周报 向嘉豪(2026-02-02)

摘要: 本周完成硕士学位论文第四章面向 32 位处理器的 SPN 密码比特切片低延迟实现的撰写工作，系统阐述了比特切片 SPN 密码的理论基础、线性层与非线性层优化方法，以及 AES 和 QARMAv2 密码的优化实现与性能评估。同时对第四篇小论文进行结构调整，删除了自适应安全级别选择协议相关内容，补充了 MQTT 后量子迁移的相关文献综述，使论文聚焦于 ML-DSA 性能基准测试与 MQTT 集成评估。

下周计划: 1) 修改第四篇小论文 2) 完成硕士学位论文第五章的撰写工作

1 硕士学位论文撰写

1.1 第四章面向 32 位处理器的 SPN 密码比特切片低延迟实现

完成了第四章面向 32 位处理器的 SPN 密码比特切片低延迟实现的撰写工作，该章节共 532 行，包括比特切片 SPN 密码的理论基础、线性层与非线性层优化方法、AES 与 QARMAv2 密码的优化实现三个主要部分。本章针对 32 位处理器架构的限制，提出了置换优化算法（OPO）和改进的比特切片门复杂度（BGC）模型编码方法，在 ARM Cortex-M 和 Xtensa LX 处理器上实现了密码的高效实现。

比特切片 SPN 密码的理论基础部分详细描述了比特切片技术的核心原理，包括将密码组件映射到二进制域中的位级操作。该部分建立了线性层和非线性层的形式化表示方法，定义了线性变换矩阵和 S 盒变换的代数标准形式（ANF）。以 QARMAv2 密码为例，说明了 64 位分组如何被分割为 16 个 4 位小空间，每个小空间由四个寄存器表示。

线性层与非线性层优化方法部分提出了两种核心优化技术。基于置换分解的线性层优化引入了置换原语操作（PPO）的形式框架，通过掩码合并性质和移位分解性质将 QARMAv2 的置换操作从 14 个 PPO 减少到 5 个，实现 64.3% 的指令减少。基于 BGC 模型的 S 盒优化采用代数标准形式简化约束函数，相比现有方法实现 11.7%–86.1% 的求解时间减少，平均加速 3.19 倍。

2 第四篇小论文修订

完成了第四篇小论文的结构调整与内容修订工作。删除了自适应安全级别选择协议（Adaptive Security Level Selection Protocol）相关的全部内容，包括设计原理、消息关键性分类、资源状态评估、安全性分析等小节，以及相关的实验评估部分（工作负载配置、开销减少、能耗节省、安全级别分布、协议开销评估）。论文贡献从三项调整为两项：性能基准测试（Performance Benchmarking）和 MQTT 集成评估（MQTT Integration Assessment）。

补充了 MQTT 后量子迁移的相关文献综述，新增了 Samandari 和 Gritti 关于 MQTT 中 Dilithium 后量子认证的延迟与负载扩展分析，Rampazzo 和 Henriques 关于 MQTT 混合后量子开销的量化研究，以及 Cho 等人关于大规模流量检测中量子就绪性滞后的观察。同时引用了 Kampanakis 和 Sikeridis 关于 TLS 和 SSH 中握手延迟与证书大小开销的性能研究，这些文献为 IoT 约束环境下的协议级开销提供了更全面的背景支撑。