周报

2025-12-29

本周研究摘要

完成 ML-DSA 论文核心技术贡献扩展

新增 Adaptive Security Level Selection Protocol 章节

Adaptive Protocol 设计

协议核心：根据消息关键性、设备资源状态动态选择 ML-DSA 参数集

设计原则：

- Message Criticality Classification：按安全敏感度分类消息
- Minimum Security Guarantees：强制每类消息最低安全级别

自适应选择算法

选择逻辑：

- $R \geq 0.7$：使用默认安全级别
- $0.4 \leq R < 0.7$：触发一级降级
- $R < 0.4$：选择最低安全级别
- Critical 消息始终使用 ML-DSA-87

协议开销：23–38 μs/消息（占 ML-DSA-44 签名延迟 $< 0.006\%$）

总结

下周计划

- **1月5日(周一)博士复试**

老师评语

全力准备好博士考试，特别去问下上一届的如何考

全力准备