周报

2025-11-10

本周研究摘要

完成 ML-DSA 算法在 IoT MQTT 环境中的完整实验工作

- 计算性能评估：密钥生成、签名生成与验证性能量化
- 内存利用分析：静态 Flash 与动态 SRAM 需求评估
- 协议级开销测试：消息大小、端到端延迟与吞吐量

测试平台：ARM Cortex-M4 微控制器（168 MHz）

参数集：ML-DSA-44、ML-DSA-65、ML-DSA-87

计算性能数据收集

密钥生成性能：

- ML-DSA-44：151.0ms（100.7 倍开销 vs ECDSA 1.50ms）
- ML-DSA-65/87：249.0ms/357.0ms（166-238 倍开销）

签名生成性能（主要瓶颈）：

- ML-DSA-44：657.0ms（71.5 倍开销 vs ECDSA 9.19ms）

签名验证性能：

- ML-DSA-44：416.0ms（26.0 倍开销 vs ECDSA 16.00ms）

关键发现：性能主要取决于核心密码学操作

内存利用数据收集

静态内存（Flash）：

- ECDSA：9.7 KB
- ML-DSA-44：37.2 KB（3.8 倍开销）

动态内存（SRAM）：

- ECDSA：2.1 KB
- ML-DSA-44：22.7 KB（10.8 倍开销）

关键约束：接近/超过 Cortex-M4 SRAM 容量限制（64-128 KB）

协议级开销数据收集

MQTT 消息大小：

- ECDSA 10 字节载荷：82 字节（4.6 倍）
- ML-DSA-44 10 字节载荷：2,438 字节（135.4 倍）
- ML-DSA-65/87：3,327/4,645 字节（185-258 倍）

端到端延迟（50 字节载荷）：

- ECDSA：54.1ms
- ML-DSA-44：1,114.2ms（20.6 倍开销）

关键发现：签名生成构成主要性能瓶颈

总结

下周计划

论文写作完善工作:

1. 优化方法章节的技术细节 突出创新性贡献
2. 进行论文全文的学术化审查和语言优化

老师评语

Hengyang Normal University, College of Computer Science and Technology, Hengyang, China 就上面这个顺序都是错的，一定要注意细节，细节决定成败！即使投会议，论文语言始终要直接简洁，不要过多冗余和科普，论文本来就是写给领域专家看的

已按最新一期 CHES 论文修改好单位