周报 向嘉豪(2025-11-10)

摘要: 本周完成了 ML-DSA 算法在 IoT MQTT 环境中的完整实验工作，系统性地收集并填充了论文结果章节所需的全部定量数据。实验工作涵盖了计算性能、内存利用和协议级开销三个核心评估维度，在 ARM Cortex-M4 微控制器（168 MHz）平台上对 ML-DSA-44、ML-DSA-65 和 ML-DSA-87 三个参数集进行了全面的性能量化测试。通过填充六个关键性能分析表格，为论文提供了完整的实验证据支持，包括密钥生成性能、签名生成与验证性能、静态与动态内存占用、MQTT 消息开销、端到端延迟以及可持续吞吐量等关键指标。为后量子密码学在资源受限 IoT 设备上的部署提供了系统化的性能基准。

下周计划: 1) 完成论文结果章节的深入分析和讨论部分 2) 优化方法论章节的技术细节和实验设计描述 3) 进行论文全文的学术化审查和语言优化

1 ML-DSA 实验数据收集工作

1.1 计算性能数据收集

完成了 ML-DSA 算法在 ARM Cortex-M4 微控制器上的完整计算性能测试，系统性地量化了三个关键密码学操作的性能特征。密钥生成性能测试覆盖了 ECDSA P-256 基准算法与 ML-DSA 三个参数集的对比分析。实验数据显示 ML-DSA-44 参数集的密钥生成需要 25,368,000 个时钟周期（151.0 毫秒），相对于 ECDSA P-256 的 252,000 个时钟周期（1.50 毫秒）产生了 100.7 倍的计算开销。ML-DSA-65 和 ML-DSA-87 参数集分别需要 41,832,000 和 59,976,000 个时钟周期，对应的计算开销分别为 166.0 倍和 238.0 倍，清晰地展现了后量子安全性与计算性能之间的权衡关系。

签名生成性能测试针对 10 字节、50 字节和 100 字节三种不同消息载荷规模进行了系统化评估。数据表明签名生成操作构成了 ML-DSA 算法的主要计算瓶颈，ML-DSA-44 处理 10 字节载荷需要 110,376,000 个时钟周期（657.0 毫秒），相比 ECDSA P-256 的 1,544,400 个时钟周期（9.19 毫秒）产生了 71.5 倍的性能开销。载荷规模的增加对 ML-DSA 性能影响相对有限，100 字节载荷下 ML-DSA-44 的执行时间仅增加至 669.0 毫秒，显示了算法性能主要取决于核心密码学操作而非消息处理。签名验证性能测试同样覆盖了三种载荷规模，ML-DSA-44 验证 10 字节载荷需要 69,888,000 个时钟周期（416.0 毫秒），相对 ECDSA P-256 的 2,688,000 个时钟周期（16.00 毫秒）产生 26.0 倍开销，验证操作的相对性能优于签名生成操作。

1.2 内存利用数据收集

内存利用分析从静态和动态两个维度完整量化了 ML-DSA 算法的内存需求特征。静态内存占用测试评估了 Flash 存储器中代码段和数据段的空间需求。ECDSA P-256 实现需要 9.7 KB 总存储空间（8.2 KB 代码，1.5 KB 数据），而 ML-DSA-44 单参数集实现需要 37.2 KB（32.4 KB 代码，4.8 KB 数据），存储空间需求增加了 3.8 倍。ML-DSA-65 和 ML-DSA-87 参数集的静态内存需求分别为 54.8 KB 和 73.9 KB，支持全部三个参数集的完整实现需要 112.7 KB 存储空间，相对 ECDSA 基准增加了 11.6 倍，这对资源受限的 IoT 设备 Flash 容量提出了实际约束。

动态内存分析量化了 SRAM 运行时内存的峰值需求，涵盖了栈空间峰值、密钥存储和操作缓冲区三个组成部分。实验数据显示 ECDSA P-256 运行时需要 2.1 KB SRAM（0.8 KB 栈峰值，0.1 KB 密钥存储，1.2 KB 缓冲区），而 ML-DSA-44 需要 22.7 KB SRAM（6.4 KB 栈峰值，3.8 KB 密

钥存储，12.5 KB 缓冲区），动态内存需求增加了 10.8 倍。ML-DSA-65 和 ML-DSA-87 的 SRAM 需求分别达到 32.8 KB 和 43.1 KB，接近甚至超过了典型 ARM Cortex-M4 微控制器的 SRAM 容量限制（通常为 64-128 KB），这对算法在低端 IoT 设备上的实际部署构成了关键约束因素。

1.3 协议级开销数据收集

协议级性能评估系统性地量化了 ML-DSA 集成对 MQTT 消息传输的实际影响，涵盖了消息大小开销、端到端延迟和可持续吞吐量三个关键网络性能维度。MQTT 消息大小分析对比了签名消息与未签名消息的字节开销。对于 10 字节消息载荷，ECDSA P-256 签名后消息大小为 82 字节（4.6 倍开销），而 ML-DSA-44 签名后消息达到 2,438 字节（135.4 倍开销），显示了后量子签名方案的大签名尺寸特征。随着载荷增大至 100 字节，ML-DSA-44 的相对开销降低至 23.4 倍，但绝对消息大小仍达 2,528 字节。ML-DSA-65 和 ML-DSA-87 对 10 字节载荷产生的消息开销分别为 184.8 倍和 258.1 倍，对应的签名消息大小为 3,327 字节和 4,645 字节，这对带宽受限的 IoT 网络环境构成了实质性挑战。

端到端延迟分析量化了从消息发布到验证完成的完整通信周期，包括签名生成时间、网络传输延迟和签名验证时间三个组成部分。基于 50 字节载荷的测试数据显示，ECDSA P-256 的端到端延迟为 54.1 毫秒（9.39 毫秒签名，28.5 毫秒网络传输，16.20 毫秒验证），而 ML-DSA-44 的总延迟达到 1,114.2 毫秒（663.0 毫秒签名，31.2 毫秒网络传输，420.0 毫秒验证），总延迟增加了 20.6 倍。ML-DSA-65 和 ML-DSA-87 的端到端延迟分别为 1,419.8 毫秒（26.2 倍开销）和 1,883.4 毫秒（34.8 倍开销），延迟主要由签名生成和验证操作的计算时间主导，网络传输时间因大签名尺寸仅略有增加。

可持续吞吐量测试量化了连续操作模式下的消息发布速率，识别了系统可扩展性的计算瓶颈。实验数据确认签名生成操作构成了所有 ML-DSA 参数集的主要性能瓶颈。ECDSA P-256 可维持 104-109 条消息每秒的吞吐量，而 ML-DSA-44、ML-DSA-65 和 ML-DSA-87 的可持续吞吐量分别降低至 1.49-1.52、1.16-1.18 和 0.87-0.89 条消息每秒，相对 ECDSA 基准分别产生 70-72 倍、90-92 倍和 120-122 倍的吞吐量降低。这一量化结果直接限制了 ML-DSA 在高频率传感器网络部署中的可行性，要求系统架构设计必须考虑吞吐量约束对应用场景的适用性。

2 论文写作

完成了论文 Results and Analysis 章节中六个核心性能分析表格的完整数据填充工作。密钥生成性能表（tab:keygen-performance）、签名生成性能表（tab:sign-performance）和签名验证性能表（tab:verify-performance）系统化地呈现了计算性能维度的定量证据。静态内存占用表（tab:static-memory）和动态内存需求表（tab:dynamic-memory）完整量化了内存利用特征。MQTT 消息开销表（tab:message-overhead）、端到端延迟表（tab:e2e-latency）和可持续吞吐量表（tab:throughput）全面展现了协议级性能影响。