周报

2025-09-29

本周研究摘要

- ML-DSA 论文重构优化：第 3 节内容架构重组，12 个子节合并为 4 个重点技术节，精简约 60%
- 后量子 MQTT 迁移技术调研：建立 MQTT 协议基础理论框架，识别 ML-DSA 四个关键影响点

ML-DSA 论文重构优化进展

第 3 节结构优化:

- 建立 4 个重点技术节架构：ML-DSA 算法特征、参数集合与安全性、MQTT 协议与安全集成、ML-DSA 集成挑战
- 新增 4 个参考文献强化学术基础
- 研究贡献重构为条目化展示，提升可读性

核心技术内容:

- 量化分析 ML-DSA 签名尺寸增长对 IoT 设备的性能影响
- 整合数学基础与计算要求分析

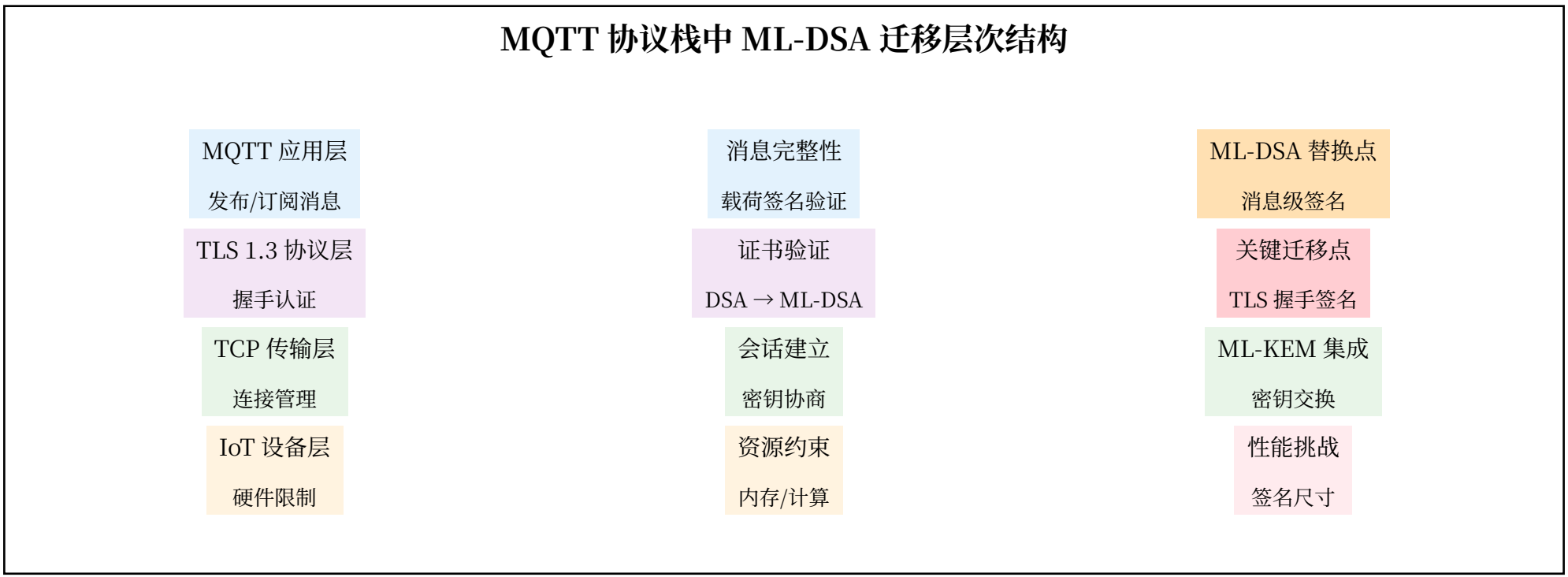
MQTT 协议基础与 ML-DSA 影响分析

MQTT 协议特征:

- 轻量级发布-订阅消息传输协议，专为物联网设计

影响点： ❶TLS 证书 ❷客户端认证 ❸消息签名 ❹会话令牌

ML-DSA 在 MQTT 协议中的迁移角色



迁移关键技术分析

MQTT 代理数字签名迁移路径:

- TLS 握手阶段的服务器认证和客户端证书验证
- 替换底层密码学原语，保持 MQTT 协议兼容性

协议层级影响:

- 应用层：可选择性集成 ML-DSA 消息级签名
- TLS 层：更新握手流程支持 ML-DSA 证书链验证
- 设备层：ML-DSA 签名尺寸增大(2420-4627 字节)对内存受限设备的影响

总结

下周计划

- 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
- 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

老师评语

CHES 最近一期截稿时间是什么时候?

- TCHES Volume 2026/2： 2025.10.15 Submission
- TCHES Volume 2026/3： 2026.01.15 Submission