RADemics

Post-Quantum Cryptographic Frameworks for Securing IoT-Enabled Power Electronics in Smart Grid and Industrial Applications

P Santhosh , R. Jegadeesh Kumar
Hyderabad Institute of Technology and Management,
Karpagam College of Engineering

11. Post-Quantum Cryptographic Frameworks for Securing IoT-Enabled Power Electronics in Smart Grid and Industrial Applications

[1]P Santhosh, Assistant Professor, Electronics and Communication Engineering Department, Hyderabad Institute of Technology and Management, santhoshp.ece@hitam.org

[2]R. Jegadeesh Kumar, Assistant Professor, Department of Electrical and Electronics Engineering, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India jegadeeshkumar.eee@gmail.com

Abstract

The rapid advancement of quantum computing poses a significant threat to classical cryptographic mechanisms, necessitating the integration of Post-Quantum Cryptography (PQC) into security frameworks for IoT-enabled power electronics. Smart grids and industrial automation systems rely on interconnected IoT devices for real-time control, monitoring, and data exchange, making them highly vulnerable to emerging quantum threats. This book chapter explores PQC frameworks tailored for securing power electronics in smart grid and industrial applications, addressing critical challenges such as computational overhead, communication latency, system compatibility, and scalability. The impact of PQC on real-time performance was evaluated, considering its influence on industrial IoT networks, cryptographic handshake efficiency, and data transmission reliability. Hybrid cryptographic solutions that combine classical and post-quantum approaches are assessed for their feasibility in power electronics IoT systems. Security resilience under adverse network conditions, including cyberattacks and network disruptions, was also analyzed to ensure seamless PQC integration without compromising operational stability. Through a comprehensive study of PQC implementation, performance optimization, and interoperability testing, this chapter provides insights into the future of secure and resilient power electronics systems in quantum-era cybersecurity landscapes.

Keywords: Post-Quantum Cryptography, Power Electronics, IoT Security, Smart Grid, Industrial Automation, Hybrid Cryptographic Solutions.

Introduction

The increasing digitization and interconnectivity of power electronics in smart grid and industrial applications have significantly improved efficiency, automation, and real-time decision-making [1,2]. These advancements also introduce substantial cybersecurity risks, particularly as quantum computing emerges as a disruptive force capable of breaking classical cryptographic algorithms [3]. Power electronics systems, which form the backbone of modern energy infrastructure, rely heavily on secure communication and data integrity to ensure reliable operations [4,5]. The transition to Post-Quantum Cryptography (PQC) was crucial to protecting these critical systems from potential quantum threats. Unlike conventional encryption mechanisms

such as RSA and ECC, PQC algorithms are designed to resist quantum-based attacks, providing long-term security for IoT-enabled power electronics [6]. The implementation of PQC in these systems was essential to maintaining data confidentiality, ensuring the authenticity of control commands, and preventing unauthorized access that could lead to catastrophic failures in power distribution networks [7].

The integration of PQC into IoT-enabled power electronics presents several technical challenges, particularly in terms of computational efficiency and communication overhead [8]. Power electronics applications, including smart inverters, industrial motor drives, and grid monitoring systems, operate under stringent real-time constraints [9]. Many of these devices have limited processing power and memory, making it difficult to accommodate the increased computational demands of PQC algorithms [10, 11]. Power grid communication relies on established industrial protocols such as IEC 61850 and DNP3, which were not originally designed to support the large key sizes and complex operations associated with quantum-resistant encryption [12]. As a result, optimizing PQC implementation for power electronics IoT networks requires a careful balance between security and performance, ensuring that cryptographic enhancements do not hinder real-time responsiveness [13].

Another significant concern was the scalability and interoperability of PQC within heterogeneous power electronics systems. Industrial automation and smart grid networks consist of a diverse range of IoT devices, including sensors, actuators, intelligent controllers, and cloud-based analytics platforms [14]. Ensuring seamless PQC deployment across these interconnected systems requires compatibility testing and standardization efforts to integrate quantum-resistant encryption without disrupting existing cybersecurity frameworks [15]. Hybrid cryptographic solutions that combine classical and post-quantum encryption schemes are being explored as a transitional approach to facilitate gradual migration to full PQC adoption [16,17]. These solutions leverage the efficiency of classical cryptography while incorporating PQC-based security enhancements for future-proofing against quantum attacks [18]. Evaluating the feasibility of hybrid approaches was essential to determining their effectiveness in securing power electronics without imposing excessive computational burdens on resource-constrained IoT devices [19].

Beyond computational and compatibility challenges, the resilience of PQC in adverse network conditions must also be considered [20]. Power grids and industrial automation systems often operate in environments where network disruptions, latency variations, and cyberattacks are common. Implementing PQC should not introduce new vulnerabilities that could compromise system stability or real-time control functions [21]. The increased key sizes and cryptographic handshake complexity of PQC protocols could lead to higher latency in secure communication channels, potentially affecting critical operations such as grid synchronization and load balancing [22]. Additionally, network security threats such as denial-of-service (DoS) attacks and packet interception attempts must be evaluated in the context of PQC integration to ensure that post-quantum security frameworks enhance, rather than weaken, existing cyber defense mechanisms [23].

This book chapter explores the challenges, optimization techniques, and practical considerations for deploying PQC in IoT-enabled power electronics used in smart grids and industrial automation [24]. It provides a detailed analysis of the impact of PQC on system latency, communication efficiency, and computational performance while assessing the feasibility of hybrid cryptographic solutions. The discussion also includes real-world testing scenarios to

evaluate PQC resilience under network disruptions and cyber threats [25]. By addressing these critical factors, this chapter aims to provide a comprehensive framework for adopting quantum-resistant security solutions in power electronics, ensuring a robust and future-proof cybersecurity infrastructure for next-generation energy systems.