周报 向嘉豪(2025-09-29)

摘要: 本周完成 ML-DSA 论文重构优化与后量子 MQTT 代理技术调研。论文方面：重构第 3 节 ML-DSA 与 MQTT 协议集成内容，将 12 个子节合并为 4 个重点技术节，精简约 60% 并保持技术准确性。新增 4 个参考文献强化学术基础，重构三大研究贡献为条目化展示。识别 ML-DSA 在 MQTT 协议中的四个关键影响点：TLS 证书验证、客户端认证、消息级签名、会话令牌管理。建立 MQTT 协议基础理论框架，量化分析 ML-DSA 签名尺寸增长对 IoT 设备的性能影响。

下周计划: 1) 深化 ML-DSA 论文 IoT 环境部署优化分析，完善资源受限设备性能评估框架。 2) 启动 ML-DSA 实验验证系统设计，准备 ARM Cortex-M4 微控制器性能基准测试。

1 ML-DSA 论文重构优化进展

1.1 第 3 节 ML-DSA 与 MQTT 协议集成

节结构优化重组 系统性重组第 3 节内容架构，建立 4 个重点技术节：3.1 ML-DSA 算法特征整合数学基础与计算要求，3.2 参数集合与安全性分析保留核心比较表格，3.3 MQTT 协议与安全集成合并协议基础与 QoS 级别，3.4 ML-DSA 集成挑战结合性能影响与权衡分析。重构过程通过合并相关内容、消除重复描述、强化技术逻辑链条，实现内容密度的显著提升。

学术基础强化与引用优化 新增 4 个参考文献以强化学术基础：Khalid2019(IoT 量子世界中的格基密码学)、Ghosh2019(IoT 轻量级后量子数字签名)、HwangKim2024(多项式乘法优化)、MLDSAHardware2024(ML-DSA 硬件实现改进)。

研究贡献结构化展示 重构三大研究贡献为条目化列表格式，采用蓝色高亮强化展示效果：计算性能基准测试量化 ARM Cortex-M4 微控制器上 ML-DSA 签名操作的计算开销，内存利用分析测量约束环境下 ML-DSA 部署的静态存储和动态内存模式，协议级 MQTT 集成评估分析 ML-DSA 集成对 MQTT 通信框架的协议级开销影响。条目化展示提升研究贡献的可读性和学术影响力。

2 ML-DSA MQTT 代理迁移技术分析

2.1 MQTT 协议基础与 ML-DSA 影响分析

MQTT 协议概述 MQTT(Message Queuing Telemetry Transport)是专为物联网设计的轻量级发布-订阅消息传输协议。协议采用客户端-代理架构，支持多个客户端通过中央 MQTT 代理进行消息交换。核心特征包括最小化网络带宽占用、减少设备资源需求、提供可靠消息传递机制，使其成为资源受限 IoT 环境的理想选择。MQTT 支持三种服务质量(QoS)级别：QoS 0(最多一次)、QoS 1(至少一次)、QoS 2(恰好一次)，为不同应用场景提供灵活的可靠性保证。

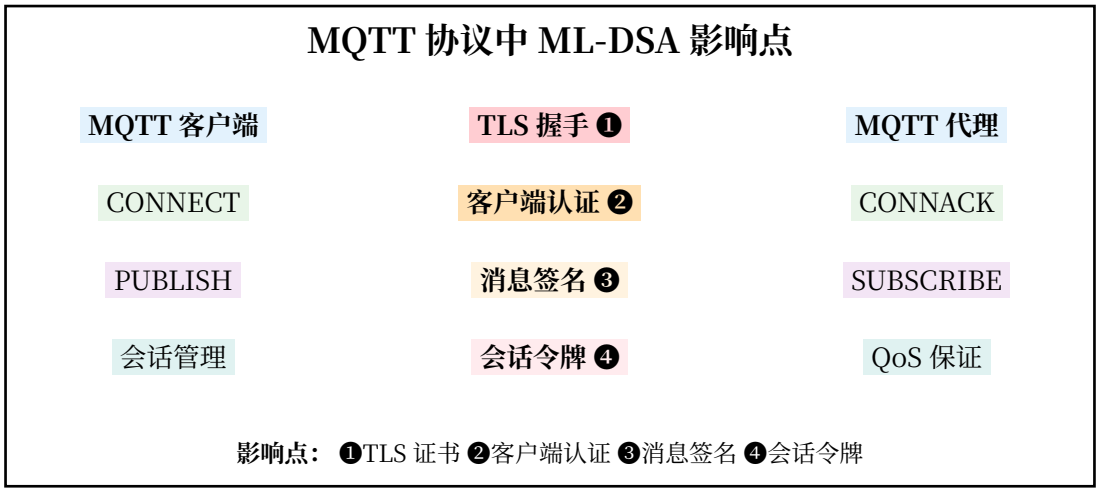

图 1　MQTT 协议中 ML-DSA 的四个关键影响点

2.2 ML-DSA 在 MQTT 协议中的迁移角色分析

MQTT 代理数字签名迁移路径 MQTT 协议中的数字签名主要应用于 TLS 握手阶段的服务器认证和客户端证书验证。传统 DSA/ECDSA 算法在 MQTT 代理的 TLS 层承担证书签名验证、消息完整性保护、身份认证等关键安全功能。ML-DSA 迁移需要在保持 MQTT 协议兼容性的前提下，替换底层密码学原语，确保 IoT 设备与代理之间的安全通信。

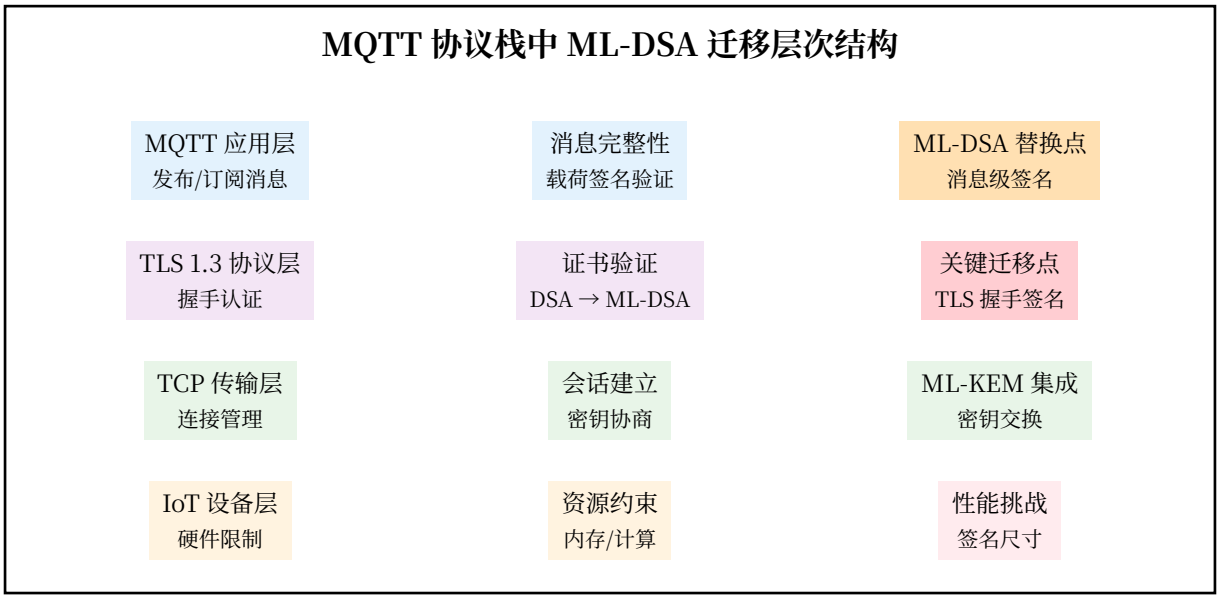

图 2　MQTT 协议栈中 ML-DSA 迁移的技术层次与关键替换点分析

MQTT 代理认证机制转换 ML-DSA 在 MQTT 代理中主要替换两个关键认证点：TLS 服务器证书签名和客户端证书验证。服务器证书中的 DSA 签名需要替换为 ML-DSA 签名，确保 IoT 设备能够验证代理身份。客户端证书验证过程中，代理需要支持 ML-DSA 签名的 IoT 设备证书，建立双向认证机制。这种迁移要求 MQTT 代理同时支持传统 DSA 和 ML-DSA 算法，实现渐进式迁移策略。

协议层级影响分析 ML-DSA 迁移对 MQTT 协议栈各层级产生不同程度影响。应用层的发布/订阅消息可选择性地集成 ML-DSA 消息级签名，提供端到端完整性保护。TLS 层是主要迁移焦点，需要更新握手流程支持 ML-DSA 证书链验证。传输层的密钥协商需要配合 ML-KEM 算法，形成完整的后量子密码学解决方案。设备层面临的挑战包括 ML-DSA 签名尺寸增大 (2420-4627 字节)对内存受限设备的影响。