周报 向嘉豪(2025-09-15)

摘要: 本周完成第四篇论文重构工作和 ML-DSA 密码第一阶段完整实现。论文方面：重构引用部分以全面涵盖资源受限 MQTT 环境中的 ML-DSA 数字签名方案，扩展相关工作章节并完善 IoT 后量子密码性能分析，识别关键研究空白。代码实现方面：完成 ML-DSA 基础层全部核心组件，包括域运算、多项式编码、数论变换等关键算法模块。

下周计划: 1) 继续第四篇论文的撰写工作。 2) 开展 ML-DSA 第二阶段核心算法层开发，实现 ML-DSA 密钥生成、签名和验证算法。

1 第四篇论文撰写进展

1.1 论文结构优化与重构工作

本周针对第四篇论文进行了系统性的结构优化和内容重构工作。重构工作主要聚焦于资源受限 MQTT 环境中 ML-DSA 数字签名方案的理论框架完善和技术路径清晰化，确保研究内容与当前后量子密码学发展趋势保持高度一致。

引用部分深度重构 对论文抽象进行了全面重构，确保内容清晰且全面覆盖了资源受限 MQTT 环境中 ML-DSA 数字签名的核心技术贡献。重构后的抽象更加精确地阐述了研究问题的关键性、技术方案的创新性以及实验验证的系统性。通过优化技术术语表述和逻辑关系梳理，使引用部分能够准确传达研究工作在后量子 IoT 安全领域的重要价值。

相关工作章节扩展与完善 系统性扩展了相关工作章节，增加了后量子密码学在 IoT 环境中的详细性能分析内容。该章节的扩展工作重点关注了现有研究在资源受限设备上的技术局限性，以及 ML-DSA 算法在 MQTT 协议环境下的适用性分析。通过对比研究和技术 gap 分析，为本研究的创新点提供了坚实的理论基础和技术背景支撑。

1.2 ARM Cortex-M4 性能分析框架

确立了以 ARM Cortex-M4 微控制器为核心的性能分析框架，该框架针对资源受限 IoT 设备的特殊需求进行了专门设计。ARM Cortex-M4 作为典型的 IoT 边缘计算平台，其 32 位架构和有限的计算资源为 ML-DSA 算法的高效实现提出了严峻挑战。性能分析框架的建立为后续实验设计和技术验证提供了标准化的评估基础。

研究空白识别与技术路径规划 通过文献调研和技术分析，明确识别了后量子 IoT 部署领域的关键研究空白。当前研究主要集中在高性能计算平台上的后量子算法实现，而针对资源严重受限的 IoT 设备的专门优化研究相对缺乏。基于这一 gap 分析，制定了涵盖算法优化、内存管理、功耗控制等多维度的技术路径规划。

2 ML-DSA-RS 密码库实现进展

2.1 第一阶段基础层架构完成

本周完成了 ML-DSA 密码库第一阶段基础层的全部核心组件实现工作。成功构建了完整的密码学基础设施框架。该阶段的实现工作为后续 ML-DSA 核心算法的开发提供了稳固的技术基础和标准化的接口规范。

Phase 1.1 基础工具组件实现 完成了 module_lattice/util.rs 中的核心工具组件开发，实现了 Truncate、Flatten 和 Unflatten 三个关键 trait。Truncate trait 提供了安全的整数截断功能并包含 unsafe 优化实现，确保了在保证内存安全的前提下实现最优性能。Flatten trait 实现了嵌套数组到平坦数组的高效转换，Unflatten trait 则提供了逆向的数组分割功能。所有工具组件均通过了完整的测试验证(7/7 测试全部通过)。

Phase 1.2-1.3 域运算与编码框架 系统性实现了完整的域运算和编码框架基础设施。Field trait 采用 Barrett 约简算法实现了高效的模运算功能，Elem 结构体封装了域元素的所有算术操作。构建了涵盖 Polynomial、Vector、NttPolynomial、NttVector、NttMatrix 等核心数据类型的完整类型系统。define_field!宏提供了创建具体域实现的标准化接口，ArraySize trait 结合 typenum 实现了编译时大小验证机制。

FIPS 标准编码算法支持 实现了符合 FIPS 203/204 标准的 SimpleBitPack 编码算法支持。EncodingSize trait 提供了位级多项式编码/解码功能，VectorEncodingSize trait 实现了向量编码并集成了 flatten/unflatten 操作。编码框架支持完整的往返编码/解码测试验证，确保了数据完整性和算法正确性。所有第一阶段基础层任务已全面完成，为第二阶段核心算法开发奠定了坚实基础。