周报

2025-10-13

本周研究摘要

- ARM Cortex-M4 性能评估体系建立
- 实验环境部署：STM32 配置完成，pqm4/MQTT 集成中

实验平台

硬件：STM32F407VG(168MHz Cortex-M4F、1MB Flash、192KB SRAM)

密码学库：pqm4(ML-DSA-44/65/87) + micro-ecc(ECDSA P-256 对比基准)

通信：Paho MQTT 客户端 + ESP32 WiFi

测量与评估方法

性能测量：DWT_CYCCNT 单周期精度 + 栈水印内存剖析 + INA219 能耗

基准测试：密钥生成/签名/验证 × 10/50/100 字节载荷 × 1000 次迭代

评估指标：计算性能(周期/时间) + 内存(Flash/RAM/栈) + 协议开销

对比分析：R = M{ML-DSA} / M{ECDSA}

MQTT 端到端认证

认证流程：发布者签名 → MQTT 传输 → 订阅者验证

延迟测量：签名生成→消息传输→网络传播→代理路由→签名验证

QoS 测试：评估 QoS 0/1/2 三级别的协议开销特征

实验环境进展

已完成:

- STM32 硬件验证(ST-Link + 串口) + 工具链(ARM GCC + OpenOCD)
- pqm4 源码分析与核心模块识别

进行中:

- pqm4 移植(HAL 适配、RNG 对接、DWT 配置)
- MQTT 集成(Paho 客户端 + ESP32-STM32 UART 方案)

总结与下周计划

下周计划

pqm4 移植：完成 ARM Cortex-M4 平台适配与功能验证

基准测试：采集密钥生成/签名/验证性能基线数据

MQTT 原型：实现载荷签名系统，测量协议级传输开销

老师评语

注意理论上的写作提升，包括形式化、推导证明等，不要写成纯工程性论文

算法实现优化部分 添加理论分析