IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN XXXX-XXXX, Vol. 0, No. 0, pp. 1–4. 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 advent of cryptographically relevant quantum computers poses a significant threat to current public-key cryptography systems. In response, NIST has standardized post-quantum cryptographic algorithms, including ML-DSA (Module-Lattice-Based Digital Signature Algorithm) based on CRYSTALS-Dilithium for secure digital signatures. This paper presents a comprehensive implementation and performance analysis of ML-DSA digital signatures integrated into the MQTT protocol for post-quantum migration in Internet of Things (IoT) environments. We implement ML-DSA variants with different security levels in resource-constrained IoT devices and evaluate their performance characteristics, including signature generation/verification times, memory consumption, and energy overhead on ARM Cortex-M4 microcontrollers. Our implementation addresses the unique challenges of post-quantum authentication in IoT environments, where computational resources, memory, and energy are severely limited. We investigate both pure post-quantum and hybrid classical-quantum approaches, with particular focus on certificate-less authentication mechanisms and protocol optimization techniques suitable for IoT deployments. Experimental results demonstrate that ML-DSA can provide viable post-quantum authentication for IoT devices with careful optimization, though significant challenges remain in signature size overhead and computational requirements. Our findings contribute to the emerging research area of post-quantum cryptography implementation in resource-constrained IoT protocols.

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

1 Introduction

The transition to post-quantum cryptography represents one of the most significant challenges in modern cybersecurity. With NIST's standardization of post-quantum cryptographic algorithms including ML-DSA (Module-Lattice-Based Digital Signature Algorithm) [NIS24b], organizations must now prepare for the migration from classical cryptographic systems that will be vulnerable to quantum attacks.

Internet of Things (IoT) environments present unique challenges for post-quantum cryptography deployment due to severe resource constraints in computational power, memory, and energy consumption. While traditional secure communication protocols like TLS have received significant attention for post-quantum migration [KSD20, SKD20], IoT-specific protocols such as MQTT have been largely unexplored in this context. Recent research has shown that post-quantum migration for IoT communication protocols remains an open challenge, with embedded devices requiring specialized optimization approaches [KS25].

This paper addresses the practical implementation of ML-DSA digital signatures in MQTT protocol frameworks, focusing on the unique constraints and requirements of

resource-limited IoT devices. Unlike traditional network environments, IoT deployments must consider factors such as limited RAM (often < 256 KB), constrained flash memory, energy efficiency for battery-powered devices, and real-time response requirements. We contribute:

- A comprehensive implementation of ML-DSA variants optimized for resource constrained IoT devices using ARM Cortex-M4 microcontrollers
- Performance analysis of ML-DSA integration with MQTT protocol, including memory consumption, computational overhead, and energy efficiency
- Investigation of certificate-less authentication mechanisms to reduce signature size overhead in IoT environments. Comparison with alternative approaches including KEM-based authentication and hybrid classical-quantum strategies

2 Background and Related Work

2.1 Post-Quantum Cryptography Standardization

NIST's Post-Quantum Cryptography standardization process, initiated in 2016, culminated in the publication of post-quantum cryptographic standards including various digital signature algorithms [NIS24b]. ML-DSA represents one approach to post-quantum digital signatures, providing multiple security levels corresponding to different classical security equivalents.

2.2 Embedded Systems and Post-Quantum Cryptography Research

The implementation of post-quantum cryptography on embedded systems has received increasing attention, with several key research efforts providing foundational insights. The pqm4 benchmarking framework has established performance baselines for post-quantum algorithms on ARM Cortex-M4 microcontrollers [KKPY24], demonstrating that lattice-based schemes including Dilithium (the basis for ML-DSA) can operate on resource-constrained devices with appropriate optimizations. Recent security analysis has revealed that embedded implementations of lattice-based signatures face unique vulnerabilities, including side-channel attacks and fault injection threats [RCDB24].

2.3 IoT Protocols and Post-Quantum Migration

Internet of Things communication protocols operate under fundamentally different constraints compared to traditional network protocols. MQTT (Message Queuing Telemetry Transport), widely deployed in IoT environments, prioritizes lightweight operation and minimal overhead [OAS19]. Recent research has demonstrated that direct application of post-quantum cryptography to IoT protocols faces significant challenges due to resource limitations [KS25].

The integration of post-quantum signatures into IoT protocols requires careful consideration of several factors: (1) computational overhead on resource-constrained microcontrollers, (2) memory consumption for signature storage and verification, (3) energy efficiency for battery-powered devices, and (4) network bandwidth limitations in low-power wireless networks. Previous work has shown that alternative approaches, such as KEM-based authentication using KEMTLS, can eliminate the need for post-quantum signatures entirely in some IoT scenarios [KS25], but this approach does not use the ML-DSA signature scheme.

However, signature-based authentication remains important for scenarios requiring non-repudiation, long-term security, and compatibility with existing certificate infrastructures.

This creates a research gap in understanding how ML-DSA can be effectively deployed in IoT environments while maintaining acceptable performance characteristics.

3 ML-DSA Algorithm Overview

3.1 ML-DSA Foundation and Characteristics

ML-DSA (Module-Lattice-Based Digital Signature Algorithm) is based on the CRYSTALS-Dilithium scheme and represents NIST's primary recommendation for post-quantum digital signatures [NIS24a]. The algorithm provides security guarantees against both classical and quantum adversaries through the hardness of the Module Learning With Errors (M-LWE) problem over polynomial rings.

For IoT applications, ML-DSA's characteristics present both opportunities and challenges. The algorithm offers good performance compared to other post-quantum signature schemes and has received extensive security analysis. However, the signature sizes (ranging from 2,420 bytes for Level 1 to 4,595 bytes for Level 5) represent a significant increase over classical signatures like ECDSA (64 bytes), posing challenges for bandwidth-constrained IoT networks.

3.2 Parameter Sets and IoT Deployment Considerations

ML-DSA defines multiple parameter sets providing different security levels, each with distinct implications for IoT deployment:

- **ML-DSA-44 (Level 1)**: Provides security equivalent to AES-128, with signature size of 2,420 bytes and public key size of 1,312 bytes
- **ML-DSA-65 (Level 3)**: Provides security equivalent to AES-192, with signature size of 3,293 bytes and public key size of 1,952 bytes
- **ML-DSA-87 (Level 5)**: Provides security equivalent to AES-256, with signature size of 4,595 bytes and public key size of 2,592 bytes

For IoT environments, the choice of parameter set involves critical trade-offs between security level, computational overhead, memory consumption, and network bandwidth usage. Level 1 parameters may be sufficient for many IoT applications while minimizing resource impact, though applications requiring long-term security may necessitate higher security levels despite the increased overhead.

The computational requirements also vary significantly across parameter sets, with Level 5 requiring approximately 40% more cycles for signature generation and 25% more for verification compared to Level 1 on ARM Cortex-M4 platforms [KKPY24].

4 Implementation Architecture

5 Experimental Methodology

6 Results and Analysis

7 Conclusion

References

[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.

[KS25] YoungBeom Kim and Seog Chung Seo. An optimized instantiation of post-quantum MQTT protocol on 8-bit AVR sensor nodes. Cryptology ePrint Archive, Paper 2025/563, 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.

[NIS24a] NIST. Fips 204: Module-lattice-based digital signature standard. Technical report, National Institute of Standards and Technology, 2024. Based on CRYSTALS-Dilithium.

[NIS24b] NIST. Post-quantum cryptography standards. NIST Post-Quantum Cryptography Standardization, 2024. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[OAS19] OASIS. Mqtt version 5.0 specification. OASIS Standard, 2019. Available at: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html.

[RCDB24] Prasanna Ravi, Anupam Chattopadhyay, Jan Pieter D'Anvers, and Anubhab Baksi. Side-channel and fault-injection attacks over lattice-based post-quantum schemes (kyber, dilithium): Survey and new results. *ACM Transactions on Embedded Computing Systems*, 23(3):1–54, 2024.

[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.