周报

2026-02-03

本周研究摘要

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撰写

对第四篇小论文进行结构调整，删除自适应协议内容，补充 MQTT 后量子迁移文献

第四章比特切片 SPN 密码理论基础

针对 32 位处理器架构限制，提出置换优化算法（OPO）和改进的 BGC 模型编码方法

- 比特切片技术：将密码组件映射到位级操作，建立线性层和非线性层形式化表示
- 64 位分组分割为 16 个 4 位小空间，每个小空间由四个寄存器表示
- 在 ARM Cortex-M 和 Xtensa LX 处理器上实现高效实现

线性层与非线性层优化

基于置换分解的线性层优化引入置换原语操作（PPO）形式框架

- 线性层：通过掩码合并与移位分解，QARMAv2 置换从 14 个 PPO 减少到 5 个，指令减少 64.3%
- 非线性层：基于 BGC 模型的 S 盒优化采用 ANF 简化约束函数
- 求解时间较现有方法减少 11.7%–86.1%，平均加速 3.19 倍

第四篇小论文修订

删除自适应安全级别选择协议相关全部内容

- 论文贡献从三项调整为两项：性能基准测试与 MQTT 集成评估
- 删除内容：设计原理、消息关键性分类、资源状态评估、实验评估等

补充 MQTT 后量子迁移相关文献综述

- 新增 Dilithium 后量子认证延迟分析、MQTT 混合后量子开销量化等文献

总结

下周计划

- 修改第四篇小论文
- 完成硕士学位论文第五章的撰写工作

老师评语

我上周跟你说的页数过少，你在本次工作报告没提？也没进行相应增加，有什么想法？

第四篇小论文经重新审视后，发现自适应安全级别选择协议的创新性不足——其本质为基于阈值的参数配置策略，缺乏形式化模型与新颖性，难以支撑发表。因此删除该部分内容，并通过补充 MQTT 后量子迁移文献综述来充实论文。页数将在后续修订中随新内容补充而增加。