周报 向嘉豪(2025-12-22)

摘要：本周 ML-DSA 论文全文内容精炼与学术表达优化，系统改进 Introduction、Related Work、ML-DSA Algorithm、Implementation Architecture 及 Experimental Methodology 章节的文本清晰度与技术准确性。重点优化包括：贡献陈述重构为具体可测量的技术指标、冗余表述消除、被动语态规范化应用、以及技术参数的精确量化表达。

下周计划: 1) 完善 Results 章节实验数据分析 2) 补充 Conclusion 章节撰写

1 Introduction 章节优化

完成了 Introduction 章节的内容精炼，将原有冗长表述压缩为简洁的技术陈述。IoT 系统部署挑战描述从“fundamentally constrain cryptographic implementation choices”简化为“constrain cryptographic implementation choices”，消除不必要的强调副词。MQTT 协议性能影响描述从“exhibits severe performance degradation when post-quantum signatures introduce prohibitive overhead”修订为“experiences performance degradation when post-quantum signatures introduce overhead”，避免主观程度判断词汇。

研究贡献陈述重构为具体可测量的技术指标：Computational Performance Benchmarking 从泛化描述改为“Cycle-accurate measurements of ML-DSA signature operations on ARM Cortex-M4 microcontrollers at 168 MHz, quantifying execution latency and throughput across all three standardized parameter sets”；Memory Utilization Analysis 改为“Static and dynamic memory profiling measuring Flash storage requirements, stack consumption, and peak SRAM utilization during signature operations”；Protocol-Level MQTT Integration Assessment 改为“End-to-end latency and message size overhead evaluation within MQTT publish-subscribe workflows, comparing ML-DSA against ECDSA P-256 baseline”。

2 Related Work 章节改进

完成了 Related Work 章节的学术表达规范化。消除冗余连接词与过度修饰：开篇从“While conventional network protocols have undergone extensive analysis”简化为“Conventional network protocols have undergone post-quantum migration analysis”，同时明确指出“IoT-specific communication protocols remain underexplored”作为研究空白。

ML-DSA Performance Benchmarks 小节精简了 Banegas 等人研究的描述，从“quantified these performance implications through comprehensive benchmarking”改为直接陈述“benchmarked CRYSTALS-Dilithium on embedded systems”。pqm4 基准测试描述整合引用格式，将分散的性能数据统一为连贯的技术陈述。

Deployment Bottlenecks 小节改进了安全漏洞描述的技术准确性，将 Marchsreiter 研究结果从泛化描述改为具体的“order-of-magnitude transaction throughput reductions on embedded blockchain nodes”量化表述。Alternative Approaches 小节将 Barrett 乘法优化的性能提升数据格式统一为“1.38–1.51”和“6.37–7.27”的标准化表示。

3 ML-DSA Algorithm 章节技术表述优化

完成了 ML-DSA Algorithm Characteristics 小节的技术参数精确化。拒绝采样迭代次数描述从泛化的“expected iteration counts of 4.25, 5.1, and 3.85 across parameter sets”改为明确的“expected iteration counts of 4.25, 5.1, and 3.85 for ML-DSA-44, ML-DSA-65, and ML-DSA-87 respectively”，建立参数集与迭代次数的直接对应关系。密钥尺寸范围采用标准化单位表示“1.3–4.9,KB”。

Signing Algorithm Structure 小节优化了算法描述的简洁性。签名过程概述从“The signing wrapper (Algorithm ref{alg:mldsa-sign}) processes context strings”改为“Algorithm ref{alg:mldsa-sign} presents the signing wrapper, which processes context strings”，采用更直接的算法引用方式。确定性签名变体描述从“this randomness is substituted with zeros to enable reproducible signatures”简化为“deterministic variants substitute zeros for reproducible signatures”。

Signing Performance Bottlenecks 小节精简了性能瓶颈描述。NTT Computational Dominance 从详细的周期数描述“reference NTT implementations consume 2.5-3.0 million cycles per transformation”压缩为“Reference Cortex-M4 implementations consume 2.5–3.0 million cycles per NTT”，消除冗余的“establishing NTT as the dominant computational primitive”结论性陈述。

4 Implementation Architecture 与 Methodology 章节改进

完成了 Implementation Architecture 章节的表述简化。章节引言从“This section presents the system architecture for ML-DSA signature integration within MQTT-based IoT communication frameworks. The implementation encompasses hardware platform configuration, software stack organization, and protocol-level integration patterns enabling post-quantum authenticated messaging on resource-constrained devices”压缩为单句“This section presents the system architecture for ML-DSA signature integration within MQTT-based IoT communication frameworks, encompassing hardware platform configuration, software stack organization, and protocol-level integration patterns”。

Hardware Platform Architecture 小节统一了技术参数格式，将“168 MHz system clock frequency”改为“168,MHz”，“1 MB Flash memory”改为“1,MB Flash memory”，“192 KB SRAM”改为“192,KB SRAM”，采用标准化的数值与单位间距表示。

Experimental Methodology 章节开篇精简为“The experimental framework evaluates ML-DSA integration within MQTT-based IoT systems through performance benchmarking on ARM Cortex-M4 microcontrollers, memory utilization analysis, and protocol-level overhead assessment”，消除“comprehensive”、“systematic”等主观修饰词，保持客观技术陈述风格。