，业界普遍采用分布式计算架构开展大规模计算任务。MapReduce[1] 等分布式框架形成了标准化范式，即将海量数据集分割为细粒度、易处理的子数据块，将计算任务分发至分布式工作节点集群或云端边缘服务器执行。在大规模机器学习场景中，分布式矩阵乘法通过并行化分片计算，为深度神经网络与复杂优化模型的高效训练提供了核心支撑。尽管高维数学运算的外包处理可大幅缩短计算耗时、缓解本地设备资源瓶颈，但该方式本质上迫使数据所有者将敏感矩阵数据暴露给第三方外部计算节点与服务设施。这种从本地集中式处理到分布式云计算的模式变革，引发了数据隐私泄露、计算完整性破坏及系统可靠性下降等多重安全风险，亟须构建高效可靠的安全防护机制。

为实现外包数据的安全防护，现有研究多基于“诚实但好奇”的半诚实威胁模型构建编码分布式计算框架。该威胁模型假设，分布式工作节点会严格遵循既定计算协议，但存在被动串通、窃取私有输入矩阵数据的风险。多项式编码可基于信息论隐私有效抵御该类被动窃听行为，但实际分布式系统面临更严峻的安全威胁，即主动攻击者的恶意破坏行为。在主动攻击模型中，被入侵或恶意拜占庭节点不仅试图窃取隐私数据，还会通过返回伪造、篡改及随机无效结果，蓄意破坏整体计算流程。该类恶意行为一方面可被攻击者用于实施机器学习模型投毒攻击，另一方面也可由惰性服务器为节约自身计算资源、规避计算开销而返回无效随机数据所引发。传统聚合方案（如朴素均值聚合、标准多项式插值）容错能力极差，拜占庭节点仅需注入少量篡改结果，即可导致最终矩阵重建结果完全失效。因此，实现安全模型从被动隐私防护到主动攻击韧性防御的升级，是当前分布式网络安全防护亟须突破的核心难题。

现阶段该领域极具代表性的研究为基于多项式编码的安全高效分布式矩阵计算（secure distributed matrix computation，SDMC）框架[2]。SDMC 协议通过对输入矩阵进行分块处理，并采用优化设计的随机扰动矩阵完成数据掩码，有效应对了数据隐私保护与滞后节点（慢节点）干扰问题。该协议通过多项式多点求值完成分布式计算，只要有效返回结果的节点数量满足预设阈值要求，客户端即可精准重建最终的矩阵乘积结果。但 SDMC 框架存在根本性局限，其安全架构严格依赖半诚实威胁模型，无法适配复杂的主动攻击场景。由于 SDMC 协议采用传统多项式解码方式，自身不具备校验节点返回结果数学正确性的内置验证机制。若 SDMC 架构内的恶意服务器蓄意篡改本地计算结果，客户端会无差别接收篡改数据并参与解码运算，最终造成矩阵解码结果错误，从而导致计算失效。Fan 等[2] 在研究结论中明确指出了该架构缺陷，并指明了未来研究方向：亟须对 SDMC 协议进行拓展，适配主动攻击威胁模型，使外包计算在抵御数据窃听的同时，可实现计算结果的数学可验证。

针对 SDMC 框架的现有缺陷，结合该领域既定未来研究方向，本文构建可验证的拜占庭容错架构，将传统 SDMC 框架从半诚实安全范式拓展至主动攻击防御场景。本文通过数学推导与仿真实验验证，提出一种可在主动攻击场景下同时保障计算隐私性与结果正确性的鲁棒方案。本文主要贡献如下。

1）构建并实现了主动威胁模型，通过配置可篡改计算结果的分布式恶意工作节点子集，验证了传统简单聚合算法在主动拜占庭攻击下的失效问题。

2）引入冗余复制计算策略，结合逐元素中位数鲁棒聚合机制，在各分块任务的恶意节点数量满足诚实多数阈值约束的条件下，保障真实矩阵乘积结果的精准恢复。

3）提出一种轻量级统计可验证机制，用于量化评估各工作节点的输出偏差。该机制通过计算工作节点返回结果与中位数鲁棒恢复结果的归一化弗罗贝尼乌斯范数（Frobenius norm，F-范数）距离，结合预设判别阈值标记高可疑度的拜占庭节点。本文通过阈值扫描实验，明确了该机制的误判率、漏判率及可落地的最优阈值区间。

1　相关工作

1.1　编码分布式计算与 SDMM

自 Yu 等[3]提出多项式编码方法以来，编码理论与分布式计算的交叉研究取得了长足的进展。多项式编码最初用于解决高维矩阵乘法中的滞后节点干扰问题，该方法将矩阵分块并编码为全局多项式的多点求值结果，使客户端可通过快速响应的节点子集完成结果解码。该思想进一步延伸至数据加密与隐私计算领域，催生了安全分布式矩阵乘法（secure distributed matrix multiplication, SDMM）系列方案。为优化通信开销与恢复阈值的权衡关系，研究者设计了多种矩阵划分与编码策略。MatDot 码与 PolyDot 码是该领域的代表性研究成果，可为分布式计算提供灵活的编码框架，有效权衡了矩阵编码上传开销与计算结果下载开销。

现阶段相关研究多聚焦于编码阈值的数学优化。例如，Mital 等[4]利用有限域离散傅里叶变换的优良特性，大幅降低了 SDMM 计算架构中的数据上传开销。此外，前沿研究逐步引入代数几何（algebraic geometry, AG）码开展优化设计[5-6]。代数几何码可支持分布式工作节点数量突破有限域规模限制，克服了传统里德−所罗门（Reed-Solomon, RS）多项式码的固有缺陷，可实现与底层函数域属数正相关的近最优恢复阈值。上述研究有效优化了通信带宽开销，提升了算法对滞后节点的容错性能，但绝大多数传统 SDMM 协议均基于半诚实节点假设设计，无法有效抵御恶意数据篡改等主动攻击，存在明显的安全缺陷。

1.2　拜占庭容错性与主动攻击者

拜占庭恶意节点的防御问题是去中心化分布式系统的研究重点，推动相关研究从被动隐私防御逐步转向主动攻击对抗。孙钰等[7]系统梳理了联邦学习场景下的拜占庭攻击与鲁棒防御策略，证明坐标中位数、截断均值、几何中位数等聚合机制可有效抑制恶意梯度干扰；但引入安全聚合、同态加密等隐私保护方案后，传统梯度统计检测方法的有效性会大幅受限，存在鲁棒性与隐私性难以兼顾的问题。在分布式机器学习任务中，拜占庭节点注入的恶意梯度可隐蔽破坏全局模型的收敛性能。

为解决该问题，学术界围绕鲁棒有界聚合规则开展了大量研究。Li 等[8]针对拜占庭鲁棒聚合算法开展了系统性实验验证，证明算术平均等基础聚合方法对主动数据投毒攻击极为脆弱；而截尾均值、中位数等鲁棒统计算子可有效识别并剔除极端异常值，保障计算结果的稳定性。Li 等[9]进一步探究了拜占庭攻击下分布式学习的鲁棒聚合难题，指出当诚实节点的本地梯度差异较大时，直接采用坐标中位数、截尾均值等鲁棒有界聚合规则会产生显著的性能退化。

在编码矩阵乘法的拜占庭容错研究中，Makkonen 与 Hollanti[10]将拜占庭容错机制引入编码矩阵乘法领域，构建了面向拜占庭攻击的线性 SDMC 通用框架，形式化推导了系统可容忍的合谋恶意节点数量理论上界。在此基础上，Hofmeister 等[11]构建了突破 Singleton 界的自适应安全框架，通过随机校验机制识别矩阵乘法的异常计算结果。Ghasvarianjahromi 等[12]提出基于逻辑环结果验证的去中心化稀疏矩阵乘法协议，可有效抵御拜占庭恶意破坏行为。周一可等[13]提出面向异步 BFT（Byzantine fault tolerance）场景的 IDumbo 协议，依托门限加密、零知识证明与分层委员会机制实现全流程隐私保护与拜占庭容错，在保障高吞吐性能的前提下，提升了系统对 Sybil 攻击与恶意节点扰动的鲁棒性。现有研究证实，主动攻击防御需依托数学冗余或密码学冗余机制，但该类防御手段会引入额外的通信冗余与计算时延，造成系统开销显著增加。因此，如何在保留 SDMC 框架高效计算优势的基础上，嵌入鲁棒聚合算子构建高弹性安全协议，是当前该领域亟待解决的关键问题。

1.3　可验证计算

外包计算场景对计算完整性的需求，推动了可验证计算（verifiable computation, VC）技术的发展。该技术可支持资源受限客户端无需本地重算，即可校验服务节点计算结果的正确性。VC 验证方式主要分为两类：高开销密码学验证与轻量化统计验证。在密码学验证领域，研究者已提出多种可验证计算方案。Ning[14]验证了多证明者零知识简洁非交互式知识论证（zero-knowledge succinct non-interactive arguments of knowledge, zk-SNARK）在分布式云场景的适用性，设计了可支持各证明者独立生成多项式求值正确性证明的验证方案。同态消息认证码（message authentication code, MAC）与安全多方计算框架可实现算术计算结果的合法性认证，保障加密数据运算的端到端可验证性[15]。

高开销密码学验证方法可提供强拜占庭容错性能，但证明生成与校验过程会分别给工作节点与客户端带来极大的计算开销，大幅抵消了矩阵乘法外

包计算的低时延优势。相对而言，轻量化统计验证依托编码冗余与经验阈值完成结果校验，开销更低、适配性更强。Wang 与 Mtibaa[16] 面向资源受限边缘设备，提出了基于任务复制的可验证计算框架。该框架通过多服务器任务复制与结果方差分析，使客户端可基于统计特征判定计算结果的正确性。本文所提扩展方案与轻量化验证范式高度契合，通过结合中位数鲁棒聚合与偏差评分机制，构建了高适用性、低开销的结果验证方法，可精准识别恶意数据篡改行为，规避了密码学证明带来的高计算开销，契合 SDMC 框架的优化发展需求。

2 系统模型与拜占庭威胁模型

分布式矩阵乘法系统的核心目标是将计算负载外包至由 N 个分布式工作节点构成的集群，支撑资源受限客户端完成超大规模矩阵的乘法运算。设两个私有输入矩阵分别为 $\boldsymbol{A}\in\mathbb{R}^{n\times m}$ 和 $\boldsymbol{B}\in\mathbb{R}^{m\times p}$。为适配并行计算架构，需对大规模原始矩阵进行分块处理，拆解为粒度更小、便于运算的子矩阵。本文系统模型采用外积划分策略完成矩阵分块。具体而言，将左矩阵 $\boldsymbol{A}$ 按列划分为 m 个独立子块，即 $\boldsymbol{A}=[A_1|A_2|\cdots|A_m]$，各子块维度为 $A_i\in\mathbb{R}^{n\times 1}$。对应地，将右矩阵 $\boldsymbol{B}$ 按行划分为 m 个匹配子块，即 $\boldsymbol{B}=[B_1;B_2;\cdots;B_m]$，各子块维度为 $B_i\in\mathbb{R}^{1\times p}$。根据线性代数外积运算规则，维度为 $n\times p$ 的目标乘积矩阵 $\boldsymbol{C}=\boldsymbol{AB}$ 可拆解为：$\boldsymbol{C}=\sum_{i=1}^{m}\boldsymbol{A}_i\boldsymbol{B}_i$。该划分方式对分布式计算场景具有显著优势，既可有效降低各工作节点的存储开销，又可实现各子矩阵乘积 $\boldsymbol{A}_i\boldsymbol{B}_i$ 的分布式独立计算，为客户端的最终结果聚合提供支撑。

2.1 半诚实模型方案

本文扩展方案以 Fan 等[2] 提出的安全高效分布式矩阵计算协议为基础框架。原始 SDMC 架构基于严格的“诚实但好奇”（半诚实）威胁模型设计。为避免工作节点窃取并推测分块 A_i 和 B_i 的隐私数据，客户端生成与各数据块维度完全一致、服从均匀随机分布的扰动矩阵（噪声矩阵）集合。随后，客户端将原始数据块与随机噪声矩阵嵌入至定制编码多项式，分别构造多项式 $f(x)$ 与 $g(x)$。针对各工作节点 W_j，客户端在不同标量点 α_j 处完成多项式求值运算。各工作节点 W_j 接收编码份额 $f(\alpha_j)$ 和 $g(\alpha_j)$，并计算局部乘积 $h(\alpha_j)=f(\alpha_j)g(\alpha_j)$。由于原始数据已通过随机扰动矩阵完成代数掩蔽，至多 T 个工作节点构成的合谋联盟无法获取原始矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$ 的任何信息论有效信息。客户端收集足够数量的节点求值结果后，可通过标准多项式插值算法（RS 解码）滤除噪声，精准还原目标矩阵：$\boldsymbol{C}=\sum_{i=1}^{m}\boldsymbol{A}_i\boldsymbol{B}_i$。该方案虽可通过数学机制实现隐私保护，但完全依赖于工作节点无差错执行局部计算 $h(\alpha_j)$ 的理想假设。

2.2 主动攻击者模型

为消除密码学理论模型与真实分布式云环境的场景差异，本文将威胁模型升级为主动攻击者模型，纳入拜占庭恶意节点的现实干扰因素。正如 Duan 与 Zhang[17] 在信息论拜占庭容错研究中指出，现代去中心化网络普遍存在节点主动偏离既定协议的恶意行为。在本文改进的威胁模型中，恶意工作节点不仅可被动窃取隐私数据，还会主动返回篡改或伪造的异常计算结果，满足 $\tilde{h}(\alpha_j)\neq h(\alpha_j)$。该类恶意行为主要分为两类：一是攻击者蓄意破坏客户端的机器学习模型收敛效果；二是惰性服务器为规避矩阵乘法 $O(n^3)$ 的高计算开销，通过随机生成噪声数据作为计算结果返回客户端，在降低自身运算成本的同时占用计算资源收益[18]。

为保障数学分析的严谨性与仿真实验的可靠性，本文对主动威胁模型的约束条件作出如下明确界定。①本文核心攻击面为计算结果篡改，恶意工作节点可通过输出随机矩阵、缩放矩阵、稀疏投毒矩阵及任意伪造矩阵实施攻击；硬件时序侧信道、DDoS 阻断、网络路由劫持等行为不属于本文核心防御范围，该类系统层干扰通常被归为节点滞后问题或可用性攻击。②恶意节点可在同一复制组内合谋协作、统一攻击策略，但只要各组内恶意节点数量严格小于复制因子 R 的 1/2，逐元素中位数聚合机制仍可准确恢复诚实多数的正确计算结果。③若攻击者具备自适应腐化多数副本、诱导诚实节点输出错误结果，或在客户端阈值确定后实施近阈值低幅度投毒等高强度攻击能力，本文方案仅能输出统计检测信号，无法提供绝对的密码学安全保证。针对该类强攻击模型，需结合认证标签、随机校验、纠错码译码等机制进一步优化防御能力。

3 鲁棒可验证的 SDMM 架构设计

为弥补传统 SDMC 框架缺失可验证计算能力的缺陷，本文构建了全新的轻量化容错技术框架。该方案不再依赖易受主动攻击破坏的标准多项式插值解码方式，引入具备强鲁棒性的统计防御机制。整体架构包含 3 个相互耦合的核心模块：冗余复制计算机制、中位数鲁棒聚合机制与偏差度量的轻量级验证机制。

3.1 冗余复制计算机制

标准编码计算模型的核心缺陷是客户端会将所有工作节点的输出结果纳入统一的联立方程组完成解码求解。若方程组内任意一项结果被恶意篡改，整体插值多项式的求解结果将完全失效。为系统性隔离攻击造成的损害，本文引入显式复制因子 R，同时定义 k 为各分块任务的恶意节点数量、n 为矩阵维度规模。

在任务分发阶段，客户端不再将矩阵分块对 (A_i,B_i)的计算任务分配至单一工作节点，而是生成相同的计算任务，批量分发至由 R 个独立工作节点构成的复制组。例如，当 R=5 时，组内 5 个不同工作节点将独立完成同一矩阵乘积计算任务。复制因子 R 为核心系统参数，直接决定系统的拜占庭容错性能。增大 R 可有效提升系统抗攻击能力，但节点上传份额与客户端下载结果的通信带宽开销将随 R 呈线性增长。因此，R 是平衡系统安全性、通信开销与计算开销的核心参数。

3.2 中位数鲁棒聚合机制

各工作节点完成局部矩阵乘法计算后，客户端将接收每个分块对 i 对应的 R 个候选结果矩阵。该组返回结果矩阵可统一表示为$\{X_{i,1},X_{i,2},\cdots,X_{i,r}\}$。由于分布式网络存在拜占庭恶意节点，该矩阵集合中存在未知数量的篡改异常结果。客户端的核心目标是从该含异常值的矩阵集合中，还原出真实无篡改的矩阵乘积结果$\widehat{A_iB_i}$。

在基础分布式架构中，客户端通常采用算术平均方法 $\frac{1}{R}\sum_{r=1}^{R}X_{i,r}$ 处理冗余数据。从统计鲁棒性角度分析，算术均值的崩溃点为 0，表明该聚合方式容错性极差：仅需单个拜占庭节点实施投毒攻击（如提交极值矩阵），即可造成聚合结果严重偏移，导致子矩阵分块重构完全失效。

为在诚实多数约束条件下实现结果鲁棒恢复，本文提出了逐元素中位数鲁棒聚合的方案，该方案的有效性已得到拜占庭鲁棒联邦学习领域相关研究的验证[9]。针对 $n\times p$ 维子矩阵的任意坐标 (u,v)，客户端提取 R 个工作节点对应位置的标量取值：$\{x_{uv}^{(1)},x_{uv}^{(2)},\cdots,x_{uv}^{(R)}\}$。随后客户端计算该组标量值的统计中位数，将其作为恢复矩阵 $\widehat{\boldsymbol{A}_i\boldsymbol{B}_i}$对应坐标$(u,v)$的真实取值。即便攻击者通过投毒注入极大或极小的异常数值，只要恶意投毒数据不占据多数，中位数机制即可自动屏蔽离群异常值，有效保留诚实节点的真实计算结果。因此，当各分块任务的恶意节点数量 k 满足诚实多数阈值条件$k\leqslant\left\lfloor\frac{R-1}{2}\right\rfloor$时，该聚合方案可精准实现矩阵乘积的无损重构。

3.3 偏差度量的轻量级验证机制

高安全性分布式系统不仅需要实现计算结果的精准恢复，还需具备恶意节点识别、惩处及后续任务剔除的能力。可验证计算是 SDMC 框架向安全可信计算演进的核心优化方向。但多证明者零知识证明、同态加密等传统密码学验证方案，会给资源受限系统带来极高的时延开销与计算开销。

针对该问题，本文构建一种基于统计偏差评分的轻量化、高严谨性验证层机制。客户端求解得到各分块对对应的中位数鲁棒矩阵 $\boldsymbol{M}_i=\mathrm{median}(X_{i,1},X_{i,2},\cdots,X_{i,R})$后，将该矩阵作为可信真实结果。随后，客户端通过计算各工作节点输出结果$X_{i,r}$与可信矩阵$\boldsymbol{M}_i$的空间距离，量化评估各节点的计算可信度。为实现多维矩阵的距离量化，本文引入 F-范数构建节点偏差评分公式：

$$S_r=\left\|X_{i,r}-M_i\right\|_F=\sqrt{\sum_u\sum_v\left((X_{i,r})_{uv}-(M_i)_{uv}\right)^2}$$

该评分机制可在极低额外计算开销的前提下，输出有效的统计验证依据[11]。正常工作节点的输出结果与中位数恢复矩阵基本一致，仅存在微小浮点舍入误差，归一化偏差评分趋近于 0；而拜占庭节点输出的篡改、缩放及随机无效矩阵，会呈现出显著的评分离群特征。通过设置趋近于零的低容错阈值，客户端可实时识别、隔离恶意节点。该机制可在主动攻击模型下满足计算可验证性要求，有效规避了复杂加密算法带来的高计算开销问题。

4 理论分析与性能保证

4.1 正确性与鲁棒性证明

为更好地刻画前文所提冗余安全分布式矩阵乘法系统的容错能力，本文定义并证明“诚实多数定理”。记复制因子为 R，任一分块对计算组内的拜占庭恶意节点数量为 k。客户端通过对 R 个返回结果的多集执行逐元素中位数求解，还原矩阵乘积的真实坐标值 x_{uv}。拜占庭对手则通过注入任意伪造数值，干扰客户端的结果恢复过程。

在鲁棒统计学中，估计量的崩溃点用于衡量其抵御观测值恶意损坏的能力，定义为估计量可处理任意受损观测值的最大比例。对于有限离散样本的中位数估计量，其理论崩溃点为 50%。对 R 个返回标量进行升序排序后，中位数取值位置为第$\left\lfloor\frac{R}{2}\right\rfloor+1$

位（索引从 1 开始，奇数 R 取中位值、偶数 R 取中间两数的平均值）。若恶意节点数满足阈值条件 $k \leqslant \left\lfloor \frac{R-1}{2} \right\rfloor$，即恶意节点数量严格少于总节点数的 1/2，此时诚实节点数 R-k 构成严格多数（strict majority）。

由于所有诚实节点均可稳定计算并输出一致的真实值 x_{uv}，返回值序列中真实值的出现次数不少于 R–k。由于 $R-k>\frac{R}{2}$，无论敌手注入何种噪声数值，真实值将稳定占据中位数的中心位置。因此，中位数运算可作为统计过滤机制，有效抵御拜占庭节点的数值篡改攻击。

该诚实多数阈值条件与 Makkonen[19] 在安全编码计算代数方法中提出的拜占庭错误阈值一致，二者区别在于：本文将错误约束于局部复制组内，依托统计聚合实现轻量化结果恢复；而传统鲁棒多项式编码依赖全局编码冗余与纠错译码完成目标矩阵恢复。这一诚实多数条件与 Makkonen[19] 在安全编码计算中所提的代数方法对拜占庭错误数的阈值要求具有一致性，区别在于本文将错误隔离在局部复制组内，通过统计聚合实现轻量恢复；鲁棒多项式编码通常通过全局编码冗余和纠错译码恢复目标系数。

4.2 隐私性保证

虽然冗余复制机制增加了参与数据处理的节点数量，但该复制操作不会破坏底层多项式掩码的信息隐私安全性。在基准 SDMC 协议中，矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$ 由均匀随机扰动矩阵掩蔽，使得编码份额在统计上等价于随机噪声，仅当敌手截获足量独立评估值时才存在隐私泄露风险。本文方案中，客户端为各分块对生成编码份额后，将同一掩码份额同步分发至复制组内全部的工作节点。

从信息论角度分析，即便拜占庭敌手获取了同一掩码份额的多组副本，也无法获得关于私有矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$ 的额外自由度与互信息增益。当复制组内 k 个恶意节点完全合谋、接收同源数据时，其整体信息获取能力在数学上等价于单个恶意节点。Soto[20] 在全域最优安全编码分布式计算研究中证实，分布式系统的隐私容量仅由合谋节点截获的线性独立、互不重复的多项式评估次数决定。本文冗余复制机制仅对已有编码份额进行副本复制，未在代数曲线上生成新的多项式评估点，因此可完全保留原始 SDMC 协议的全局隐私阈值 T_{global}。由此可知，在不突破原始 SDMC 全局隐私阈值的条件下，冗余复制操作不会引入新增独立多项式评估点，可完整保留原始多项式掩码的被动隐私保护性能。

4.3 计算开销与复杂度分析

通过冗余复制实现拜占庭容错会提升分布式系统的运行开销，本文从通信开销、工作节点计算开销、客户端聚合计算开销 3 个维度完成复杂度分析。在标准 SDMC 协议中，客户端向工作节点下发分块矩阵、工作节点计算后回传结果，构成了协议的基准通信复杂度。本文在各分块计算任务中引入复制因子 R 后，客户端需下发 R 组同源任务并接收 R 份结果矩阵，上下行通信链路开销随 R 呈线性增长。

在工作节点计算开销层面，为简化代数分析，假设子矩阵为方阵，单节点矩阵乘法的计算复杂度为 $O(n^3)$。由于复制组任务可并行执行，客户端视角下的矩阵乘法延迟由诚实节点的最慢返回时延决定，而系统整体计算资源消耗随复制因子 R 线性增长。客户端聚合阶段需对每个矩阵坐标的 r 个候选值求解中位数：采用常规排序算法的复杂度为 $O(r \log r)$，采用 nth_element、Quickselect 等线性选择算法的期望复杂度为 $O(r)$ 且常数因子更低，因此客户端整体聚合复杂度为 $O(n^2 r)$。

在本文 R=5、R=7 的小常数复制因子设置下，随着矩阵维度 n 持续增大，$O(n^3)$规模的矩阵乘法运算将主导整体耗时，$O(n^2 r)$客户端聚合开销占比将显著降低。复杂度分析结果表明，在复制组满足诚实多数的条件下，本文方案可实现稳定可预测的鲁棒结果恢复，通信开销与系统总计算开销均随复制因子线性增长；随着矩阵规模提升，客户端聚合运算与偏差验证的相对开销会被主体矩阵乘法运算逐步摊薄。

5 实验评估

5.1 实验环境

为系统评估本文所提面向主动敌手的容错安全分布式矩阵乘法框架，本文基于大规模软件仿真完成实验验证。仿真环境基于 Python3 搭建，依托 NumPy 实现高效张量运算，通过 Matplotlib 完成实验结果可视化。为消除随机因素引发的实验偏差，所有实验统一固定随机种子为 42，有限域实验采用 GF(2^{65537})。本文构建的仿真系统完整建模了客户端编码、聚合流程与工作节点本地计算流程，实现了全流程端到端执行，并通过多次重复实验验证了实验结果的可复现性。本次实验方案与现有编码计算领域拜占庭鲁棒性评估的主流仿真方法保持一致[8,11]。实验内容还包含偏差阈值误判与漏判分析，同时在

同等实验规模下，与同态 MAC、基于纠错码的鲁棒多项式编码方案的客户端验证与恢复开销进行对比实验。实验核心自变量包括：矩阵维度 n（由 32 倍增至 512）、复制因子 R（取值 1~10）、工作节点数量（取值 16~128，并在 100 附近加密采样）。

5.2　计算性能与规模扩展分析

为量化评估本文冗余复制机制的计算性能，本文将该方案运行耗时与基准有限域矩阵乘法方案进行对比测试。图 1 给出不同方法的运行时间与矩阵规模关系。实验结果表明，在 n 为 [32，512] 的测试区间内，两种方法的计算时间均随矩阵维度呈多项式增长，与稠密矩阵乘法 $O(n^3)$的理论复杂度特征一致。相比基准方案，本文冗余复制机制因新增任务分发与中位数聚合流程，会产生一定的额外计算开销。

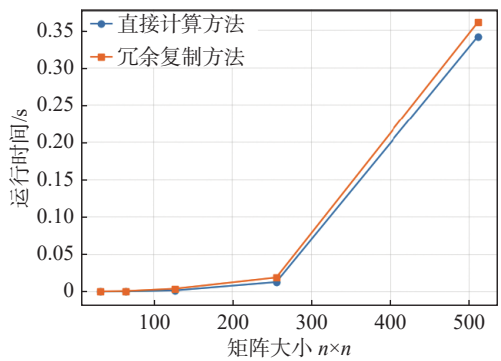

图 1　不同方法的运行时间与矩阵规模关系

Fig. 1　Runtime comparison of different methods versus matrix size

为进一步量化该开销，表 1 给出不同矩阵规模下的性能开销。由表 1 可知，小规模场景（n=32）下，基准计算开销仅为 0.000 028 s，冗余计算开销为 0.000 135 s，运行开销比为 4.86；当矩阵规模扩增至 n=512 时，基准计算开销为 0.341 497 s，冗余计算开销为 0.360 432 s，运行开销比降至 1.06。n 在 64~128 区间内的运行开销比存在小幅波动，主要源于本地 CPU 计时误差与实验重复次数的细微差异。该结果表明，当 $O(n^3)$复杂度的核心矩阵乘法占据主要耗时开销时，$O(R)$级的额外聚合开销影响被大幅弱化，验证了本文方案在大规模计算场景下的良好可扩展性。

5.3　重构成功率与容错能力分析

为验证本文方案在存在主动篡改的拜占庭攻击环境中的鲁棒性能，本文测试了不同参数配置下的矩阵重构成功率。图 2 为固定复制因子 R=5 时，不同矩阵维度对应的系统重构性能。实验结果表明，在 n 在 32~512 的全部测试场景中，系统均可实现无损正确重构。该结果充分验证了逐元素中位数聚合机制的有效性：在满足诚实多数条件的前提下，中位数算法可自动剔除投毒离群数据，且重构性能不受矩阵规模增长引发的数值波动影响。

表 1　不同矩阵规模下的性能开销

Table 1　Runtime and overhead across matrix sizes

矩阵规模	基准计算开销/s	冗余计算开销/s	运行开销比
32	0.000 028	0.000 135	4.86
64	0.000 181	0.000 538	2.97
128	0.001 427	0.003 790	2.66
256	0.012 610	0.018 696	1.48
512	0.341 497	0.360 432	1.06

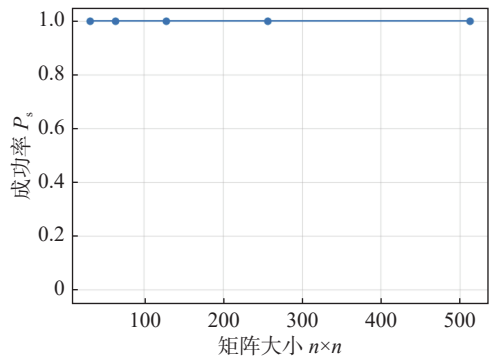

图 2　不同矩阵规模下的重构成功率

Fig. 2　Recovery rate across different matrix sizes

通过调控恶意节点数量 k，本文进一步测试了系统的临界容错阈值。如图 3 所示，当复制因子 R=5 时，若恶意节点数 k≤2，系统可实现无损重构；当 k 增大至 3 时，重构成功率直接降至 0。该阶跃式临界变化规律与本文 4.1 节推导的诚实多数定理阈值 $k \leqslant \left\lfloor \frac{R-1}{2} \right\rfloor$ 完全吻合。实验结果证实，当诚实节点结果占据数量优势时，中位数运算可精准锁定真实数值；反之，若恶意节点占据多数，将导致中位数排序位置偏移，最终引发矩阵重构失效。

在固定攻击规模 k=2 的条件下，图 4 展示了重构成功率随复制因子 R 的变化趋势。结果表明，当 R=1、R=3 时系统无法完成有效重构，当 R≥5 时重构成功率稳定维持在 1.0。该结果进一步证明，增大复制因子可有效提升系统的拜占庭容错能力。

5.4　通信开销与运行开销分析

分布式系统的安全增强通常会带来一定的性能损耗。本节通过量化通信开销与运行代价，分析本

文方案安全性与运行效率的权衡关系。

图 5 实验数据表明，系统总通信开销与复制因子 R 呈严格线性相关，与前文理论分析模型完全契合。虽然增大 R 会成倍提升网络带宽消耗，但该开销变化规律是确定的且可预测。结合前文成功率分析可得，在本文攻击场景设置下，R=5 可容忍 2 个恶意拜占庭节点，同时仅引入可控的 5 倍通信冗余开销。而 $O(R)$级冗余开销在工程应用中是完全可接受的。

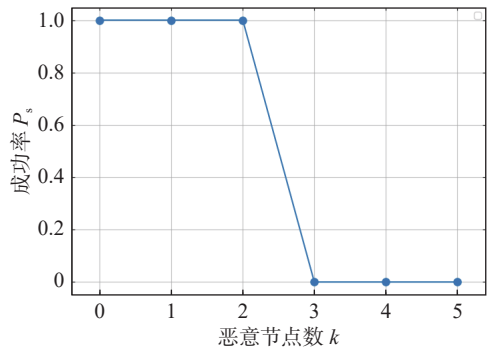

图 3 恶意节点数对重构成功率的影响

Fig. 3 Impact of malicious node count on recovery rate

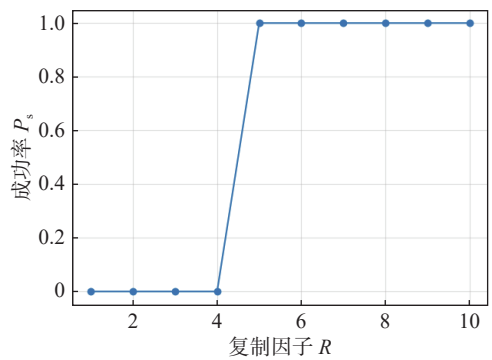

图 4 复制因子数对重构成功率的影响

Fig. 4 Impact of replication factor on recovery rate

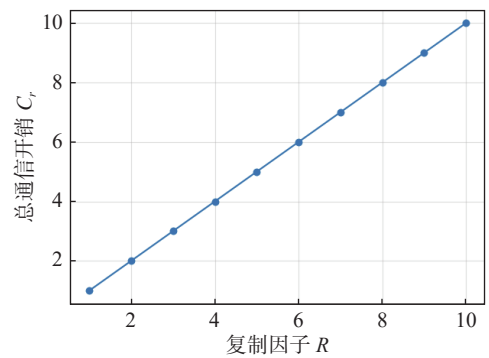

图 5 总通信开销与复制因子的关系

Fig. 5 Overall communication overhead versus replication factor

图 6 展示了运行开销比与矩阵规模的关系。由图 6 可知，随着矩阵规模增大，冗余机制引入的相对运行开销比显著降低。该结果进一步表明，在计算密集型场景下，额外的鲁棒性开销在渐近意义下趋于可忽略，充分验证了本文方法的可扩展性。

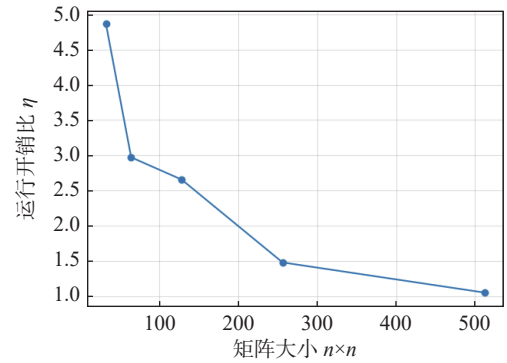

图 6 运行开销比与矩阵规模的关系

Fig. 6 Runtime overhead ratio versus matrix size

5.5 系统可扩展性分析（工作节点规模）

为评估系统在大规模分布式环境下的扩展能力，本文分析了运行时间与工作节点数量的关系。图 7 展示了不同节点规模下的系统性能变化，该模型结合并行负载分配、固定调度机制和聚合开销特征，预估 16~128 个工作节点规模下的系统运行时间，并在 90~110 节点区间内加密采样。实验结果表明，随着工作节点数量增加，单节点计算负载降低，系统整体运行时间随之减少；但节点规模达到 100 个左右时，时间下降幅度逐渐变小，表明调度开销与通信开销的占比逐步提升。该预估模型默认节点间无额外通信竞争，而真实集群运行会受网络拥塞、任务协调开销与负载抖动影响，因此系统存在最优工作节点部署规模。该现象与已有研究结论一致，如 Severinson[21] 在滞后节点分布式计算研究中证实，处理细粒度任务时，过多的并行节点会引入额外通信开销，进而抵消并行计算带来的加速收益。因此，在实际部署过程中，需在任务划分粒度与节点部署规模之间进行权衡，以保障系统最优运行性能。

5.6 偏差阈值识别与误判分析

为验证本文偏差评分机制的误判与漏判问题，本文在 n=128、R=5、k=2 的参数设置下开展 80 组重复实验，累计获取 240 组诚实节点评分与 160 组恶意节点评分，分别统计各类节点相对于中位数恢复结果的归一化 Frobenius 偏差。其评分表示为 $\delta_{i,r}=\dfrac{\|X_{i,r}-M_i\|_F}{\max(\|M_i\|_F,1)}$，其中 $X_{i,r}$ 为第 i 个分块的第 r 个副本输

出，M_i为对应的中位数恢复矩阵。阈值τ为无量纲判定阈值，当$\delta_{i,r}>\tau$时，标记该副本可疑，$\delta_{i,r}\leqslant\tau$时则不触发标记。实验攻击类型涵盖密集低幅度扰动、稀疏投毒、随机矩阵攻击与缩放矩阵攻击。如图 8 所示，诚实节点偏差为$1.77\times10^{-17}\sim2.38\times10^{-17}$，恶意节点偏差为$2.61\times10^{-7}\sim7.14\times10^{-1}$，二者存在明显的数值间隔。当阈值$\tau$取值为$1.00\times10^{-14}\sim2.54\times10^{-7}$时，系统误判率与漏判率均为 0。需要注意的是，该零误判区间上界与下一采样点3.71×10^{-7}仅间隔一个对数步长；实际部署中可在该区间内选取保守阈值，即取值于诚实节点最大偏差与恶意节点最小偏差之间、远离双侧边界的数值，推荐取值为1.00×10^{-10}。随机矩阵攻击与缩放矩阵攻击的偏差分别处于 0.69~0.71、0.49~0.51，均高于本次扫描最大阈值$\tau=0.1$，因此即便阈值提升至扫描上界，两类攻击仍可被有效检出。图 8 中后段漏判率稳定在 0.5，这是低幅度扰动与稀疏投毒攻击的漏判导致的，并非所有攻击检测机制整体失效。若攻击者采用自适应低幅度投毒策略，使输出偏差无限趋近阈值区间边界，可结合随机抽检或消息认证码验证机制提升系统安全裕度。

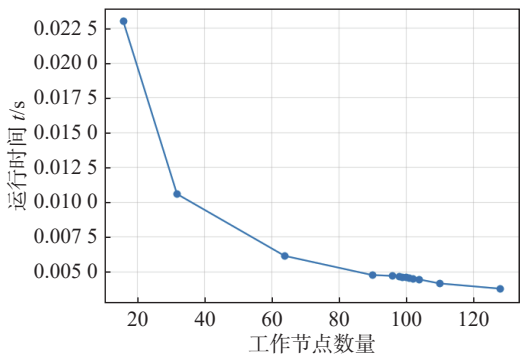

图 7　运行时间与工作节点数量关系

Fig. 7　Runtime versus number of worker nodes

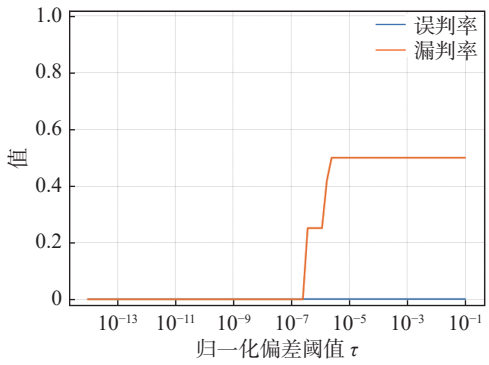

图 8　偏差阈值对误判率和漏判率的影响

Fig. 8　Impact of threshold on false positive rate and false negative rate

5.7　不同聚合策略的对比分析

本文在统一拜占庭攻击模型下，对比分析了算术平均聚合与逐元素中位数聚合两种策略的运行性能。实验结果表明，存在恶意节点干扰时，算术平均聚合方案会完全失效，无法恢复正确的矩阵乘积结果。由于算术均值的统计崩溃点为 0，单个恶意节点输出的极端数值即可造成聚合结果大幅偏移，最终引发矩阵重构失败。相比之下，中位数聚合方法具备优异的统计鲁棒性，在相同攻击条件下可有效过滤异常离群值，稳定还原真实计算结果。当恶意节点数量满足诚实多数阈值约束时，系统可稳定实现矩阵精准重构，充分验证了该方法在拜占庭攻击场景下的运行可靠性。同时，本文结合偏差度量的验证机制可精准区分诚实节点与恶意节点。实验结果表明，恶意副本相对于中位数基准结果的偏差更大，在统计分布中呈现为明显离群样本，为系统提供了无额外密码学开销的高效验证手段。

5.8　不同拜占庭容错 SDMM 方案对比

为进一步明确本文轻量化方案与现有代数、密码学容错方案的优劣势差异，本文选取同态 MAC[15]与基于纠错码的鲁棒多项式编码作为主流对照方案。

图 9 对比了矩阵规模为 128、256、512 时，各方案客户端验证与恢复阶段的代理开销，实验仅统计客户端验证、恢复流程开销，不包含工作节点矩阵乘法运算开销。本文采用复杂度等价代理模型：同态 MAC 方案通过逐元素认证标签校验近似表征客户端验证开销，鲁棒多项式编码方案通过同尺寸结果回传与密集线性译码变换近似表征客户端恢复开销。该对照模型仅保留同等纠错目标下的最小下载分片数以保证复杂度等价，未纳入 MAC 方案的密钥管理、批量认证、标签生成开销，同时省略了鲁棒多项式编码的具体编码域与实现常数，因此真实系统的绝对耗时会高于实验测试结果。

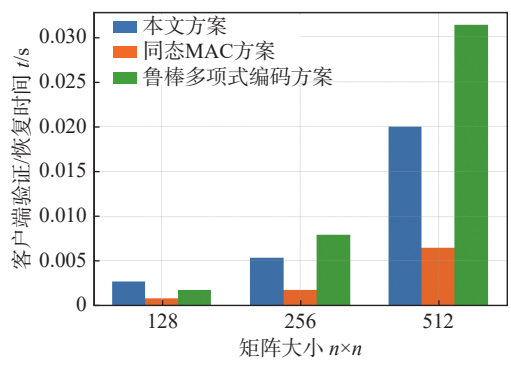

图 9　不同 SDMM 方案的客户端验证/恢复代理开销对比

Fig. 9　Comparison of client verification/recovery and proxy overheads across different SDMM schemes

本文所提“轻量化”核心定义为：无需复杂密码学证明，可将异常检测与误差纠错融合至同一运算流程，并非指代客户端纯验证耗时一定低于仅执行标签校验的 MAC 方案。中位数聚合需逐元素遍历求解，运算常数因子高于标签校验；而 MAC 方案仅侧重异常检测，识别错误后仍需任务重试或依赖足量合法副本完成结果恢复。同态 MAC 方案的优势在于强完整性检测能力，鲁棒多项式编码可依托编码冗余实现错误纠正，但存在下载冗余量大、译码复杂度高的问题。本文方案通过舍弃多数恶意节点攻击场景下的绝对容错保证，换取了实现难度低、偏差可量化、通信冗余度小的综合优势。

6 结束语

本文在基础 SDMC 框架的半诚实模型之上，构建了一种面向主动攻击的鲁棒可验证扩展方案。通过引入冗余复制计算与逐元素中位数聚合机制，系统能够在复制组满足诚实多数条件时正确恢复矩阵乘积。此外，基于 F-范数的偏差度量提供了一种轻量级统计验证方式，可在无需复杂密码学机制的情况下识别并隔离恶意节点。

后面的工作可从多个方向进一步展开：一个极具前景的方向是将本文的鲁棒统计聚合技术与基于硬件的可信执行环境相结合[22]。例如，在英特尔 SGX 等安全硬件隔离区中执行本地子矩阵乘法，有望在硬件隔离层降低工作节点主动篡改结果的风险。在其他方面，可研究自适应复制策略，以在动态攻击环境中实现安全性与系统开销间的更优权衡。此外，将该框架推广至更一般的分布式线性代数运算或联邦学习场景，也具有重要的研究价值。

参考文献：

[1] Dean J，Ghemawat S. MapReduce：simplified data processing on large clusters[J]. Commun ACM，2008，51（1）：107-113.

[2] Fan X W，Zhang Y F，Zhang T H，et al. Secure and efficient distributed matrix multiplication based on polynomial coding[C]//Proceedings of the 2025 7th International Conference on Next Generation Data-driven Networks（NGDN）. Piscataway：IEEE Press，2025：332-339.

[3] Yu Q，Maddah-Ali M，Avestimehr S. Polynomial codes：an optimal design for high-dimensional coded matrix multiplication[J]. Advances in Neural Information Processing Systems，2017，30.

[4] Mital N，Ling C，Gündüz D. Secure distributed matrix computation with discrete Fourier transform[J]. IEEE Transactions on Information Theory，2022，68（7）：4666-4680.

[5] Makkonen O，Saçıkara E，Hollanti C. Algebraic geometry codes for secure distributed matrix multiplication[J]. IEEE Transactions on Information Theory，2025，71（4）：2373-2382.

[6] Matthews G L，Soto P. Algebraic geometric rook codes for coded distributed computing[C]//Proceedings of the 2024 IEEE Information Theory Workshop（ITW）. Piscataway：IEEE Press，2024：717-722.

[7] 孙钰，刘霏霏，李大伟，等. 联邦学习拜占庭攻击与防御研究综述 [J]. 网络空间安全科学学报，2023，1（1）：17-37.
Sun Y，Liu F F，Li D W，et al. Survey on Byzantine attacks and defenses in federated learning[J]. Journal of Cybersecurity，2023，1（1）：17-37.

[8] Li S H，Ngai E C H，Voigt T. An experimental study of Byzantine-robust aggregation schemes in federated learning[J]. IEEE Transactions on Big Data，2024，10（6）：975-988.

[9] Li C X，Xiao M，Skoglund M. Coded robust aggregation for distributed learning under Byzantine attacks[J]. IEEE Transactions on Information Forensics and Security，2025，20：11636-11651.

[10] Makkonen O，Hollanti C. General framework for linear secure distributed matrix multiplication with Byzantine servers[J]. IEEE Transactions on Information Theory，2024，70（6）：3864-3877.

[11] Hofmeister C，Bitar R，Xhemrishi M，et al. Secure private and adaptive matrix multiplication beyond the singleton bound[J]. IEEE Journal on Selected Areas in Information Theory，2022，3（2）：275-285.

[12] Ghasvarianjahromi S，Yakimenka Y，Kliewer J. Decentralized sparse matrix multiplication under Byzantine attacks[J]. IEEE Transactions on Information Forensics and Security，2025，20：7333-7346.

[13] 周一可，朱友文，吴启晖. IDumbo：全流程隐私保护异步拜占庭共识协议 [J]. 网络空间安全科学学报，2025，3（2）：49-58.
Zhou Y K，Zhu Y W，Wu Q H. IDumbo：whole-process privacy-preserving asynchronous Byzantine consensus protocol[J]. Journal of Cybersecurity，2025，3（2）：49-58.

[14] Ning X. Practical secure outsourcing computation in complex cloud environments[C]//Proceedings of the 2025 2nd Interna-

tional Conference on Image Processing，Intelligent Control and Computer Engineering. New York：ACM，2025：71-77.

［15］Wu D Y，Liang B，Lu Z J，et al. Efficient secure multi-party computation for multi-dimensional arithmetics and its applications[J]. Cryptography，2025，9（3）：50.

［16］Wang J Y，Mtibaa A. CoVFeFE：collusion-resilient verifiable computing framework for resource-constrained devices at network edge[C]//Proceedings of the 2024 IEEE 13th International Conference on Cloud Networking （CloudNet）. Piscataway：IEEE Press，2024：1-9.

［17］Duan S，Zhang H，Zhao B. WaterBear: information-theoretic asynchronous BFT made practical[J/OL]. IACR Cryptology ePrint Archive, 2022: 21. https://ia.cr/2022/021.

［18］Zhu J B，Tang H X，Li S Z，et al. Generalized Lagrange coded computing：a flexible computation-communication tradeoff for resilient，secure，and private computation[J]. IEEE Transactions on Communications，2025，73（6）：4213-4227.

［19］Makkonen O. New schemes for secure distributed matrix multiplication：cooperative and analog SDMM[D]. Aalto University，2022.

［20］Soto P. Optimal secure coded distributed computation over all fields[PP/OL]. V1. arXiv （2025-04-25）[2025-12-12]. https://doi.org/10.48550/arXiv.2504.18038.

［21］Severinson L A. Straggler-resilient distributed computing[D]. Gothenburg：Chalmers University of Technology，2022.

［22］Liu T，Huang Z，Li J A，et al. SoK：opportunities for accelerating multi - party computation via trusted hardware[C]//Proceedings of the 2024 International Symposium on Secure and Private Execution Environment Design （SEED）. Piscataway：IEEE Press，2024：143-154.