周报 - 第四篇论文和 ML-DSA 实现

2025-09-16

本周研究摘要

本周完成第四篇论文重构工作和 ML-DSA 密码第一阶段完整实现：

- 第四篇论文系统性重构：引用部分深度重构，相关工作章节扩展完善，ARM Cortex-M4 性能分析框架确立
- ML-DSA 基础层全部核心组件完成：域运算、多项式编码、数论变换等关键算法模块实现

第四篇论文撰写进展

论文结构优化与重构工作:

- 引用部分深度重构：全面覆盖资源受限 MQTT 环境中 ML-DSA 数字签名方案
- 相关工作章节扩展：增加后量子密码学在 IoT 环境中的详细性能分析

ARM Cortex-M4 性能分析框架:

- 确立以 ARM Cortex-M4 为核心的性能分析框架
- 针对资源受限 IoT 设备的特殊需求专门设计

研究空白识别与技术路径

关键研究空白识别:

- 现有研究主要集中在高性能计算平台
- 资源严重受限 IoT 设备的专门优化研究相对缺乏

技术路径规划:

- 算法优化维度
- 内存管理维度
- 功耗控制维度

ML-DSA 密码实现进展

第一阶段基础层架构完成:

- 完整的密码学基础设施框架构建
- 标准化接口规范建立

核心组件全面实现:

- 域运算与编码框架基础设施
- 多项式、向量、NTT 相关数据类型
- Barrett 约简算法高效模运算

基础层核心组件详解

Phase 1.1 基础工具组件:

- Truncate trait：安全整数截断功能
- Flatten/Unflatten trait：数组转换功能

Phase 1.2-1.3 域运算框架:

- Field trait + Barrett 约简算法
- 完整类型系统：Polynomial, Vector, NTT 系列
- define_field!宏标准化接口

总结

下周计划

- 第四篇论文撰写工作
- ML-DSA 第二阶段 开展核心算法层开发，实现 ML-DSA 密钥生成、签名和验证算法

老师评语

摘要里一定要体现是怎么做的，而不只是要做的结果，即要体现主要技术创新细节

论文主要技术创新确定后，对摘要进行补充完善