RADemics

Post Quantum Cryptographic Algorithms for Future Ready IoT Networks

G. Umarani Srikanth, S. Devisri
PANIMALAR ENGINEERING COLLEGE, VELLALAR COLLEGE OF ENGINEERING AND TECHNOLOGY

Post Quantum Cryptographic Algorithms for Future Ready IoT Networks

[1]G. Umarani Srikanth, Professor, Department of Computer science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu, India. umaranisrikanth@gmail.com

[2]S. Devisri, Assistant professor, Department of Computer Science and Engineering, Vellalar College of Engineering and Technology, Thindal, Erode. devivcet23@gmail.com

Abstract

The impending threat posed by quantum computing to classical cryptographic systems has accelerated the need for post-quantum cryptographic (PQC) solutions, particularly within the rapidly expanding domain of the Internet of Things (IoT). As IoT devices operate under severe constraints in terms of memory, processing power, and energy, integrating quantum-resilient algorithms presents both a critical necessity and a formidable challenge. This chapter provides a comprehensive study of PQC implementations on constrained IoT platforms, exploring algorithmic performance, memory consumption, execution time, and energy efficiency across various benchmarking environments. It offers a comparative analysis of bare-metal and RTOS-based deployments, evaluates the trade-offs between security and real-time responsiveness, and investigates power-aware scheduling and duty cycling strategies for secure task execution. Case studies involving smart sensors, medical wearables, and industrial nodes highlight the practical implications and optimizations required for effective PQC integration. Emphasis was placed on hardware-software co-design, library selection, and communication stack alignment to ensure future-ready, quantum-secure IoT deployments. This chapter bridges theoretical cryptographic resilience and applied system-level engineering, laying a foundational framework for scalable and secure post-quantum IoT ecosystems.

Keywords: Post-Quantum Cryptography, Internet of Things, Energy Efficiency, Real-Time Systems, Cryptographic Benchmarking, Hardware-Software Co-Design

Introduction

The emergence of quantum computing as a viable technological threat has introduced significant concerns over the long-term security of classical cryptographic algorithms [1]. Widely deployed public key schemes such as RSA, elliptic curve cryptography (ECC), and Diffie-Hellman key exchange are mathematically susceptible to quantum attacks, particularly through Shor's algorithm, which enables polynomial-time factorization and discrete logarithm solving [2]. These vulnerabilities have prompted global cryptographic communities to accelerate research and standardization of post-quantum cryptographic (PQC) algorithms designed to resist both classical and quantum adversaries [3]. Unlike symmetric cryptography, which can be made quantum-resistant with increased key sizes, public key cryptography requires a complete redesign of the underlying mathematical problems [4]. As the future of digital security hinges on the proactive adoption of quantum-safe solutions, the urgency to transition from legacy algorithms to PQC standards has never been greater [5].

The Internet of Things (IoT) represents a particularly sensitive domain in this cryptographic shift, due to its scale, diversity, and intrinsic hardware limitations [6]. IoT systems encompass billions of interconnected devices ranging from simple sensors and wearables to autonomous vehicles and critical infrastructure controllers [7]. These devices typically operate under severe constraints in processing power, memory, storage, and energy consumption [8]. Integrating PQC into such environments poses unique implementation challenges, as post-quantum algorithms generally require larger key sizes, more memory, and higher computational loads compared to their classical counterparts [9]. These constraints must be addressed through optimized code design, lightweight protocol integration, and tailored hardware-software co-design strategies that align cryptographic operations with system capabilities without degrading performance or reliability [10].