隐私计算中的安全多方计算协议优化与性能评估

蒋忠群

（南宁理工学院 南宁 541006）

摘 要 随着隐私保护需求的增长，安全多方计算作为隐私计算的关键技术，受到了广泛关注。文中分析了安全多方计算协议的优化和性能评估方法，通过对计算复杂度、通信开销、执行效率及安全性增强技术的研究，提出了多种优化策略。为验证这些优化策略的有效性和实用性，设计了一系列实验，如模拟不同规模的数据集上的计算任务、对比优化前后协议的执行时间和资源消耗等。实验结果表明，优化后的安全多方计算协议不仅显著提高了计算效率，还增强了系统的整体安全性，为提高安全多方计算协议的执行效率和安全性提供了有价值的参考。

关键词： 隐私计算；安全多方计算；协议优化；计算复杂度；通信开销

中图分类号 TP309

Optimization and Performance Evaluation of Secure Multi Party Computing Protocol in Privacy Computing

JIANG Zhongqun

（Nanning Institute of Technology，Nanning 541006，China）

Abstract With the increasing demand of privacy protection, secure multi-party computing, as a key technology of federated learning, has received extensive attention. This paper analyzes the optimization and performance evaluation methods of secure multi-party computing protocols. Through in-depth research on computational complexity, communication overhead, execution efficiency and security enhancement technologies, a variety of optimization strategies are proposed. To verify the effectiveness and practicality of these optimization strategies, a series of experiments are designed, such as simulating computing tasks on datasets of different sizes, comparing the execution time and resource consumption of protocols before and after optimization, etc. The experimental results show that the optimized secure multi-party computing protocol not only significantly improves the computing efficiency, but also enhances the overall security of the system, providing a valuable reference for improving the execution efficiency and security of the secure multi-party computing protocol.

Key words Privacy computing，Secure multi-party computation，Protocol optimization，Computational complexity，Communication expenses

0 引言

随着大数据和云计算技术的快速发展，隐私保护成为数据共享与计算中的关键问题。安全多方计算（Secure Multi-Party Computation，SMPC）作为一种有效的隐私保护技术，能在多方参与下实现数据的联合计算，同时保证数据的隐私性和安全性。本文探讨了安全多方计算协议的优化技术和性能评估方法，以提高SMPC协议的执行效率和安全性，为隐私计算领域的进一步发展提供技术支持。

1 安全多方计算的基础理论

1.1 安全多方计算的定义与目标

SMPC可以在密码学的基础上对多方协同计算过程进行优化，实现了多方在不泄露各自输入数据的情况下共同执行计算任务，其核心目标是保护参与方的数据隐私安全，避免恶意参与方获取其他参与方的数据信息。SMPC技术在保证计算过程的安全性和正确性的同时，还能有效提高计算过程的透明度和计算结果的可信性。

1.2 基本协议与构建原理

SMPC通过一系列密码学技术来确保多方能在不泄露各自输入的情况下共同执行计算任务。SMPC的核心构建原理包括秘密分享、混淆电路、同态加密等技术。秘密分享技术允许将一个秘密分成多个份额，让每个参与方只持有其中的一部分，而无法单独获取完整的秘密；混淆电路技术则通过构建一个电路来执行计算，参与方可输入经过加密的秘密份额，由电路执行计算后输出加密结果，只有所有参与方解密后才能得到最终结果；同态加密技术则允许在加

作者简介：蒋忠群（1985—），本科，高级工程师，研究方向为计算机网络工程。

密数据上直接进行计算，实现数据隐私保护[1]。

2 安全多方计算协议的优化

2.1 计算复杂度优化

计算复杂度优化可以在计算过程中减少时间和资源的消耗。相较于传统的RSA加密方法，高效密码学（如基于椭圆曲线密码学的同态加密技术）可大大减小密钥大小，减少计算量。对秘密分享方案进行改进，如采用阈值秘密分享技术，在减少秘密份额数量的同时，降低计算复杂度。利用同态加密技术的特性，可以在加密数据上直接进行计算，避免频繁的解密与加密操作，降低计算复杂度。将SMPC协议引入并行计算机制，可以在分布式计算框架下将计算任务分解到多个节点上同时执行，从而提高计算效率；对于特定的场景，需要定制SMPC协议，去掉不必要的计算步骤，减少冗余操作，以降低计算的复杂度；在实际计算之前，还需要进行预处理，生成所需的加密材料和秘密份额，以降低计算负担[2]。通过这种方式，可以在多个节点上同时执行计算任务，在提高计算效率的基础上满足安全性要求。

2.2 通信开销优化

在安全多方计算协议中，可以采用如图1所示的方法来降低通信开销。采用Hofmann编码或LZ77等高效的数据压缩算法，可以降低数据量；采用批量加密技术来减少加密次数，如将多个消息打包成更大的消息块，可以实现加密传输，降低由于加密操作而产生的额外通信支出；将通信路径优化到网络层面，在数据传输中选择最短路径或最小延时路径，可以降低网络延迟。通过控制数据包在网络中的跳数来降低传输延迟和丢包率（利用优化路由协议实现），可以利用中间节点缓存数据，减少重复数据的传递，在经常需要分享数据的场景下较为适用。在多方参与的场景中，可只向需要数据的参加者传送数据，而不向全体参加者广播数据，以减少不必要的数据传送[3]。采用多广播技术，可以将数据同时发送给多个接收方，减少数据的复制和转发，有效降低网络通信的成本。在设计SMPC协议时，交互轮次应最小化，在线阶段的通信次数则应以预先计算、离线处理等方式实现最小化。

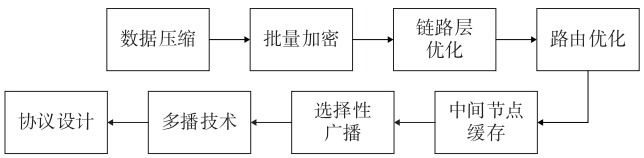

图1 通信开销优化方法

2.3 执行效率优化

（1）提高协议性能的关键是优化执行效率，将计算任务分解到多个处理器或计算节点上同时执行，以提高计算速度。例如，可以将计算任务分解成若干个子任务，每个子任务可以并行执行在不同的计算节点上，以节省计算时间。（2）自定义的SMPC协议可用于特定的应用场景，去除不必要的计算步骤，减少冗余操作，降低计算复杂度。例如，针对特定类型的计算任务，为减少不必要的加解密操作，可以设计特殊的协议，对数据进行预处理后再实施运算，降低计算量。（3）预处理技术能提升数据质量，显著提高计算效率。另外，可以减少内存存取次数，并通过优化数据结构来提升数据处理速度。例如，使用哈希表格数据结构，可以提高数据的查找速度和任务执行效率。（4）采用高效算法，减少运算步骤，提高运算速度[4]。例如，在SMPC协议中，快速傅里叶变换（FastFourierTransform，FFT）可以用于加速多项式乘法，从而提高协议的执行效率。（5）利用特殊硬件，如GPU或TPU，提升特定类型的计算任务的执行效率。

2.4 安全性增强技术

在安全多方计算协议中，为确保协议的安全性，可以利用秘密分享方案来确保敏感数据的安全性。秘密分享方案可以将秘密信息分散成多个份额，只有当足够多的份额聚合时才能重构原始的秘密信息。例如，使用Shamir的秘密分享方案，可以将秘密s编码成多项式的系数，如式（1）所示：

$$f(x)=s+\sum_{i=1}^{t-1}a_i x^i \tag{1}$$

其中，a_i可随机选择，t是阈值。每个参与者i将获得$f(i)$作为其份额。只有当至少t个份额被聚合时，秘密s才能被重构。

使用零知识证明技术来验证计算过程的正确性，同时不泄露任何额外的信息。零知识证明可以让一方（证明者）向另一方（验证者）证明一个陈述是真的，而不需要透露任何除结果之外的信息。例如，使用基于∑协议的零知识证明来验证一个秘密份额的有效性，可以确保秘密份额的正确性，同时不会泄露份额的具体值。还可以采用同态加密技术来保护计算过程的安全性。同态加密允许在加密数据上直接进行计算，而无需解密数据。例如，使用Paillier加密体制，可以实现加法同态性，即如果$E(a)$和$E(b)$分别是a和b的加密形式，如式（2）所示：

$$E(a)\cdot E(b)=E(a+b) \tag{2}$$

利用特定的机制来检测并惩罚恶意行为，如使用信誉系统或经济激励机制来鼓励所有参与者作出真实行为[5]。例如，可以设计一个惩罚函数P，当检测到某参与方i发送了错误的份额s'_i时，即可对该参与方实施惩罚（惩罚力度可以根据错误行为的严重程度调整）。

3 安全多方计算协议的性能评估

3.1 性能评估指标与方法

在安全多方计算协议的性能评估中，关键指标包括计算时间、通信量、存储需求和安全性，评估方式一般涉及理论分析和实际检验。其中，理论分析用于推导协议的时间复杂度和空间复杂度，而实际测试则通过模拟或在真实环

境下的实验来验证协议的实际性能。

3.2 评估工具与实验方法

3.2.1 模拟工具与仿真环境

仿真工具和仿真环境是安全多方计算协议性能考核中必不可少的工具。这些工具能在不同场景下评估协议的性能表现，提供一个可控的环境来模拟协议的执行过程。常用的模拟工具包括编程语言中的模拟框架，如Simulink、MATLAB和Python。模拟环境则需要通过模拟真实的网络延迟、丢包率等因素，构建一个类似于实际应用的网络环境，以便对协议的性能进行精确的评估。

3.2.2 实验过程

实验过程如图2所示。(1)搭建一个模拟或真实的网络环境，确保与实际应用场景相似。(2)根据评估指标的需求配置相应的实验参数，如参与方数量、数据规模等。(3)执行SMPC协议，并记录关键数据，如计算时间、通信量等。(4)对收集到的数据进行统计分析，以评估协议的实际性能。

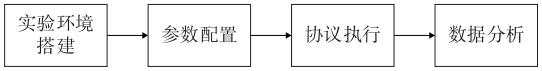

图2 实验过程

3.3 安全多方计算协议的性能评估

评估结果显示，参与方数量和数据规模对安全多方计算协议的性能具有显著影响，具体如表1所列。在参与方数量为3时，随着数据规模从100 KB增加到200 KB，计算时间从15.2 s增加到18.3 s，通信量从456 KB增加到520 KB，存储需求从2.1 MB增加到2.3 MB。当参与方数量增加到5时，在100 KB数据规模下，计算时间减少到了13.5 s，通信量减少到了430 KB，存储需求减少到了1.9 MB。然而，当数据规模增加到200 KB时，计算时间增加到了21.4 s，通信量增加到了580 KB，存储需求增加到了2.6 MB。安全性评估显示，在数据规模为100 KB时，无论是3个还是5个参与方，安全性评估均为“高”，而在数据规模为200 KB时，安全性评估降为“中”。

表1 安全多方计算协议的性能评估结果

参与方数量	数据规模/KB	计算时间/秒	通信量/KB	存储需求/MB	安全性评估
3	100	15.2	456	2.1	高
3	200	18.3	520	2.3	中
5	100	13.5	430	1.9	高
5	200	21.4	580	2.6	中

4 结语

合理地对SMPC协议进行优化，可以得到明显的性能提升，特别在计算时间、通信体、和存储需求等方面。未来，该领域的研究会着重于进一步提高SMPC协议的安全性和效率，探索更高效的数据处理方法和技术，以进一步提高协议性能。

参考文献

[1] 张茹，易鑫，樊玲，等.量子安全多方计算协议研究进展[J].中央民族大学学报(自然科学版)，2024，33(1)：46-53.

[2] 孙帆，雷旭，李存华.一种基于安全多方计算的边缘学习协议[J].江苏海洋大学学报(自然科学版)，2023，32(4)：84-89.

[3] 涂航.基于全同态加密的安全多方计算协议[J].通信技术，2021，54(12)：2674-2678.

[4] 徐秋亮，蒋瀚，赵圣楠.安全多方计算关键技术：茫然传输协议[J].山东大学学报(理学版)，2021，56(10)：61-71.

[5] 朱宗武，黄汝维.基于高效全同态加密的安全多方计算协议[J].计算机科学，2022，49(11)：345-350.