周报 - ML-DSA 学习与论文写作

2025-07-01

研究概述

本周研究摘要

本周系统性地分析了 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。

完成了六个核心功能模块的架构设计。

ML-DSA 算法学习

核心算法理论掌握

系统掌握了 ML-DSA 的核心技术原理

数学基础

- 基于模学习误差问题(MLWE)和模短整数解问题(MSIS)
- 在环$R_q = \frac{Z_{q[X]}}{X^{\{256\}}+1}$上操作，其中$q = 8,380,417$
- 采用 Fiat-Shamir 启发式方法的 Schnorr 类签名方案

密钥生成算法

密钥生成过程确保密钥对的正确性和安全性($(\boldsymbol{A}, \boldsymbol{T})$公钥,$(s_1, s_2)$私钥):

1. 使用 SHAKE-128 生成随机矩阵$\boldsymbol{A}$
2. 采样具有小系数的私钥向量$\boldsymbol{s}_1, \boldsymbol{s}_2$
3. 计算公钥$\boldsymbol{T} = \boldsymbol{A}\boldsymbol{s}_1 + \boldsymbol{s}_2$

签名生成与验证

签名生成过程

采用概率性方法并应用拒绝采样技术：

- 采样随机向量y并计算承诺$\boldsymbol{w} = \boldsymbol{A}\boldsymbol{y}$
- 从消息和承诺中生成挑战c
- 计算响应$\boldsymbol{z} = \boldsymbol{y} + c\boldsymbol{s}_1$

签名验证

- 重构验证值并检查边界条件
- 校验 $\boldsymbol{A}\boldsymbol{z} - \boldsymbol{T}\boldsymbol{c} \approx \boldsymbol{w}_{\text{Approx}}$

架构设计与实现

依据 FIPS-204 中给出的 43 个算法，设计了六个核心功能模块

- **代数运算模块**(algebra.rs)：环R_q上的多项式运算
- **数论变换模块**(ntt.rs)：NTT 优化多项式乘法
- **密码学原语模块**(crypto.rs)：SHAKE-128/256 哈希函数
- **采样模块**(sampling.rs)：均匀采样、高斯采样和拒绝采样
- **编码模块**(encode.rs)：多项式和签名的序列化
- **提示系统**(hint.rs)：签名压缩的提示机制

论文写作进展

引言部分完善

补充了多个 ML-DSA 研究最新成果，包括 ARM Cortex-M 性能基准测试、电磁故障注入攻击分析等。

总结

下周计划

1) 完成 ML-DSA 核心算法模块，并将其集成到嵌入式系统中，验证其在资源受限环境下的可行性

2) 设计 MQTT 协议集成 ML-DSA 的测试框架，评估签名延迟、网络开销和能耗等性能指标

老师评语

你的工作报告用词不错，比如通过 XXXXX 建立了 XXXX，这个用在摘要中也很高大上，但论文里的内容就得充分来证明你的创新和工作量

提高论文创新和写作