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

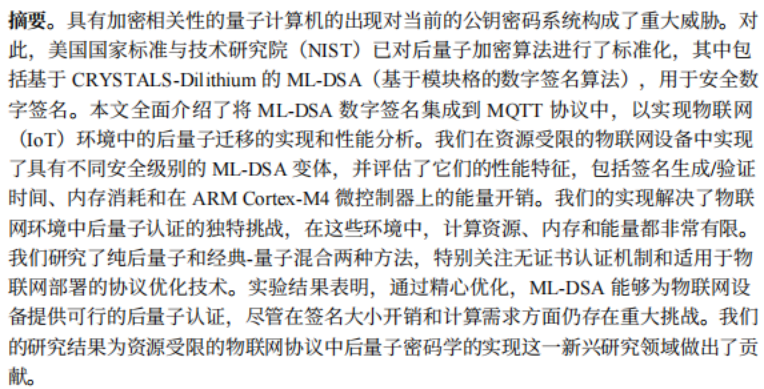
下周计划

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



摘要。具有加密相关性的量子计算机的出现对当前的公钥密码系统构成了重大威胁。对此，美国国家标准与技术研究院（NIST）已对后量子加密算法进行了标准化，其中包括基于 CRYSTALS-Dilithium 的 ML-DSA（基于模块格的数字签名算法），用于安全数字签名。本文全面介绍了将 ML-DSA 数字签名集成到 MQTT 协议中，以实现物联网（IoT）环境中的后量子迁移的实现和性能分析。我们在资源受限的物联网设备中实现了具有不同安全级别的 ML-DSA 变体，并评估了它们的性能特征，包括签名生成/验证时间、内存消耗和在 ARM Cortex-M4 微控制器上的能量开销。我们的实现解决了物联网环境中后量子认证的独特挑战，在这些环境中，计算资源、内存和能量都非常有限。我们研究了纯后量子和经典-量子混合两种方法，特别关注无证书认证机制和适用于物联网部署的协议优化技术。实验结果表明，通过精心优化，ML-DSA 能够为物联网设备提供可行的后量子认证，尽管在签名大小开销和计算需求方面仍存在重大挑战。我们的研究结果为资源受限的物联网协议中后量子密码学的实现这一新兴研究领域做出了贡献。

1）先看下这个摘要的第一句话，作为研究生写得如此不通顺的中文我比较少见。

“相关性”此处是错误的 应该是攻击性✓

老师评语

2）论文要用第 3 人称，这个说了很多次吧，你看下你这用了多少第 1 人称，一个人不去思考不听取教育那如何进步???

是的老师说了很多次了，学生会努力改正的。

3）你这摘要创新是在堆砌几个点还是围绕着一个点在递进？至少我从摘要写作上看不出是围绕一个核心困难问题在递进解决。

现在的摘要是对该方向下，可研究点的汇总，随着研究的深入，学生会围绕一个核心问题进行深入研究。