IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN XXXX-XXXX, Vol. 0, No. 0, pp. 1–7. DOI:XXXXXXXX

ML-DSA Digital Signatures in Resource-Constrained MQTT Environments

Jiahao Xiang[1] and Lang Li[1]

Hengyang Normal University, College of Computer Science and Technology, Hengyang, China

Abstract. The imminent threat of large-scale quantum computers necessitates the migration of Internet of Things (IoT) systems to post-quantum cryptographic standards. While NIST has standardized ML-DSA (Module-Lattice-Based Digital Signature Algorithm) for digital signatures, the practical deployment of post-quantum authentication in resource-constrained IoT environments remains unexplored. This research evaluates ML-DSA integration within MQTT-based IoT systems through comprehensive performance analysis on ARM Cortex-M4 microcontrollers. Our methodology encompasses signature generation and verification benchmarking, memory utilization analysis, and protocol overhead assessment under realistic IoT constraints. We analyze the performance implications of ML-DSA deployment compared to classical signature schemes, examining computational overhead, memory requirements, and verification latency on resource-constrained devices. These findings will reveal fundamental trade-offs between post-quantum security and IoT performance requirements, providing critical insights for practical deployment strategies in resource-limited environments.

Keywords: Post-Quantum Cryptography · ML-DSA · MQTT Protocol · IoT Security · Resource-Constrained Devices

1 Introduction

The emergence of quantum computing poses an existential threat to current cryptographic infrastructures, necessitating systematic migration to post-quantum cryptographic standards across all computing domains [KMLO19]. The National Institute of Standards and Technology (NIST) has formalized ML-DSA (Module-Lattice-Based Digital Signature Algorithm) within FIPS 204 [NIS24], establishing this CRYSTALS-Dilithium-based scheme as the primary standard for post-quantum digital signatures.

The transition from theoretical post-quantum standardization to practical deployment has revealed fundamental implementation challenges that extend beyond algorithmic considerations [Ano24]. Post-quantum signature schemes impose substantial computational and storage overhead compared to classical alternatives. ML-DSA signatures range from 2,420 bytes to 4,627 bytes across security levels, representing 30-70× size increases relative to 64-byte ECDSA signatures. These expanded signature sizes, combined with elevated computational demands, frequently exceed the processing capabilities of resource-constrained devices [HKS24].

Internet of Things (IoT) systems exemplify these deployment challenges, where computational, memory, and energy limitations fundamentally constrain cryptographic implementation choices [GMS19]. Despite performance overhead, signature-based authentication mechanisms remain essential for applications requiring cryptographic non-repudiation, comprehensive audit trails, and compatibility with existing public key infrastructure frameworks. The MQTT protocol, widely adopted for IoT messaging due to its lightweight characteristics, becomes particularly problematic when post-quantum signatures impose

prohibitive performance overhead on resource-constrained devices. This disparity creates a critical gap between standardization achievements and practical deployment feasibility in IoT environments.

This research systematically addresses the challenge of ML-DSA integration within MQTT-based IoT systems through comprehensive performance analysis on ARM Cortex-M4 microcontrollers. Our work provides three primary contributions to post-quantum IoT deployment:

- **Computational Performance Benchmarking**: We conduct comprehensive benchmarking of ML-DSA signature operations on resource-constrained ARM Cortex-M4 microcontrollers, quantifying computational overhead, execution latency, and performance variations across all three standardized ML-DSA parameter sets under realistic IoT operating conditions.
- **Memory Utilization Analysis**: We provide systematic memory utilization analysis for ML-DSA deployment in constrained environments, measuring static storage requirements, dynamic memory allocation patterns, and peak memory consumption during signature generation and verification operations.
- **Protocol-Level MQTT Integration Assessment**: We evaluate protocol-level overhead implications of ML-DSA integration within MQTT communication frameworks, analyzing message size increases, transmission latency impacts, and network throughput degradation relative to classical signature schemes.

Through comparative analysis with classical signature schemes, these contributions establish fundamental trade-offs between post-quantum security guarantees and IoT performance requirements, providing essential insights for practical deployment strategies in resource-limited environments.

The remainder of this paper is organized as follows: Section 2 presents background information on post-quantum cryptography and related work in IoT deployments. Section 3 provides an overview of the ML-DSA algorithm and its implementation considerations. Section 4 describes our implementation architecture for MQTT-based IoT systems. Section 5 details our experimental methodology for performance evaluation on ARM Cortex-M4 microcontrollers. Section 6 presents and analyzes our experimental results, examining the trade-offs between security and performance. Finally, Section 7 concludes with implications for practical deployment and future research directions.

2 Related Work and Motivation

While conventional network protocols have undergone extensive analysis for post-quantum migration [KSD20, SKD20], IoT-specific communication protocols remain inadequately addressed, creating deployment barriers in resource-constrained environments.

2.1 ML-DSA Performance Benchmarks on Embedded Systems

Banegas et al. [BZB+22] quantified these performance implications through comprehensive benchmarking on embedded systems, establishing that CRYSTALS-Dilithium signature operations require approximately 45% additional computational cycles compared to classical ECDSA implementations on ARM Cortex-M4 processors. This computational overhead compounds with memory constraints to create deployment bottlenecks in IoT environments.

The ongoing pqm4 benchmarking campaign extends these observations to the standardized ML-DSA parameter sets, reporting that even aggressively optimized implementations still consume tens of kilobytes of static and dynamic memory and millions of CPU cycles

per signature on Cortex-M4 targets [KKPY24]. Complementary measurements on higher performance IoT-class microcontrollers demonstrate that migrating to newer cores such as Cortex-M7 reduces latency but leaves signature generation and verification firmly in the tens-of-milliseconds regime, keeping ML-DSA near the edge of acceptable responsiveness for interactive device workloads [HW23].

2.2 Deployment Bottlenecks in IoT Applications

Practical deployment scenarios reveal critical performance bottlenecks that challenge IoT system viability. Analysis of the SUIT (Software Update for the Internet of Things) framework demonstrates that post-quantum signature verification operations require up to 3.2 seconds on low-power microcontrollers, substantially exceeding acceptable latency constraints for real-time IoT applications.

These performance constraints are compounded by security vulnerabilities and protocol-level throughput ceilings. Marchsreiter [Mar24] shows that blockchain workloads on embedded nodes experience order-of-magnitude drops in transactions-per-second once ML-DSA is introduced, with signing latency alone dominating system throughput. Fault injection research targeting ML-DSA and ML-KEM implementations achieved 89.5% attack success rates on ARM Cortex-M processors through electromagnetic fault injection techniques [WYQ+24]. The analyses demonstrate that Keccak-based hash functions—integral to ML-DSA randomness generation and signature computation—exhibit particular susceptibility to loop-abort faults enabling complete private key recovery, necessitating additional countermeasures that further impact performance.

2.3 Alternative Approaches and Limitations

Recent research has explored alternative authentication architectures to address these deployment challenges. Kim and Seo [KS25] demonstrate that direct application of post-quantum signatures to MQTT authentication introduces prohibitive performance overhead, prompting KEM-based authentication architectures that eliminate signature operations entirely. While their CRYSTALS-Kyber implementation achieves 4.32-second handshake completion on 8-bit AVR microcontrollers, this approach circumvents rather than resolves the fundamental challenge of post-quantum signature deployment in signature-dependent applications.

Current algorithmic optimization research reveals limitations in addressing fundamental resource constraints. Barrett multiplication techniques achieve 1.38-1.51× performance improvements on ARM Cortex-M3 processors and 6.37-7.27× improvements on 8-bit AVR platforms [HKS25]. However, these optimizations provide insufficient performance gains to bridge the gap between post-quantum signature requirements and IoT device capabilities, necessitating comprehensive system-level analysis.

2.4 Research Gap and Motivation

The absence of comprehensive empirical studies specifically evaluating ML-DSA performance within MQTT protocol implementations represents a critical knowledge gap in post-quantum IoT deployment. This gap becomes particularly significant given MQTT's widespread adoption in industrial IoT deployments, where signature-based authentication remains mandatory for regulatory compliance and security audit requirements.

Existing research primarily focuses on isolated cryptographic operations or alternative protocol architectures, failing to address the systematic integration challenges inherent in MQTT-based IoT systems. This research addresses these limitations through comprehensive performance analysis of ML-DSA deployment within realistic MQTT environments, providing essential insights for practical post-quantum IoT migration strategies.

3 ML-DSA and MQTT Protocol Integration

3.1 ML-DSA Algorithm Characteristics

ML-DSA constitutes NIST's standardized post-quantum digital signature scheme (FIPS 204 [NIS24]) based on CRYSTALS-Dilithium. The algorithm employs the Fiat-Shamir With Aborts paradigm over polynomial rings $R_q = \mathbb{Z}_q[X]/(X^{256} + 1)$ with security derived from Module Learning With Errors (MLWE) and Module Short Integer Solution (MSIS) assumptions. Polynomial arithmetic utilizes Number Theoretic Transform (NTT) operations achieving $O(n \log n)$ complexity.

ML-DSA implements rejection sampling requiring iterative signature generation with expected iteration counts of 4.25, 5.1, and 3.85 across parameter sets, directly impacting timing predictability. The algorithm comprises three operations: key generation with $O(k \cdot \ell \cdot n \log n)$ complexity producing keys of 1.3-4.9 KB, computationally intensive signature generation with variable execution time, and deterministic verification with $O((k + \ell) \cdot n \log n)$ complexity—all substantially exceeding classical signature costs.

3.2 Parameter Sets and Security Analysis

NIST standardizes three ML-DSA parameter sets with distinct security-performance trade-offs. Table 1 summarizes the key parameters and resulting implementation characteristics.

Table 1: ML-DSA Parameter Sets and Implementation Characteristics

Parameter	ML-DSA-44	ML-DSA-65	ML-DSA-87
Security Category	2 (AES-128)	3 (AES-192)	5 (AES-256)
Matrix (k, ℓ)	$(4, 4)$	$(6, 5)$	$(8, 7)$
Private Key (bytes)	2,560	4,032	4,896
Public Key (bytes)	1,312	1,952	2,592
Signature (bytes)	2,420	3,309	4,627
Expected Iterations	4.25	5.1	3.85

These parameter selections demonstrate the fundamental trade-off between quantum security strength and implementation overhead. Signature sizes increase by factors of 30-70× relative to classical ECDSA schemes, reflecting the inherent cost of lattice-based post-quantum security.

3.3 MQTT Protocol and Security Integration

Message Queuing Telemetry Transport (MQTT) constitutes an OASIS standard messaging protocol implementing publish-subscribe architecture with minimal overhead for resource-constrained IoT devices. MQTT utilizes binary packet structure comprising fixed header (2-byte mandatory component specifying packet type and control flags), variable header (packet-specific control information), and payload (message content up to 256 MB).

MQTT specifies three Quality of Service levels affecting signature integration: QoS 0 (fire-and-forget transmission), QoS 1 (guaranteed delivery via PUBACK acknowledgments), and QoS 2 (exactly-once delivery through four-way handshake). Native security provisions include username/password authentication, TLS integration, and X.509 certificate-based mutual authentication, but lack built-in digital signature support.

3.4 ML-DSA Integration Challenges and Performance Impact

ML-DSA integration within MQTT environments presents three primary implementation approaches: payload-embedded signatures (preserving compatibility but substantially

increasing packet size), header extensions (requiring protocol modifications), and meta-message patterns (maintaining compliance with additional network overhead). Applications requiring non-repudiation necessitate asymmetric signatures like ML-DSA despite computational costs, while message authentication can utilize faster MACs with shared secrets.

ML-DSA signatures span 2,420-4,627 bytes compared to 64 bytes for ECDSA, representing 38×-72× overhead amplification. For typical IoT sensor data (10-100 bytes), signatures dominate packet composition, transforming 20-byte temperature measurements into 2.4-4.6 KB transmissions. ARM Cortex-M4 platforms require tens of milliseconds for signature generation and substantial memory resources (1.3-4.9 KB keys, tens of kilobytes working memory), creating processing bottlenecks that violate MQTT responsiveness guarantees.

Integration challenges include backward compatibility constraints, broker computational requirements, error handling extensions, processing power limitations, energy consumption escalation, and real-time constraint violations. These factors necessitate comprehensive empirical analysis to quantify performance trade-offs and inform practical deployment strategies within resource-constrained MQTT environments.

4 Implementation Architecture

5 Experimental Methodology

6 Results and Analysis

7 Conclusion

References

[Ano24] Anonymous. Improved ML-DSA hardware implementation with first order masking countermeasure. Cryptology ePrint Archive, Paper 2024/1817, 2024.

[BZB+22] Gustavo Banegas, Koen Zandberg, Emmanuel Baccelli, Adrian Herrmann, and Benjamin Smith. Quantum-resistant security for software updates on low-power networked embedded devices. In *Applied Cryptography and Network Security*, ACNS 2022. Springer, 2022. Also available at: https://eprint.iacr.org/2021/781.

[GMS19] Santosh Ghosh, Rafael Misoczki, and Manoj R. Sastry. Lightweight post-quantum-secure digital signature approach for IoT motes. Cryptology ePrint Archive, Paper 2019/122, 2019.

[HKS24] Vincent Hwang, YoungBeom Kim, and Seog Chung Seo. Multiplying polynomials without powerful multiplication instructions (long paper). Cryptology ePrint Archive, Paper 2024/1649, 2024.

[HKS25] Vincent Hwang, YoungBeom Kim, and Seog Chung Seo. Multiplying polynomials without powerful multiplication instructions. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(1):160–202, 2025. Extended version of Barrett Multiplication for Dilithium on Embedded Devices.

[HW23] James Howe and Bas Westerbaan. Benchmarking and analysing the nist pqc lattice-based signature schemes standards on the arm cortex m7. In *Progress in Cryptology - AFRICACRYPT 2023*, volume 14064 of *Lecture Notes in Computer Science*. Springer, 2023.

[KKPY24] Matthias J. Kannwischer, Markus Krausz, Richard Petri, and Shang-Yi Yang. pqm4: Benchmarking NIST additional post-quantum signature schemes on microcontrollers. Cryptology ePrint Archive, Paper 2024/112, 2024.

[KMLO19] Ayesha Khalid, Sarah McCarthy, Weiqiang Liu, and Maire O'Neill. Lattice-based cryptography for IoT in a quantum world: Are we ready? Cryptology ePrint Archive, Paper 2019/681, 2019.

[KS25] YoungBeom Kim and Seog Chung Seo. An optimized instantiation of post-quantum MQTT protocol on 8-bit AVR sensor nodes. In *Proceedings of the 2025 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '25, pages 1–19. ACM, 2025.

[KSD20] Panos Kampanakis, Dimitrios Sikeridis, and Michael Devetsikiotis. Post-quantum authentication in tls 1.3: A performance study. In *Proceedings 2020 Network and Distributed System Security Symposium*. Internet Society, 2020.

[Mar24] Dominik Marchsreiter. Towards quantum-safe blockchain: Exploration of pqc and public-key recovery on embedded systems. Cryptology ePrint Archive, Paper 2024/1178, 2024.

[NIS24] NIST. Fips 204: Module-lattice-based digital signature standard. Federal Information Processing Standards Publication, 2024. Available at: https://csrc.nist.gov/pubs/fips/204/final.

[SKD20] Dimitrios Sikeridis, Panos Kampanakis, and Michael Devetsikiotis. Assessing the overhead of post-quantum cryptography in tls 1.3 and ssh. In *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*, pages 149–156. ACM, 2020.

[WYQ+24] Yuxuan Wang, Jintong Yu, Shipei Qu, Xiaolin Zhang, Xiaowei Li, Chi Zhang, and Dawu Gu. Mind the faulty keccak: A practical fault injection attack scheme apply to all phases of ml-kem and ml-dsa. Cryptology ePrint Archive, Paper 2024/1522, 2024.