周报

2025-09-22

本周研究摘要

- ML-DSA 介绍写作
- 基金申请书研究方案设计：构建分组密码实现技术与性能评估研究的四大研究方向综合技术框架

ML-DSA 介绍写作

核心算法:

- ML-DSA 三大核心算法规范化：密钥生成、签名生成、签名验证算法的完整形式化
- ML-DSA 参数集合与安全性能分析框架：ML-DSA-44、ML-DSA-65、ML-DSA-87 三套完整参数集合技术规范

模学习理论与计算复杂度分析:

- 建立模学习困难问题(MLWE)和模短整数解问题(MSIS)的背景
- 集成多项式环运算和数论变换(NTT)优化技术的分析

基金申请书研究方案设计

四大核心研究方向架构设计:

- 研究方向一：分组密码的硬件实现技术研究(FPGA、ASIC 平台优化)
- 研究方向二：分组密码的软件实现技术研究(通用处理器和嵌入式系统)
- 研究方向三：分组密码的软硬件协同设计研究
- 研究方向四：跨平台分组密码性能评估系统构建

总结

下周计划

- 继续深化 ML-DSA 论文技术内容：重点完善 IoT 环境部署优化策略分析
- 开展 ML-DSA 实验验证框架设计：准备性能基准测试环境搭建

老师评语

优先推进论文完稿

抓紧论文进度

《分组密码实现技术与性能评估研究》 基金这个题目你内容写得再好也不行，项目申报你找 1-2 个同学（包括研 2 也可以）开会研究确定：题目、4 个研究内容我们再定

已与岳兴起和谢抗同学讨论