周报 向嘉豪(2025-09-22)

摘要: 本周完成 ML-DSA 算法深度重构与基金申请书撰写两项重要工作。论文方面：完成 ML-DSA 算法介绍，实现密钥生成、签名生成、签名验证三大核心算法的完整形式化规范，集成 ML-DSA 参数集合与计算复杂度分析框架。基金申请方面：完成“分组密码实现技术与性能评估研究”基金申请介绍文档，构建涵盖硬件实现、软件实现、协同设计、性能评估四大研究方向的综合技术框架。

下周计划: 1) 继续深化 ML-DSA 论文技术内容，重点完善 IoT 环境部署优化策略分析。 2) 开展 ML-DSA 实验验证框架设计，准备性能基准测试环境搭建。

1 ML-DSA 深度论文重构进展

1.1 核心算法规范完整化实现

本周针对 ML-DSA 深度论文进行了系统性的算法规范化重构工作，实现了从理论框架到技术实现的全面规范化文档建设。重构工作聚焦于 FIPS 204 标准 ML-DSA 算法的完整技术规范建立，确保论文内容与国际标准保持严格一致性，为后续 IoT 环境优化分析提供权威技术基础。

ML-DSA 三大核心算法完整规范化 完成了 ML-DSA 算法体系的三大核心算法完整形式化规范建设。算法 1 实现了 ML-DSA 密钥生成算法的完整规范，涵盖种子扩展、矩阵生成、秘密向量采样等关键步骤。算法 2 建立了签名生成算法的详细技术流程，包括随机性生成、承诺计算、挑战生成、响应计算等核心操作。算法 3 构建了签名验证算法的完整验证框架，实现承诺重构、挑战验证、范围检查等关键验证步骤。所有算法规范均采用严格的数学记号体系和标准化的伪代码表示。

ML-DSA 参数集合与安全性能分析框架 系统性集成了 ML-DSA-44、ML-DSA-65、ML-DSA-87 三套完整参数集合的技术规范。建立了涵盖安全级别、密钥长度、签名长度、计算复杂度等多维度的性能评估框架。ML-DSA-44 面向 128 位安全级别的轻量化应用场景，ML-DSA-65 提供 192 位安全级别的平衡型解决方案，ML-DSA-87 实现 256 位安全级别的高安全性保障。参数集合分析为 IoT 环境的算法选择和性能优化提供了量化的决策支持基础。

模学习理论与计算复杂度分析 完成了 ML-DSA 算法数学基础理论的介绍工作。建立了模学习困难问题(MLWE)和模短整数解问题(MSIS)的完整理论框架，为 ML-DSA 算法的安全性分析提供了坚实的数学理论基础。集成了多项式环运算和数论变换(NTT)优化技术的详细分析，重点关注资源受限环境下的计算效率优化策略。理论分析涵盖了时间复杂度、空间复杂度、通信复杂度等多维度的性能指标评估。

2 基金申请书研究方案设计

2.1 分组密码研究框架总体设计

完成了“分组密码实现技术与性能评估研究”基金申请书的研究框架总体设计工作。该研究框架针对分组密码算法在多平台环境下的实现技术和性能评估问题，构建了涵盖理论研究、技术开发、系统集成、评估验证等多层次的综合研究体系。研究框架的建立为分组密码技术的深入研究和产业化应用提供了系统性的技术路径。

四大核心研究方向架构设计 建立了分组密码研究的四大核心技术方向架构。研究方向一“分组密码的硬件实现技术研究”聚焦于 FPGA、ASIC 等硬件平台的高效实现策略，重点关注硬件资源优化和性能最大化。研究方向二“分组密码的软件实现技术研究”针对通用处理器和嵌入式系统的软件优化技术，侧重代码优化和平台适配。研究方向三“分组密码的软硬件协同设计研究”探索软硬件协同优化的创新实现模式。研究方向四“跨平台分组密码性能评估系统构建”建立标准化的性能评估和比较分析框架。

跨平台性能评估系统创新设计 设计了跨平台分组密码性能评估系统的创新技术框架，该系统旨在为不同实现技术路径提供统一的性能评估标准和比较分析工具。评估系统涵盖了吞吐量、延迟、功耗、资源占用等多维度性能指标，支持硬件实现、软件实现、协同设计等多种技术路径的综合评估。系统设计注重评估结果的客观性、可重现性和可比较性，为分组密码技术的优化决策提供科学依据。