Pre-Proposal

Edited by
陈　昊 PB20051077
牛午甲 PB20111656
潘云石 PB20111657
石磊鑫 PB20111658
孙霄鹃 PB20111659

基于安全多方计算的理论机制以及应用场景的调研

- 研究动机
  随着网络和信息技术的不断普及，人类产生的数据量正在呈指数级增长，其中自然会有大规模数据量和计算量的任务：例如人们通过分布式计算尤其是云计算技术，实现数据的共享。与此同时，由于数据安全问题时有发生，人们对数据隐私保护的需求日渐显现，这无疑降低了不同实体间共享数据的可能性，导致数据难以共享，形成“数据孤岛”。安全多方计算融合了密码学和分布式计算技术，是信息安全领域的一个重要研究方向,具有重要的研究价值和意义。本次调研致力于对安全多方计算的理论机制进行梳理总结，并就一些实际的应用场景进行总结与改进。
- 技术挑战
  - 加密会带来额外计算开销：SMPC算法通常需要高计算资源，特别是对于涉及大型数据集或复杂计算的任务。另外，参与者数量会影响其性能，参与者数量的增加会大大增加计算过程中的开销。
  - 难以抵御恶意攻击：威胁模型定义了SMPC协议应该承受的各种攻击类型。例如，恶意参与者可能试图从计算中学习更多信息，试图操纵输出结果。此外，可信第三方可能不诚实，可能违背参与者的利益。
- 可能的解决方案
  - 使用并行计算，使用数据分区等技术减少通信开销以及预处理输入数据。此外，使用硬件和云计算技术。
  - 通过压缩技术或减少数据中的冗余、设计SMPC协议时考虑资源效率因素以最小化计算过程所需的资源量。
  - 形式化地描述威胁模型，并分析SMPC协议在不同攻击情况下的安全性。
- 调研计划
  - 前置知识准备
    - 姚氏混淆电路
    - 不经意传输

        - 同态加密
        - 零知识证明
        - ……
    - SMPC SOTA methods调研
    - 应用场景
        - 百万富翁问题
        - 基于安全多方计算的机器学习
        - ……