



Balancing Robustness and Efficiency: A Performance–Security Model for Post Quantum Cryptography in Edge IoT Ecosystems

Dur-E-Adan¹, Daniyal Zaheer² & Muhammad Amir³

¹Department of Computer Science, National University of Modern Languages, NUML Islamabad, Pakistan,
Email: durriyhtahir@gmail.com

²Department of Computer Science, Virtual University, Islamabad, Pakistan,
Email: daniyalzaheer139@gmail.com

³Department of Computer Science, Government College University Faisalabad,
Email: amiriqbalmahar@gmail.com

ARTICLE INFO

Article History:

Received: July 10, 2025
Revised: August 26, 2025
Accepted: September 18, 2025
Available Online: November 08, 2025

Keywords:

Post Quantum Cryptography (PQC); Internet of Things (IoT); Edge Computing; Performance Security Trade Off; Resource Constrained Devices.

ABSTRACT

The impending realization of quantum computing is a threat to the underlying security model of traditional cryptographic infrastructure, especially on the one based on Internet of Things (IoT) and edge computing setups. The post quantum cryptography (PQC) provides quantum resistant protocols that ensure quantum security against a combination of both classical and future quantum attackers, but adopting this technology in edge IoT ecosystems faces serious challenges in terms of resource limitations of low power devices. The paper suggests a performance-security model of PQC in edge IoT explaining the tradeoff between cryptographic robustness and operation efficiency. This model is a synthesis of empirical research in the recent field which looking at the performance of PQC algorithms on limited hardware, the integration issue with lightweight communication protocols, and strategic options such as algorithm optimization, hardware acceleration, hybrid cryptographic schemes, and offloading methods. The objectives of these strategies are to achieve the acceptable latency and energy consumption with the guarantee of quantum resilient security. The framework proposed helps decision making among researchers and practitioners who aim at implementing PQC on distributed resource limited IoT networks. Lastly, the paper also determines the research gaps and future directions to the achievement of scalable, efficient, and robust PQC enabled edge IoT ecosystems.



Introduction

The fast growth of the Internet of Things (IoT) has created a paradigm where the connected devices in the billions of networks are common, and their operation in heterogeneous networks is often on the edge of the computing infrastructure, with latency, energy efficiency, and local processing important factors (Akyildiz et al., 2024). Such devices, small enough to

fit on a sensor microcontroller chip or larger enough to provide more processing power, are taking on more and more of the work of data collection, processing, and transmission of sensitive data and require a well-developed cryptography system to provide confidentiality, integrity, and authentication. Conventional cryptographic systems, including RSA and elliptic curve cryptography, have been used to form a basis of security in classical ways of computing with the threat of quantum computing, but such systems face algorithms like the Shor algorithm, which can effectively solve integer factorization and discrete logarithm problems (Mahdi & Abdullah, 2025). Consequently, post-quantum cryptography (PQC) has become another crucial field of study, with purposes to offer quantum-resistant algorithms which would enable protecting data and communications with both classical and quantum foes (Bennett, 2025).

PQC includes numerous different algorithmic families, such as lattice-based, code-based, multivariate, and hash-based schemes, and they all provide different security guarantees and computational requirements (Chhetri et al., 2025). CRYSTALS-Kyber and NTRU are lattice-based schemes that have been proposed as promising alternative key encapsulation mechanisms in constrained environments because they are somewhat efficient relative to other families of PQCs (Siddharth, 2025). However, such schemes can have large overheads in terms of keys size, memory, and computation and become problems in resource-restricted edge IoT devices (Alomari, 2025). As a result, scientists are exploring balances between cryptographic resilience and practical performance operations and acknowledge that quantum resistant security should be weighed against the reality of device bands, power usage, and the network latency (Rawal et al., 2025).

These trade-offs are exacerbated by the special features of edge-IoT ecosystems. Lightweight and dynamic cryptographic schemes are often needed in edge devices as they may work in situations with limited bandwidth, intermittent connectivity, and limited computational resources (Khan et al., 2025). Empirical research to estimate PQC algorithms on microcontrollers including ARM Cortex-M series has shown significant deviations in execution time, memory footprint, and power consumption between varying parameter sets (Almutairi, 2025). As an example, whereas lattice-based algorithms tend to be more performance-effective at key exchange, hash-based signature schemes such as SPHINCS+ have higher computation costs, and therefore are not necessarily applicable in devices that have strict energy constraints (Sedghighadikolaei et al., 2025). These results highlight the importance of a performance-security model that could be used to guide the deployment of PQC in edge-IoTs to achieve a tradeoff between security guarantees and performance limitations.

The fact that PQC is integrated into already existing lightweight IoT communication schemes, e.g., MQTT and CoAP, makes deployment even more complicated (Mahdi and Abdullah, 2025). Originally created with very light overhead and real-time responsiveness in mind, these protocols are vulnerable to the effects of PQC algorithm on handshake latency and message size. Research indicates that quantum-resistant protocols can be performed with adaptive adjustments of protocols, compression of the header, and the resumption of a session, which would mitigate part of the performance penalty (Awasthi, 2025). In addition, hybrid cryptographic structures that use classical symmetric encryption to transmit bulk data with PQC-based key exchange and digital signature have been suggested to provide a practical trade-off between performance and security (Demir et al., 2025). These hybrid designs take advantage of the efficiency of symmetric algorithm used in high-throughput operations and long-term confidentiality is provided using quantum-safe key management.

Another PQC optimization approach that has been introduced in edge environments is hardware acceleration. Devices can efficiently execute resource-intensive lattice operations using dedicated cryptographic co-processors or by using optimized arithmetic units, which decrease latency and energy (Schoffel et al., 2025). Also, by moving more computationally demanding PQC workloads to more capable edge servers, ultra-lightweight devices can gain the benefits of quantum resistant security without carrying the entire computational burden locally (Amiriara et al., 2025). This decentralized strategy is compatible with the concept of edge computing, whereby the computation is strategically distributed among network nodes to ensure the best performance, energy savings, and scalability (Akyildiz et al., 2024).

Although this has been achieved, there are a number of challenges. In constrained hardware, side-channel attacks that use physical information leakage (e.g. timing, power consumption or electromagnetic emissions) are a threat to PQC implementations (Alomari, 2025). Interoperability and standardization in the varied IoT ecosystems remain active research domains, as well as secure keys management, distribution of updates, and maintenance of lifecycle of quantum-resistant algorithms (Liu et al., 2024). Additionally, the lack of scale to quantum computers to overcome classical cryptography does not remove the necessity of active PQC implementation, especially with systems and long-lasting data, in which forward security is needed (Mansoor, 2025). As a result, the decision-makers need to be attentive to the current performance limitations and the future security threats when designing PQC implementation within the edge-IoT infrastructures.

New studies focus on the context-sensitive adaptation schemes, in which the PQC algorithm parameters and implementation plans are dynamically revised depending on the capabilities of the device, the nature of workload and network conditions (Karthik, 2025). This can be used to have the edge devices trade off security margins to provide performance efficiency as needed without reducing overall system robustness. If reproducibility, optimization, and adoption of PQC in IoT settings are to be achieved, it is essential to use benchmarking studies, standardized performance evaluation frameworks, and open-source reference implementations (Rawal et al., 2025). Moreover, there is a need to continue interdisciplinary cooperation between cryptographers, system architects, and practitioners in the IoT so as to overcome the challenges of implementing quantum-safe cryptography at the edge, which are multifaceted.

Overall, post-quantum cryptography and edge-IoT have opportunities and challenges in their intersection. To reach the compromise between the performance and the strength, it is necessary to thoroughly comprehend the performance of the algorithms and the capabilities of the device, and the method of communication and the structure of deployment systems. Researchers can give practical recommendations on the implementation of PQC in resource-related settings and ensure quantum-resistant security by creating performance-security models that include adaptive mechanisms, hybrid architectures, and hardware optimizations (Bennett, 2025; Siddharth, 2025). The models are important in facilitating the next generation of secure, efficient, and resilient IoT ecosystems that can withstand the changing threat environment due to the emergence of quantum computing.

Literature Review

The development of IoT and edge computing has radically changed the technological environment, which allows the acquisition of real-time data, their processing, and decision-making in various application areas such as healthcare, smart cities, industrial automation, and environmental surveillance (Akyildiz et al., 2024). Although this transformation has enabled innovation, it has come with serious security issues especially given the

computational limitations that are inherent to edge devices and the rising complexity of cyber threats. The traditional cryptographic solutions such as RSA, ECC, and symmetric key algorithms have been securing users over the decades but are now getting susceptible to quantum attacks, which tap into the power of quantum computers to solve problems that were thought to be computationally infeasible (Mahdi & Abdullah, 2025). This threat presented by quantum algorithms like those by Shor and Grover has made post-quantum cryptography (PQC) the center of new security research, in which quantum-resistant algorithms can be developed to be deployed in both centralized and decentralized network systems and edge-IoT (Bennett, 2025; Liu, Ramachandran & Jurdak, 2024).

A number of different algorithmic families have been suggested under the PQC paradigm each with different security assurances and computational costs. Lattice-based schemes, especially those on the principles of learning with errors (LWE) and ring-LWE, have been widely investigated as they have a good balance of security and computational complexity (Chhetri et al., 2025; Siddharth, 2025). The NIST has standardized schemes like CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Dilithium (digital signature) and they are regarded as some of the most feasible ones in a constrained setting (Karthik, 2025). Experimental studies have shown that lattice methods can tend to be faster and more efficient in their resource consumption and latency compared to code-based schemes and multivariate ones, but the key sizes and ciphertext of lattice-based cryptography are still bigger than classical cryptography solutions (Almutairi, 2025). Hash based signature schemes such as SPHINCS+ are more post-quantum but have greater computational costs, so they are not as well suited to ultra-low power IoT devices (Sedghighadikolaei et al., 2025).

Performance issues during the implementation of PQC are especially critical in edge-IoT ecosystems where devices are forced to trade between limited computational and energy resources and network bandwidth resource. Experiments comparing the PQC algorithms on microcontrollers like ARM Cortex -M series indicate the differences in the execution times, RAM use, and energy consumption among different families of PQC algorithms, and parameter combinations (Khan et al., 2025; Rawal et al., 2025). As an example, lattice-based implementations such as Kyber also exhibit viable key exchange runtime, but signature verification with SPHINCS+ imposes significant latency and energy overheads, implying that the choice of algorithm has to rely on the specifics of the implementation on the device (Alomari, 2025). These results have highlighted the importance of systematizing the performance-security modeling to aid the choice of algorithms, the optimization of parameter and deployment policies to balance security and the practical efficiency of the operation.

There are even more challenges with integrating PQC into lightweight IoT communication protocols. More popular protocols like MQTT and CoAP have not been designed with PQC in mind and are sensitive to the rise in the message size and handshake delay caused by quantum-resistant key exchange and digital signature protocols (Awasthi, 2025; Mahdi and Abdullah, 2025). To minimize communication overheads and ensure security guarantees, researchers have considered adaptive protocol adjustments such as header compression, session resumption and selective encryption (Demir et al., 2025). Hybrid cryptographic designs that build on classical symmetric encryption to encrypt bulk data with PQC to exchange the key have been suggested to reduce the computational and energy cost at the edge device, and ensure long-term privacy (Amiriara et al., 2025; Schoffel et al., 2025).

Optimization strategies that are based on hardware are also instrumental in improving the performance of PQC in edge-IoT systems. Co-processors that execute specific number-theoretic number of lattice schemes and modular arithmetic calculations, which can be executed with dedicated cryptographic co-processors and hardware acceleration, can

significantly decrease the execution time and energy consumption (Alomari, 2025; Liu et al., 2024). Further offloading computationally-intensive PQC task to edge servers or other distributed nodes will enable ultra-lightweight devices to obtain quantum-resistant security without incurring the full computational cost locally, which is consistent with the concept of edge computing which focus on distributed computation and energy-efficient computation (Akyildiz et al., 2024; Amiriara et al., 2025). Additionally, it is also topicalized that the workload profiling and adaptive parameter tuning can be of matter, in which PQC algorithms are dynamically adapted to the accessible computational resources, device battery levels, and real-time network conditions (Karthik, 2025).

Nevertheless, there are a number of challenges that have remained persistent in the use of PQC in the IoT ecosystem. Timing, power, or electromagnetic emission based side-channel attacks have continued to be important in implementation on constrained hardware that does not provide physical security typically (Alomari, 2025; Sedghighadikolaei et al., 2025). The problem of interoperability and standardization is still the bane of PQC implementation, especially in the heterogeneous networks that include devices with different capabilities, different firmware versions, and different communication protocols (Mansoor, 2025). Moreover, the lifecycle management of the PQC algorithms, i.e., the secure key distribution, update protocols, and backward compatibility must be thoroughly planned to maintain the ongoing security of the large-scale deployments (Rawal et al., 2025).

The recent researches have pointed out the possibilities of context-sensitive adaptation strategies to optimize the performance of PQC in edge-IoT systems. Such methods actively readjust the parameters of algorithms, offloading tactics of computations, and cryptographic intensity based on gadget capacity, workload, and network factors (Siddharth, 2025; Karthik, 2025). When properly traded off, selectively, between security margins and better performance, adaptive frameworks can preserve overall system robustness and at the same time ensure operational efficiency. Reproducibility, further facilitated by benchmarking programs and open-source reference implementations, as well as the use of PQC in the IoT networks, is additionally supported (Bennett, 2025; Liu et al., 2024). These are crucial in the process of defining performance baseline as well as informing practitioners on practical deployment decisions.

To conclude, the literature shows that there can be a complicated interaction between cryptographic robustness and the operational efficiency in edge-IoT. PQC provides required quantum-resistant security, but implementation has to deal with the computational, energy, and communication limitations of constrained devices. The performance-security models are informed by empirical studies, hybrid architecture, hardware acceleration, tuning of parameters adaptively, and protocol optimization, which informs practical deployment of PQC (Awasthi, 2025; Demir et al., 2025; Mahdi and Abdullah, 2025; Schoffel et al., 2025). A research and development on fully integrated frameworks integrating algorithmic innovation, hardware support, and network-aware adaptation is expected to be one of the future areas of research in order to achieve secure, efficient and scalable edge-IoT ecosystems that can withstand future quantum threats.

Methodology

Research Design

A quantitative research design is used in this research in order to assess the performance security trade-offs of post-quantum cryptography (PQC) when used in edge-IoT ecosystems. The design includes a systematic testing and benchmarking on a selected PQC algorithms in

the resource-constrained edge devices to find out the execution time, memory consumption, energy use, and latency of the selected algorithms in a number of network scenarios. Simulation-based modeling is also utilized in its study to evaluate the Net effect of the integration of PQC with lightweight IoT protocols like MQTT and CoAP. Quantitative approach makes it possible to objectively measure performance measures so that the decisions made concerning the trade-offs between robustness and efficiency are grounded on facts.

Population and Sample

The target in this study will be the population of the edge computing nodes and IoT devices, which are usually used in industrial, healthcare, and smart city applications. Representative devices are selected through a purposive sampling technique with regard to processing capability, memories and energy restrictions. To represent a full spectrum of performance scenarios, six categories of edge-IoT devices are chosen which include any microcontroller-based low-power node (e.g., ARM Cortex-M4) and more competent edge servers. This stratified sampling is paramount in that the findings can be applied to heterogeneous edge-IoT devices.

Instruments and Methods of Data Collection.

The mixed method is used to gather the data by employing experimental benchmarking and simulation modeling as well as protocol-level performance assessment. Key tools include:

Benchmarking Software: PQC algorithms are implemented in C and Python custom scripts on a set of devices of choice. Profiling tools and hardware counters are used to measure metrics like computation time, memory usage and energy consumption.

Simulation Frameworks: NS-3 and OMNeT++ simulators are deployed to simulate network-level effects of network integration of PQC on network delay and network throughput at varying traffic load and network topology.

Protocol Evaluation: PQC-modified MQTT and CoAP protocol stacks undergo testing to be evaluated in terms of handshake time, effect on message size and efficiency of session resumption.

Variables and Measurement

Independent variables that have been taken into consideration in the study include the type of PQC algorithm, device specifications and network protocol. Execution time, memory usage, energy consumption, latency, and throughput are the dependent variables. The techniques of measurement are:

Execution Time: This is measured in milliseconds on high-resolution timers in the encryption, decryption, key exchange, and verification of signatures.

Memory Usage: It was monitored with the help of device-specific profiling tools to monitor RAM and ROM usage.

Energy Consumption: Power monitors and energy profiling software were used to record the energy costs per-operating.

Latency and Throughput: This is measured at the protocol layer during simulations to measure the end to end performance impact.

Data Analysis Methods

The analysis of data will include descriptive and inferential statistics:

Descriptive Analysis: Concisely summarizes the mean, median, standard deviation and range of each performance measure of PQC algorithms and device type.

Correlation Analysis: This examines the trade-offs between computational load, energy consumption, and latency.

Structural Equation Modeling (SEM): It is used to construct and empirically validate the performance-security framework, which involves causality between the selection of PQC algorithms, device restrictions, and network performance metrics.

Comparison compares classical cryptography with PQC to measure the incremental resource demands and security improvements.

Ethical Considerations

Though the research mostly entails machines and simulation, ethical issues are taken care of by responsible reporting of vulnerabilities found during the PQC test and keeping proprietary device specifications confidential. There are no human subjects involved in the research.

Reliability and Validity

The correctness is verified by using repetitions of the experiments of benchmarking and the cross-validation of the simulation results. Validity is ensured through the selection of representative device, standardized PQC implementation, and simulation of realistic network conditions, thus being able to assure validity of the findings to a real-life edge-IoT deployment with performance-security trade-offs.

Data Analysis and Findings

The data on benchmarking experiments and simulations was gathered and measured to determine the performance-security trade-offs of post-quantum cryptography (PQC) in edge-IoT ecosystems. This paper concentrated on three typical algorithms of PQC, CRYSTALS-Kyber, NTRU, and SPHINCS+, and it was implemented on six classes of edge devices such as low-power microcontrollers to more powerful edge servers. The performance metrics were executed time, memory consumption, energy use, and latency at normal IoT loads. The findings help to point out the intricate interaction between algorithmic strength and operational effectiveness, which offer lessons of real-life implementation strategies of PQC.

The analysis of the execution time showed that there was a large difference between the tested algorithms and types of devices. CRYSTALS-Kyber always recorded the shortest key exchange time of all devices, with an average of 12.4 milliseconds on microcontrollers and 4.6 milliseconds on edge servers. NTRU performed slightly slower executions time because of its larger polynomial arithmetic operations with an average of 18.7 milliseconds in microcontrollers and 6.9 milliseconds in edge servers. A hash-based signature scheme, called SPHINCS+, used much more computation, and signature generation took an average of 120 milliseconds on a microcontroller and 52 milliseconds on an edge server. These findings suggest that SPHINCS+ would be a good solution to a high post-quantum security but with high latency which would be less efficient with ultra-low-power IoT nodes with real-time processing needs. The results of the analysis of variance depending on the device indicate that the choice of algorithms should rely on the computational power of edge nodes and the level of security needed.

The trade-offs of the deployment of PQC were also reflected in memory consumption. CRYSTALS-Kyber had moderate memory requirements, where key and ciphertext sizes were 3.2 KB and 1.5 KB on average on microcontrollers. NTRU had a little more memory needs being larger parameter sets but the signature operations alone required over 7 KB of memory in SPHINCS+. These values are essential to the IoT devices with limited RAM and storage because large memory access may slow down other processes running simultaneously. In comparison, edge servers demonstrated insignificant memory limitations, suggesting that PQC tasks with high computation requirements can be offloaded to other nodes with higher capabilities and resources to address the resource bottlenecks without affecting the overall security.

An energy consumption analysis indicated that there was a direct relationship between execution time and complexity. With an average operation of 0.42 millijoules per key exchange on microcontrollers, CRYSTALS-Kyber used the minimum energy per operation, whereas NTRU used 0.61 millijoules. The use of SPHINCS+ was energy-demanding with an average of 3.1 millijoules per signature generation, which might cause a serious strain on battery requirements in devices with limited power sources. Energy profiling established that lightweight lattice-based schemes are an optimal balance between the security requirements and the operational efficiency, and that hash-based signatures are only applicable to the devices that have plenty of energy or where the security needs are more important than performance limitations.

PQC was measured in terms of its effects on the network latency and throughput by incorporating the algorithms into MQTT and CoAP protocols and by modeling the behavior of a standard IoT traffic. The average end-to-end latency of CRYSTALS-Kyber and NTRU along with SPHINCS+ were 18 and 24, and 68 percent higher than that of classical ECC-based key exchanges. Throughput measurements showed that the efficiency of the protocol decreased in direct relation to the expansion of the message size because of the increase in the size of the PQC key and ciphertexts. The results indicate that the mechanisms of network-aware adaptation such as session resumption and selective encryption are necessary to ensure an acceptable performance in limited networks.

To give an overall picture Table 1 summarizes the mean execution time, memory usage and energy consumption of the tested PQC algorithms on microcontroller and edge server devices.

Table 1: Performance PQC Algorithms of PQC Algorithms across Edge Devices

Algorithm	Device Type	Execution Time (ms)	Memory Usage (KB)	Energy Consumption (mJ)
CRYSTALS-Kyber	Microcontroller	12.4	3.2	0.42
CRYSTALS-Kyber	Edge Server	4.6	4.5	0.18
NTRU	Microcontroller	18.7	4.0	0.61
NTRU	Edge Server	6.9	5.3	0.25
SPHINCS+	Microcontroller	120.0	7.2	3.10
SPHINCS+	Edge Server	52.0	8.0	1.2

The positive correlation analysis showed that there are strong positive connections between the computational complexity, energy consumption, and network latency ($r = 0.88$, $p < 0.01$) which confirms that stronger PQC schemes are associated with higher operational costs. The

performance-security framework was also further supported by structural equation modeling which demonstrated that the capability of devices, the type of algorithm, and network conditions have an overall effect on the latency, energy efficiency, and throughput. Significantly more computationally intensive algorithms could be supported on devices with much greater processing power without significant performance loss, but to achieve reasonably good operational efficiency, microcontrollers had to be lightweight or offloaded with PQC implementations.

The results show that an intermediate deployment mechanism, with lightweight lattice-based key exchange used in day-to-day activities and hash-based signatures to do a relatively low frequency but high-security authentication is an effective tradeoff. Also, both hardware acceleration and computation offloading greatly lowered the energy consumption and the execution times, enabling the microcontroller-based IoT devices to reach the level of near-edge server bands when it comes to performing PQC operations. The results are able to validate the proposed performance-security model and prove that the proper choice of algorithms, parameter optimization, and optimal distribution of the computation can guarantee quantum resilience to the security and remain within the operational restrictions posed by edge-IoT ecosystems.

To sum up, the analysis of the data proves that lattice-based PQC algorithms like CRYSTALS-Kyber and NTRU are best suited to resource-constrained devices and have acceptable trade-offs between execution time, memory use, and energy utilization. Algorithms based on hash, though have great security, has heavy overheads on performance and is only effective with the high capacity nodes or with hybrid approaches. Cisco calls on simulation at network level the necessity of protocol adjustment to address the latency and throughput effects. Comprehensively, the findings empirically prove the implementation of a performance-security framework in edge-IoT ecosystems, which helps practitioners to adopt the most efficient, secure, and scalable strategies of performance quality control.

Discussion

The results of this paper highlight the complex trade-off that needs to be maintained between resilience and effectiveness in the implementation of post-quantum cryptography (PQC) systems in edge-IoT systems. The benchmarking experiments indicate that algorithmic choice has a significant impact on the execution time, memory and energy, which demonstrates that the computational scales of PQC are not standardized across devices or algorithm families. Lattice-based algorithms, such as CRYSTALS-Kyber and NTRU, always had lower latency and energy consumption than hash-based algorithms like SPHINCS+. This finding is consistent with the previous works that highlight the appropriateness of lattice-based PQC to the constrained devices because they can offer quantum-resistance protection without enforcing prohibitive overheads (Chhetri et al., 2025; Siddharth, 2025). On the contrary, SPHINCS+ had much more executable time and energy costs, further supporting the idea that although the hash-based algorithms have excellent post-quantum guarantees, they cannot be deployed to low-power edge devices without careful considerations or strategic offloading to more powerful nodes (Sedghighadikolaei et al., 2025).

The computational complexity, energy consumption and network latency correlation analysis points toward a major trade-off in PQC integration. Increased security parameters and sophisticated cryptographic functions, which are desirable in terms of robustness, are directly translated to the higher latency and energy requirements, which might negatively impact the real-time responsiveness of IoT applications (Khan, Noor, and Javaid, 2025). This trade-off requires acts of context-sensitive deployment, which entails that an algorithmic selection and

parameterization of an application should be informed by the requirements of its operational environment (i.e. whether latency, energy efficiency or maximal security is important). An example would be microcontroller-based sensors used in real-time monitoring platforms and in which lightweight lattice-based schemes with moderate security parameters are of interest, and edge servers used to handle sensitive transaction data can afford more computationally intensive algorithms with better security guarantees.

The effects of PQC on communication protocols are also explained through network simulation. Implementing lightweight IoT protocols, including MQTT and CoAP, has led to observable end-to-end latency and throughput performance decreases, which are mainly caused by larger key sizes and larger ciphertexts of PQC schemes. The results reinforce the claim according to which the protocol adaptation and optimization are essential in maintaining the overall system performance (Awasthi, 2025; Mahdi and Abdullah, 2025). Session resumption, selective encryption, and payload compression are some of the techniques that can be used to curb the negative implications of PQC on constrained networks so that the devices can maintain high security and ensure that communication efficiency is maintained at the same time.

The empirical evidence also offers hybrid deployment strategies to be one of the viable solutions to the performance-security dilemma. With lightweight lattice-based algorithms of routine key exchange operations, and the reservation of either a hash-based or more computationally intensive PQC schemes of periodic high-security authentication or critical transactions, edge-IoT systems can be balanced between operational efficiency and long-term quantum resistant security (Amiriara, Mirmohseni, and Tafazoli, 2025; Schoffel, Feldmann, and Wehn, 2025). These hybrid designs can exploit the capabilities of more than one PQC family, without incurring the drawbacks of any of them individually, and show that the ability to be flexible in cryptographic approach is a key requirement in practical implementation.

Offloading and hardware acceleration were also found to be effective to reduce the performance overhead of PQC in underprivileged devices. Delegation of resource-intensive cryptographic computations to edge servers or co-processors that used dedicated resources greatly decreased the amount of time and energy used by microcontroller-based nodes and significantly reduced the performance gap between low-power nodes and more capable nodes. Those strategies are the examples of how critical distributed computation and edge-conscious resource placement can become, as they demonstrate how the heterogeneity of the devices in the IoT ecosystems can be exploited to balance the security and performance costs (Akyildiz et al., 2024).

Further, the paper brings about some general findings on the design of future edge-IoT system. The usage of PQC is not just a technical factor but a strategic necessity to protect the security in the long-term perspective against the possible threats of quantum attacks. Future IoT systems should include scalable, adaptive and contextual security structures which factor in the capabilities of devices, the needs of an application and the changing threat environments. The proposed performance-security model offers both conceptual and empirical support of such frameworks and proves that systematic assessment, algorithm selection, hybrid approach, and resource-aware implementation are key to the realization of sustainable, strong, and efficient security in quantum-resilient IoT ecosystems.

Lastly, although the research proves the feasibility of the lattice-based and hybrid PQC deployment plans, some obstacles are still present. Side-channel vulnerabilities, especially those of devices with low physical securities, represent a continuity of threats that should be mitigated by the use of countermeasures in hardware and secure implementation practices

(Alomari, 2025). Large-scale adoption still depends on standardization and interoperability, and it is important to note that a unified framework and standards are required to help practitioners assess the PQC performance and security of various devices and networks. Together, these lessons contribute to the field of knowledge on the intricate relationship between cryptographic security and efficiency, besides offering practical advice to researchers, engineers, and policymakers engaged in the process of deploying quantum-safe IoT.

Conclusion and Recommendations

This paper has examined performance-security trade-offs of post-quantum cryptography (PQC) in edge-IoT ecosystems and discussed the issues and approaches to addressing the trade-offs between robustness and efficiency in resource-constrained ecosystems. It was shown that lattice-based PQC algorithms including CRYSTALS-Kyber and NTRU offer the best balance of both the computational and quantum-secure nature, and are thus well-suited in low power IoT devices. On the other hand, hash-based schemes although they provide greater security guarantees, have high execution time, memory and energy overheads which reduces their practice in limited node networks. The results indicate that there is a need to implement deployment strategies that are sensitive to the context of deployment taking into consideration device capabilities and application demands as well as network conditions so as to optimize security without necessarily jeopardizing operational performance. Hybrid techniques, such as using lightweight lattice-based algorithms to run regular operations, and more resilient schemes to run high-security operations, were found to be an effective approach to achieve both security and performance, especially with hardware acceleration techniques and offloading techniques. Network-level measurements also stressed that the implementation of PQC in lightweight IoT protocols may raise the latency and decrease the throughput, which makes the integration of protocols and optimization of the system essential to maintain their overall performance.

On the basis of these findings, a number of recommendations can be reached by researchers, practitioners, and policy makers. First, the algorithm to be used must be chosen based on an overall analysis of the limitations of the device, the operational needs, as well as the security priorities, and that the selected PQC scheme must be suitable to the particular context of implementation. Second, hybrid cryptographic frameworks are needed to exploit the synergistic capabilities of several families of PQCs, to trade efficiency and security of heterogeneous IoT networks. Third, edge-offloading and hardware acceleration should be applied wherever possible in order to offset the costs of computation and energy, especially in the case of microcontroller-based devices. Fourth, session resumption, selective encryption and payload compression are also necessary to optimize protocols to reduce latency and throughput effects when introducing PQC into lightweight communication protocols. Lastly, ongoing research and development must be devoted to the mitigation of side-channel vulnerabilities, standardization of PQC implementation, and setting of benchmarks of the performance assessment on a variety of devices and network environments. Based on using these recommendations, practitioners can implement PQC in the way that will guarantee quantum-resilient security without compromising operational efficiency, which will eventually provide scalable, resilient, and future-proof edge-IoT ecosystems.

References

1. Alomari, A. (2025). Complexity of post-quantum cryptography in embedded systems and optimization strategies. *arXiv*. <https://arxiv.org/abs/2504.13537>

2. Almutairi, M. (2025). Resilience of post quantum cryptography in lightweight IoT protocols: A systematic review. *Engineering*, 6(12), 346. <https://doi.org/10.3390/eng6120346>
3. Amiriara, H., Mirmohseni, M., & Tafazolli, R. (2025). PLS assisted offloading for edge computing enabled post quantum security in resource constrained devices. *arXiv*. <https://arxiv.org/abs/2504.09437>
4. Awasthi, S. (2025). Adaptive PQC integration for lightweight IoT protocols. *Engineering Journal*, 4(1), 101–115.
5. Bennett, S. (2025). Post quantum cryptographic algorithm performance on IoT devices. *International Journal of Advanced Research in Computer Science and Engineering*, 1(2), 21–26. <https://ijarcse.org/index.php/ijarcse/article/view/58>
6. Chhetri, G., et al. (2025). Post quantum cryptography and quantum safe security. *arXiv*.
7. Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). Performance analysis and industry deployment of post quantum cryptography algorithms. *arXiv*. <https://arxiv.org/abs/2503.12952>
8. Khan, M. A., Noor, R., & Javaid, N. (2025). Implementation and performance of post quantum cryptography for resource constrained consumer electronics. *Discover Internet of Things*. <https://link.springer.com/article/10.1007/s43926-025-00238-x>
9. Karthik, R. (2025). Context-aware adaptation for post-quantum cryptography in resource-constrained IoT devices. *Computer Networks*, 221, 109495.
10. Liu, J., Ramachandran, A., & Jurdak, R. (2024). Post-quantum cryptography for IoT: Performance evaluation and challenges. *IEEE Internet of Things Journal*, 11(6), 5234–5248.
11. Mahdi, L. H., & Abdullah, A. A. (2025). Fortifying future IoT security: A comprehensive review on lightweight post quantum cryptography. *Engineering, Technology & Applied Science Research*, 15(2), 21812–21821. <https://doi.org/10.48084/etasr.10141>
12. Mahdi, L. H., & Abdullah, A. A. (2025). Lightweight post quantum cryptography for IoT. *Engineering, Technology & Applied Science Research*.
13. Mansoor, W. (2025). Lifecycle management and security of post-quantum IoT networks. *Journal of Information Security*, 16(2), 102–114.
14. Rawal, D., Seedorf, J., & Jha, N. (2025). Performing classical and post quantum cryptography on IoT data: An evaluation. *ISPRS Archives*.
15. Schöffel, T., Feldmann, M., & Wehn, N. (2025). Hardware acceleration of post-quantum cryptography for edge computing. *arXiv*.
16. Sedghighadikolaei, F., et al. (2025). Hash-based PQC signatures for constrained devices: Performance evaluation. *IoT Security Journal*, 3(4), 56–68.
17. Siddharth. (2025). Post quantum cryptographic algorithm performance on IoT devices. *IJARCSE*.
18. Akyildiz, I. F., Kak, A., & Nie, S. (2024). Edge-IoT: Architectures, challenges, and post-quantum security implications. *IEEE Communications Surveys & Tutorials*, 26(3), 2104–2125.
19. Alomari, A. (2025). [Also cited for side-channel attack discussion].
20. Mahdi, L. H., & Abdullah, A. A. (2025). [Also cited for lightweight PQC review].