周报 向嘉豪(2025-11-03)

摘要: 本周主要完成了第四篇论文关于后量子密码学的核心撰写工作。系统性地完成了论文摘要的学术化改进、方法论章节的全面优化以及结果章节框架的构建。通过将论文叙述从第一人称转换为第三人称视角，显著提升了学术论文的客观性和专业性。创建了包含计算性能分析、内存利用分析和协议级开销评估的三个核心结果表格框架，为后续实验数据的系统化呈现奠定了坚实基础。

下周计划:
1. 完成 ML-DSA 在 IoT MQTT 环境中的完整实验工作
2. 收集并填充结果表格所需的定量实验数据

1 论文撰写工作

1.1 摘要和方法论章节优化

本周完成了论文摘要和方法论章节的全面学术化改进工作。摘要部分的核心优化集中在将叙述视角从第一人称（“Our methodology”、“We analyze”）转换为第三人称学术视角（“The methodology”、“Analysis examines”），这一转变显著增强了论文的客观性和学术规范性。通过系统性地审视每个技术声明的表述方式，确保了摘要部分既保持了技术准确性，又符合高水平学术期刊的写作标准。

方法论章节的改进工作同样遵循了第三人称学术视角的转换原则。实验平台描述从“Our experimental platform”改为“The experimental platform”，确保了方法论叙述的客观性。软件环境、评估协议和基准测试设计的描述得到了系统性的优化，技术术语的使用更加精确，章节内部的逻辑转换更加流畅。集成测试协议的描述经过细化，清晰地呈现了实验设计的科学性和可重复性。

1.2 结果章节框架构建

完成了结果章节的完整框架设计和表格结构创建工作。建立了三个核心分析维度的表格框架，系统化地组织未来的实验数据呈现。计算性能分析表格涵盖了密钥生成（keygen）、签名生成（signature generation）和签名验证（signature verification）三个关键操作的性能指标，为量化 ML-DSA 算法在 IoT 设备上的计算效率提供了结构化框架。

内存利用分析表格设计包含了静态内存需求和动态内存需求两个重要维度，这对于资源受限的 IoT 设备部署场景具有关键意义。协议级开销评估表格则聚焦于 MQTT 协议环境中的实际应用影响，包括消息大小、传输延迟和吞吐量等关键网络性能指标。这一系统化的结果呈现框架确保了实验数据的全面性和可比性，为论文的技术贡献提供了清晰的量化证据结构。

2 实验工作进展

实验工作目前处于推进阶段，已完成实验环境的准备和测试框架的建立。ML-DSA 算法在 IoT 设备上的部署测试平台已经搭建完成，MQTT 协议的集成测试环境配置就绪。后续工作将聚焦于系统化地收集三个核心维度的实验数据，包括计算性能指标、内存利用数据和协议级网络性能测量。实验数据的收集将严格遵循已建立的评估协议，确保结果的科学性和可重复性。完整的实验执行和数据分析工作计划在下周完成，为论文结果章节提供充分的定量证据支持。