IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN XXXX-XXXX, Vol. 0, No. 0, pp. 1–3. DOI:XXXXXXXX

Post-Quantum Authentication for IoT: Optimizing 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 fundamental question of whether post-quantum authentication can be practically deployed in resource-constrained IoT environments remains unresolved. This research investigates the viability of ML-DSA integration within MQTT-based IoT systems, where severe limitations in computational resources, memory, and energy consumption present unprecedented challenges for post-quantum cryptographic deployment.

Keywords: Post-Quantum Cryptography · ML-DSA · Digital Signatures · 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. 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. However, the deployment of post-quantum cryptography encounters severe constraints in resource-limited environments, where Internet of Things (IoT) systems present fundamental challenges due to computational, memory, and energy limitations that may preclude practical implementation.

Existing research reveals a critical disparity between post-quantum standardization efforts and IoT deployment feasibility. While conventional network protocols have undergone extensive analysis for post-quantum migration [KSD20, SKD20], IoT-specific communication protocols remain insufficiently investigated. Empirical evaluations demonstrate that post-quantum signature schemes, particularly CRYSTALS-Dilithium implementations underlying ML-DSA, impose substantial computational overhead on ARM Cortex-M microcontrollers commonly deployed in IoT devices [BZB+22, Mar24]. Post-quantum signatures exhibit 30-70× size increases compared to classical schemes—ranging from 2,420 bytes (Level 1) to 4,595 bytes (Level 5) versus 64 bytes for ECDSA—while computational demands frequently exceed the processing capabilities of resource-constrained devices.

Comprehensive benchmarking studies have quantified the performance implications of post-quantum cryptography deployment on embedded systems. Banegas et al. [BZB+22] established that CRYSTALS-Dilithium signature operations require approximately 45% additional computational cycles compared to classical ECDSA implementations on ARM Cortex-M4 processors. Critical performance bottlenecks emerge in practical deployment

scenarios: analysis of the SUIT (Software Update for the Internet of Things) framework demonstrates that post-quantum signature verification operations can require up to 3.2 seconds on low-power microcontrollers, substantially exceeding acceptable latency constraints for real-time IoT applications.

Security analysis of embedded post-quantum implementations has identified significant attack vulnerabilities that exacerbate deployment challenges. 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]. These analyses demonstrate that Keccak-based hash functions—integral to ML-DSA randomness generation and signature computation—exhibit particular susceptibility to loop-abort faults that enable complete private key recovery, raising fundamental questions about the security assurance of post-quantum implementations in physically accessible IoT environments.

The MQTT protocol, widely adopted in IoT deployments due to its lightweight messaging characteristics, exemplifies the fundamental challenges of post-quantum migration in resource-constrained environments. Kim and Seo [KS25] demonstrate that direct application of post-quantum signatures to MQTT authentication introduces prohibitive performance overhead, prompting alternative 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 core challenge of post-quantum signature deployment. Signature-based authentication mechanisms remain essential for applications requiring cryptographic non-repudiation, comprehensive audit trails, and compatibility with existing public key infrastructure frameworks.

Current optimization research demonstrates the limitations of algorithmic improvements in addressing fundamental resource constraints. While 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], these optimizations provide insufficient performance gains to bridge the gap between post-quantum signature requirements and IoT device capabilities. The absence of comprehensive empirical studies specifically evaluating ML-DSA performance within MQTT protocol implementations represents a critical knowledge gap, particularly given MQTT's widespread adoption in industrial IoT deployments where signature-based authentication remains mandatory for regulatory compliance and security audit requirements.

References

[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.

[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.

[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.