# 周报 - 论文选题

向嘉豪

2025-06-24

# 研究概述

# 本周研究摘要

本周报告分析了后量子密码学（PQC）算法标准化现状，重点关注数字签名算法（DSA）在网络协议迁移中面临的技术挑战。

资源约束环境下物联网协议的算法优化实现，具有较大研究意义。

# 本周研究摘要

本周报告分析了后量子密码学（PQC）算法标准化现状，重点关注数字签名算法（DSA）在网络协议迁移中面临的技术挑战。

资源约束环境下物联网协议的算法优化实现，具有较大研究意义。

关键发现：后量子签名算法的大签名尺寸是协议迁移的主要瓶颈

研究方向：ML-DSA 在 MQTT 协议下的迁移实现优化

# NIST 标准化进程 - 2025

# 后量子密码学标准化现状

## 密钥封装机制（KEM）

- FIPS 203（ML-KEM）基于 CRYSTALS-Kyber 已于 2024 年正式发布
- 为密钥交换提供了标准化解决方案

# 后量子密码学标准化现状

## 密钥封装机制（KEM）

- FIPS 203（ML-KEM）基于 CRYSTALS-Kyber 已于 2024 年正式发布
- 为密钥交换提供了标准化解决方案

## 数字签名算法（DSA）

- FIPS 204（ML-DSA）基于 CRYSTALS-Dilithium
- FIPS 205（SLH-DSA）基于 SPHINCS+
- FIPS 206（FN-DSA）基于 FALCON（预计 2025 年夏季发布）

# 标准化时间线

2025 年 3 月重要进展：

- HQC 算法被选中，作为 ML-KEM 备选
- 14 个第二轮 On-Ramp 签名候选算法确定

# 标准化时间线

2025 年 3 月重要进展：

- HQC 算法被选中，作为 ML-KEM 备选
- 14 个第二轮 On-Ramp 签名候选算法确定

重要时间节点：旧签名和密钥封装算法标准将于 2035 年废止

迫切需要向后量子安全算法迁移

# 协议迁移挑战

# 协议迁移技术挑战分析

基于 NCCoE SP 1800-38C 的协议迁移测试结果：

数字签名算法(DSA)迁移比密钥交换迁移面临更严峻的挑战

# 协议迁移技术挑战分析

基于 NCCoE SP 1800-38C 的协议迁移测试结果：

数字签名算法(DSA)迁移比密钥交换迁移面临更严峻的挑战

## TLS 1.3 性能表现

- Kyber-768：681 次握手/秒
- 经典 P384：223 次握手/秒
- Kyber 显示出优异性能优势

# 签名算法挑战

Dilithium 证书大小达到 18-22 KB，在 QUIC 协议中触发了额外的往返传输

导致的问题：

- 放大保护机制启动
- 拥塞控制窗口限制
- 网络开销显著增加

# DSA 算法实现进展

# ML-DSA（FIPS 204）

NIST 主要推荐算法，性能与安全性平衡良好

GPU 加速研究显示 cuML-DSA 在服务器 GPU 上实现了 170.7×到 294.2×的性能提升

优化方法：

- 深度优先稀疏三元多项式乘法优化
- 分支消除方法
- 为高吞吐量服务器环境提供可行解决方案

# SLH-DSA（FIPS 205）

基于哈希函数的保守安全基础

限制因素：极大的签名尺寸和较慢的签名速度限制了实际应用场景

硬件加速：

- SLotH 实现可达到 300×性能提升
- 仍难以满足高频次签名需求和资源受限环境

# FN-DSA（FIPS 206）

优势：

- 最小的签名尺寸
- 快速验证

安全挑战：2025 年发现的 Rowhammer 攻击显示单个比特翻转可以通过数亿次签名恢复完整密钥

其他限制：

- 浮点运算敏感性
- 侧信道漏洞

# 研究方向选择

# ML-DSA 与 MQTT 协议研究方向

经过综合评估，确定 ML-DSA 与 MQTT 物联网协议结合作为主要研究方向

## 算法选择理由

- NIST 主要推荐的后量子签名算法
- 相对成熟的安全分析和实现基础
- GPU 加速研究进展为服务器端优化提供参考
- 模格假设具有更好的理论基础

# 协议选择理由

2025 年 KEM-MQTT 研究成果：

- 在 8 位 AVR 设备上优化实现
- 发表于 25-CCS（CCF-A）安全顶会
- 证明了资源受限环境下实现后量子安全的研究价值

25CCS 文章未将 DSA 迁移入 MQTT 实现，ML-DSA-MQTT 协议集成研究为空白

# 总结

# 下周计划

制定 ML-DSA 在 MQTT 协议中的实现优化研究计划

具体任务：

- 深入分析 ML-DSA 算法特性
- 研究 MQTT 协议的资源约束特点
- 设计针对 IoT 环境的优化策略
- 制定详细的实现方案

# 老师评语

请关注当前幻灯片编号。