周报 向嘉豪(2025-06-30)

摘要: 本周分析了 ML-DSA FIPS-204 标准的数学基础与工程实现，深入阐述了基于模格密码学的数字签名算法在后量子密码学标准化进程中的关键作用。通过对环$R_q = \frac{Z_{q[X]}}{X^{\{256\}}+1}$上多项式运算机制和 Fiat-Shamir 启发式变换的理论研究，完成了六个核心功能模块的架构设计。在学术研究方面，建立了物联网环境下 MQTT 协议与 ML-DSA 算法优化集成的完整研究框架，通过理论分析与实验验证相结合的方法论，为资源受限设备的后量子认证机制提供了系统性的技术解决方案和学术贡献。

本周计划 1) 完整实现 ML-DSA FIPS-204 标准的核心算法模块 2) 完成 ML-DSA 在 ARM Cortex-M4 平台上的移植优化，验证资源受限环境下的部署可行性

ML-DSA FIPS-204 学习与实现

ML-DSA (Module-Lattice-Based Digital Signature Algorithm) FIPS-204 标准的学习和实现进展。ML-DSA 是基于模格密码学的数字签名算法，为后量子密码学的重要组成部分。

核心算法理论学习

通过深入研读 FIPS-204 标准文档，系统掌握了 ML-DSA 的核心技术原理。在数学基础方面，ML-DSA 基于模学习误差问题(Module Learning With Errors, MLWE)，其安全性依赖于求解 MLWE 问题和模短整数解问题(Module Short Integer Solution, MSIS)的困难性。算法在环$R_q = \frac{Z_{q[X]}}{X^{\{256\}}+1}$上操作，其中$q = 8,380,417$。

在签名机制设计上，该算法采用 Fiat-Shamir 启发式方法的 Schnorr 类签名方案，通过拒绝采样技术避免签名泄露私钥信息。签名过程包含承诺生成、挑战计算和响应验证三个关键步骤，确保了签名的安全性和不可伪造性。

标准定义了三个不同的安全级别参数集：ML-DSA-44 等效于 AES-128 安全强度，适用于一般应用场景；ML-DSA-65 等效于 AES-192 安全强度，提供更高的安全保障；ML-DSA-87 等效于 AES-256 安全强度，满足最高安全要求。

架构设计与实现

基于对标准的理解，完成了 ML-DSA 的模块化架构设计，采用 Rust 语言实现，便于集成进嵌入式系统。

核心模块结构

系统实现了六个核心功能模块。代数运算模块(`algebra.rs`)负责实现环R_q上的多项式运算，包括加法、乘法和无穷范数计算等基础操作。数论变换模块(`ntt.rs`)通过 NTT 优化多项式乘法，使用预计算的单位根显著提高运算效率。密码学原语模块(`crypto.rs`)实现了 SHAKE-128/256 哈希函数和可扩展输出函数，为算法提供必要的密码学基础。采样模块(`sampling.rs`)实现了均匀采样、高斯采样和拒绝采样算法，确保随机数生成的安全性。编码模块(`encode.rs`)处理多项式和签名的序列化与反序列化，保证数据传输的正确性。提示系统(`hint.rs`)实现了签名压缩的提示机制，有效减少签名大小。

算法流程实现

密钥生成算法首先使用 SHAKE-128 生成随机矩阵$\boldsymbol{A}$，然后采样具有小系数的私钥向量$\boldsymbol{s}_1, \boldsymbol{s}_2$，最后计算公钥$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{s}_1 + \boldsymbol{s}_2$。整个过程确保了密钥对的正确性和安全性。

签名生成过程采用概率性方法，首先采样随机向量$\boldsymbol{y}$并计算承诺$\boldsymbol{w} = \boldsymbol{A}\boldsymbol{y}$，然后从消息和承诺中生成挑战$c$，接着计算响应$\boldsymbol{z} = \boldsymbol{y} + c\boldsymbol{s}_1$。为确保安全性，算法应用拒绝采样技术，只有满足特定条件的签名才会被接受，有效防止私钥信息泄露。

签名验证算法通过重构验证值并检查边界条件来验证签名的有效性。验证过程包括挑战一致性检验和提示正确性验证，确保签名确实由相应私钥生成且未被篡改。

论文写作

引言部分的深化完善

通过广泛的文献调研，引言部分整合了多个研究领域的最新成果，包括 Banegas 等人关于 ARM Cortex-M 处理器上 CRYSTALS-Dilithium 性能基准测试的开创性工作，Li 等人关于格基密码学电磁故障注入攻击的安全性分析，以及 Kim 和 Seo 关于 MQTT 协议后量子认证机制的初步探索。这些文献不仅为本研究提供了坚实的理论基础，也明确了现有研究的局限性和改进空间。

章节架构的系统化设计

基于研究内容的逻辑关系和学术论文的标准结构，确定了七个主要章节的组织框架。Introduction 章节已完成并经过多次修订，确保了研究动机的清晰表达和问题定义的准确性。Background and Related Work 章节将系统回顾后量子密码学发展历程、ML-DSA 算法的技术细节、IoT 安全挑战以及 MQTT 协议的安全扩展机制。ML-DSA Algorithm Overview 章节将深入阐述算法的数学基础、安全性分析和标准化参数选择。Implementation Architecture 章节将详细描述针对资源受限设备的优化实现策略。Experimental Methodology 章节将说明性能测试平台搭建和基准测试设计。Results and Analysis 章节将呈现实验数据并进行深入分析。Conclusion 章节将总结研究贡献并展望未来研究方向。