周报 向嘉豪 (2025 年 6 月 23 日)

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。通过对 NIST 标准化进程、协议迁移测试结果以及相关研究工作的系统性分析，确定了 ML-DSA 与 MQTT 协议结合作为物联网环境下后量子签名算法研究的主要方向。其中，后量子签名算法的大签名尺寸是协议迁移的主要瓶颈，而物联网协议的资源约束环境进一步放大算法优化实现的研究意义。

下周计划： 1) 制定 ML-DSA 在 MQTT 协议中的实现优化研究计划

1 研究进展分析

1.1 后量子密码学标准化现状

NIST 后量子密码学标准化进程已基本完成，形成了两大类核心算法标准。在密钥封装机制（KEM）方面，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）领域则包含三个标准：FIPS 204（ML-DSA）基于 CRYSTALS-Dilithium、FIPS 205（SLH-DSA）基于 SPHINCS+，以及正在开发中的 FIPS 206（FN-DSA）基于 FALCON，预计 2025 年夏季发布。

2025 年 3 月的重要进展包括 HQC 算法被选中进行标准化以及 14 个第二轮 On-Ramp 签名候选算法的确定。这些发展表明后量子密码学正从理论研究转向实际部署阶段，但同时也暴露出算法多样性带来的选择复杂性。重要的是，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。

1.2 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。关键发现包括：

在 TLS 1.3 协议中，Kyber 密钥交换显示出优异的性能表现，Kyber-768 实现了 681 次握手/秒的吞吐量，与经典 P384 算法的 223 次握手/秒相比具有明显优势。然而，后量子签名算法的大尺寸特性带来了显著的网络开销。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，导致放大保护机制启动和拥塞控制窗口限制。

SSH 协议由于其多轮传输设计，对后量子签名的性能影响相对较小。但在认证支持方面，当时测试中仅有 OQS-OpenSSH 提供了后量子认证功能，显示出实现生态系统的不成熟。

1.3 DSA 算法与协议适配性评估

通过对三种标准化 DSA 算法的深入分析，发现各算法在不同应用场景下的适用性存在显著差异：

ML-DSA（FIPS 204）作为 NIST 的主要推荐算法，在性能和安全性之间提供了良好的平衡。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，通过深度优先稀疏三元多项式乘法优化和分支消除方法，为高吞吐量服务器环境提供了可行的解决方案。

FN-DSA（FIPS 206）虽然提供最小的签名尺寸和快速验证，但面临严重的安全挑战。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，浮点运算敏感性和侧信道漏洞进一步限制了其实际部署的安全性。

SLH-DSA（FIPS 205）基于哈希函数的保守安全基础，但其极大的签名尺寸和较慢的签名速度限制了实际应用场景。硬件加速研究显示 SLotH 实现可达到 300× 的性能提升，但仍难以满足高频次签名需求和资源受限环境。

1.4 ML-DSA 与 MQTT 协议研究方向确定

经过综合评估，确定 ML-DSA 与 MQTT 协议结合作为主要研究方向，基于以下关键考虑：

算法选择理由：ML-DSA 作为 NIST 主要推荐的后量子签名算法，具有相对成熟的安全分析和实现基础。其在 GPU 加速方面的研究进展为服务器端优化提供了参考，同时其模格假设相比其他算法具有更好的理论基础。

协议选择理由：物联网环境下的 MQTT 协议迁移研究相对不足，现有研究主要集中在 KEM-MQTT 实现上，直接的 ML-DSA 与 IoT 协议集成研究几乎空白。2025 年的 KEM-MQTT 研究在 8 位 AVR 设备上优化实现，并发表于最新 25-CCS（CCF-A）安全顶会，证明了在资源受限环境下实现后量子安全的研究价值。

研究机会识别：物联网设备的资源约束特性为算法优化提供了独特的研究机会。现有的嵌入式系统研究（如 pqm4 基准测试框架）为 ML-DSA 在 ARM Cortex-M4 上的性能评估提供了基础，但缺乏针对 IoT 协议的专门优化。侧信道安全研究显示了在微控制器上实现安全 ML-DSA 的挑战和对策，为安全实现提供了指导。

实际应用价值：随着 IoT 设备数量的快速增长和量子计算威胁的逐步现实化，为资源受限的 IoT 环境提供量子安全的认证机制具有重要的实际意义。传统的证书链方法在 IoT 环境下面临带宽和存储限制，需要创新的轻量级认证策略，也是未来研究的方向之一。