JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 01, 2026

End-to-End Integration and Performance Evaluation of Post-Quantum Cryptography in Secure Computing Systems

Ali Abbas Hussain[1*], Abdul Karim Sajid Ali[2]

[1*]Master of Information Technology & Management, University of Texas at Dallas USA.
Email: aliabbas.graduateschool@gmail.com

[2] Master of Information Technology and Management, Illinois Institute of Technology, Chicago, USA.
Email: aali62@hawk.iit.edu

ABSTRACT

Due to the pace of the revolution in the domain of quantum computing, classical cryptography systems have become at risk, which has prompted the creation and implementation of post-quantum cryptography (PQC). This review will give an analysis of end-to-end integration and performance measurement of PQC in secure computing systems. It looks at the development and categorization of PQC-based schemes, such as lattice-based, code-based, and hash-based schemes, and their mathematical underpinnings. The paper also examines the hurdles of interoperability with PQC with existing architectures (including overheads in computation), key size (including very large sizes), and compatibility (with existing protocols). One of the main areas is performance assessment, and such aspects as execution time or memory consumption, energy efficiency, and scalability in various settings such as the IoT, the embedded system, or cloud platforms are of importance. The comparison of major algorithms of PQC reveals security/efficiency trade-offs, showing that the appropriateness of algorithms is extremely dependent on the application. New solutions, like hybrid cryptographic models and hardware optimization methods, are also discussed in the review to overcome the deployment barriers. Comprehensively, this research has shown the need to develop more research, standardization of standards, and optimization activities to make sure PQC is practically used. The results help to better comprehend how quantum-resistant cryptographic schemes could be successfully implemented into the current secure computing infrastructure.

Keywords: Post-Quantum Cryptography, Quantum Computing, Lattice-Based Cryptography, Performance Evaluation, Secure Computing Systems, Cryptographic Integration

1. Introduction

The advent of quantum computing threatens the basic implementation of classical cryptography that forms the backbone of both common and secure computing infrastructures. In traditional public-key cryptographic schemes, including RSA and elliptic curve cryptography, computational hardness assumptions, such as integer factorization and discrete logarithms, which in theory can be solved effectively by large-scale quantum computers using algorithms such as the Shor algorithm. This projected weakness has spurred intense research activities on post-quantum cryptography (PQC), an approach to creating cryptographic primitives that are immune to quantum foes and retain their functionality to be used in the real world (Bernstein and Lange, 2017).

Property formalization and standardisation were first initiated by organizations like the National Institute of Standards and Technology (NIST), which started a multi-round process of standardisation to assess and choose quantum-resistant algorithms. Initial requirement documents defined the requirements and security assumptions as well as candidate schemes that should be used in post-quantum settings (Chen et al., 2016). Follow-up assessments like the second-round status report offered an in-depth assessment of algorithmic performance, security, and algorithm implementation trade-offs, with a variety of methods that included lattice-based, code-based, and multivariate cryptography (Moody et al., 2020). This is complemented by rules on how to migrate cryptographic systems to ones that are resistant to quantum, with an urgency placed on migration plans (Barker and Roginsky, 2019).

Lattice-based cryptography has been one of the most prominent candidates for the different PQCs, as it offers great security assurances and feasible efficiency. The theoretical basis of most lattice-based constructions is the Learning With Errors (LWE) problem, suggested by Regev (2009), which has since been extensively used in the key encapsulation schemes FrodoKEM (Bos et al., 2016). The design space of PQC is even larger since there are other design choices that may be implemented with the intention of providing alternative security assumptions and performance attributes, such as rank-metric code-based encryption (Loidreau, 2017). The developments are indicative of the abundance of cryptographic primitives that are under investigation to be quantum-resistant.

The expedient implementation of quantum computing has heightened the necessity of the implementation of PQC. Quantum hardware capabilities can be rapidly advanced, exhibited by experimental demonstrations, including quantum supremacy due to superconducting processors (Arute et al., 2019). Whilst the large-scale, fault-tolerant quantum computers are not commonly available, these achievements highlight the importance of taking measures to successfully incorporate PQC into existing systems. This change is especially essential to the long-term data security, where encrypted data is to be kept secret for decades.

A few challenges are associated with integrating PQC into secure computing systems, such as performance, scalability, and compatibility with existing protocols. As an example, the PQC algorithms can usually have a large computing overhead or key size relative to their classical counterparts, which may affect system performance and resource consumption. Recent literature has assessed the implementation of PQC into a practical environment, such as consumer electronics and network security protocols, which has shown a trade-off between security and performance (Commey et al., 2025; Bae et al., 2022). Comparisons of the most well-known algorithms like Kyber, SNTRUP761, and FrodoKEM further point out differences in latency, throughput, as well as the usage of resources (Ünsal, 2025).

Besides performance factors, the integration of PQC should concentrate on the rising dangers in current computing setups, such as side-channel attacks and exploits in a form of malware. Attack methods have also been advanced using machine learning, especially in the side-channel analysis, which requires a strong defense against such attacks in PQC applications (Picek et al., 2017). Equally, the innovative nature of cybersecurity security risks, with advanced malware prevalence issues, demonstrates the necessity of effective and secure cryptography solutions (Ceschin et al., 2018). Efficient zero-knowledge constructions, as well as other protocol-level approaches towards the provision of such services as secure data composition, are also crucial towards system robustness when utilizing PQC-based services (Ciampi et al., 2016).

The thorough knowledge of cryptographic principles is still crucial in analyzing and implementing PQC solutions. Root texts give us the conceptual background to evaluate the security properties and implementation trade-offs in both classical and post-quantum environments (Smart, 2016). Due to the persistent development of the area, end-to-end integration and performance assessment of PQC in the area of secure computing systems have become the key topics of research. These would help in reducing the difference between the theoretical design of cryptographic construction and its real-life application, such that future- generation security infrastructure is tough against any classical and quantum attackers.

2. The Aim of the Review

This review aims to survey the end-to-end implementation of post-quantum cryptographic algorithms in secure computing systems, their performance, scalability, and thrusts towards practical deployment. It focuses on comparing various PQC schemes, their efficiency in practice, and some of the major limitations and optimization strategies to help facilitate a secure switch between classical and quantum-resistant cryptographic infrastructures.

3. History and development of post-quantum cryptography

The fast development of quantum computing practically changed the security premises of classical cryptography. Public-key encryption algorithms like RSA and elliptic curve cryptography are based on computational hardness problems that are vulnerable to quantum algorithms. This has led to the post-quantum cryptography (PQC) emerging as a research topic with a priority in creating quantum adversary resistant cryptographic primitives. Theoretical works were the foundation of the initial studies that constructed alternative hard constructions such as lattice, hash, and code constructions (Fathalla and Azab, 2024; Borges et al., 2020). The change in the theory and the practice requirements have all contributed to the development of PQC. The first part of work has been based on identifying mathematically safe problems, and the second stage of work is effective algorithms to be incorporated into real-life systems. One such is lattice-based cryptography that became one of the leading ones by offering high security guarantees and being applicable in realizing a diverse number of cryptographic operations. At the same time, hash-based signature schemes came back as trusted quantum-resistant solutions since they are minimally dependent on complicated mathematical premises (Fathalla & Azab, 2024). This work and co-workers led to a more diversified ecosystem of PQC algorithms.

The research then took a different turn towards which behavior to study performance and viability of PQC in real contexts became the focus of the research. Comparative research supported by the findings of key agreement mechanisms, identified security versus computational performance trade-offs, especially in the case of constrained systems (Borges et al., 2020). The consumption of power also became a critical problem and, specifically, battery-operated and embedded devices, where PQC algorithms often are more prriced in areas of computational complexity than classical algorithms (Roma et al., 2021). These results highlighted the importance of using optimization strategies to enhance security and efficiency. The development of application requirements further spurred development of PQC. Lightweight but secure cryptographic solutions are required in modern computing communities, such as Internet of Things (IoT), blockchain and cyber-physical systems. Research has revealed that it is preferable to set up PQC implementations to these regions, which is constrained in resources and require real-time processing, making it challenging (Paul et al., 2022; Wang and Ismail, 2025). To exemplify, IoT systems are sensitive to the key size and low-latency processing but blockchain application is sensitive to transaction scalability and throughput.

The latest study has also delved into the integration of PQC into the newer technologies, where some have reported its importance in ensuring the new generation infrastructures. PQC is under investigation in blockchain systems to resolve the risk of quantum attacks on the digital signatures and consensus (Revathi and Suganthi 2025). Similarly, PQC is being incorporated in smarter transportation systems and in other significant scope distributed settings to offer data

safety in the long run and system endurance (Al Mamun et al., 2026). The developments above illustrate the way PQC is stretching itself to other applications besides the traditional cryptography applications. In general, the history of post-quantum cryptography can be viewed as a shift towards a more practical approach, rather than opportunities to explore theory. Studies along this line are already being developed in the areas of interdisciplinary research into cryptographic theory, system design and optimization of systems. With advances in quantum computing, the relevance of PQC is only going to increase and there would be a need to thoroughly review and overlay strategies to ensure the safety of computing systems in the quantum era.

4. NIST Standards Process and Prospective Algorithms

Immediate realization Massification of post-quantum cryptography algorithms is a significant step towards their broad compromise in the safe computers. National Institute of Standards and Technology (NIST) has been leading in this effort through a multi-rounded measurement procedure that will help to choose those algorithms that fulfill high standard of safety and performance. Significant analysis of candidate schemes, the opposition of famous attacks, and their performance in computational costs, suitability to different application conditions are discussed (Montenegro et al., 2025). The applicability to the real world is one of the most important factors of the NIST standardization initiative. Candidate algorithms are not just judged based on their theoretical security bases, but also based on their performance based on real life implementations. This has benchmarking on different platforms, which are embedded systems, cloud computing setups, and heterogeneous computing setups. It has been proven that the performance can change considerably based on the underlying hardware and system setup, thus the significant role of in-depth assessment frameworks (Abbasi et al., 2025; Dong and Wang, 2024).

The process of standardization also assisted in the development of the best implementations with exclusive applications. In a case in point, research on post-quantum Transport Layer Security (TLS) protocol has provided insight into the manner in which PQC algorithms can be incorporated in the current communication infrastructure. According to these studies, PQC changes the handshake latency and bandwidth as well as the overall network performance, which is vital in bringing into deployment in a real-world system (Montenegro et al., 2025; Tasopoulos et al., 2022). This kind of assessment will be fundamental in compatibility with the existing security measures. Standardization is also largely influenced by industry adoption, besides performance issues. The appropriateness of the PQC algorithms to be applied during a commercial environment has been the focus of recent research, and in this case, issues with scalability, interoperability, and system integration are the challenges (Demir et al., 2025). These articles highlight the significance of academia-industry-standardization collaboration to provide a successful quantum-resistant cryptography initiative beyond the classical one.

This is also made complicated by the fact that the candidate algorithms have diverse types in terms of diversity. PQC schemes are based on a diverse array of mathematical underpinnings, including lattices, codes and multivariate polynomials, each with its brilliant and weak points. Such disparities have been observed based on the review of the benchmarking works observed in heterogeneous environments and significantly influences how the two aspects,

security and efficiency, trade-offs and how both aspects can be implemented (Abbasi et al., 2025). Diversity also enables the realization of application requirements in terms of using standardized algorithms to suit a diversity of purposes. Also PQC absorption on dedicated domains, such as virtualised environments and cloud systems, has been explored to understand how PQC impacts the performance and security of the system. Studies show that virtualization brings about some additional overhead, which should be taken into account when implementing PQC algorithms in those settings (Kasbi et al., 2025). Conflicts in these results point to the necessity of dealing with context-specific assessment in the process of standardization.

The NIST program has helped a lot towards post-quantum cryptography application because it has provided a rational framework of analysis and selection of reliable and cost-effective algorithms. It is centered in the rigor of the theory and functionality to the real world which ensures that the standards developed can be highly applicable to real world. As the process progresses, continual research and benchmarking will be instrumental in improving these algorithms and assist in making them a part of secure computing systems.

5. Classification of Post-Quantum Cryptographic Scheme

The cryptography that is post-quantum includes a wide variety of cryptographic schemes using various mathematical hardness assumptions. Such schemes are classified as lattice-based, code based, hash based, multivariate polymath-based and isogeny-based cryptography. Each of the two categories possesses distinctive strengths in the eyes of security, efficiency and complexity of implementation and requires classification in order to understand the application of both of the categories to safe computing systems. The problem forms the basis of lattice-based algorithms, such as Learning With Errors (LWE), which are popular in that they have solid security proofs and are versatile (Demir et al., 2025).

One of the oldest strategies of PQC is code-based cryptography, and the security is based on the infeasibility of decoding random linear codes. The distinguishing trait of these techniques is that they are resistant to classical and

quantum attacks on a lengthy scale but are likely to be key size intensive, thus they are not very practical under constrained conditions. Comparative studies have also shown that despite code-based schemes being extremely secure, performance trade-offs need to be well constrained with their usage into life systems (Borges et al., 2020).

Another significant type of cryptography is hash-based cryptography, which is mainly utilized with digital signatures. These protocols are based on quantum numbers of cryptography hash functions and not on intricate algebraic designs and, therefore, are comparatively easy and resistant to quantum assaults. They too, may, however, possess big signature sizes and state management issues, particularly stateful versions. Recent reviews also found them to be reliable and can be debated as appropriate to be employed in long-term security applications (Fathalla & Azab, 2024).

Multivariate cryptography relies on the mathematical challenge of solving systems of multivariate polynomials in finite

fields, computationally infeasible to students when using classical and all quantum adversarial tools as well. Such designs do not necessarily generate signatures slowly, and verify them quickly, but are linked to some key size problems and structural vulnerability. Their performance attributes can be utilized in some applications that put a lot of emphasis on speed (Wang and Ismail, 2025).

They are accompanied by the hybrid and application-specific PQC schemes which are gaining popularity. Hybrid methods incorporate both classical algorithms and post-quantum algorithms in an attempt to be backward compatible and not a radical transition. They are particularly effective in the case of such systems as enterprise and large-scale systems, which cannot immediately switch to PQC (Aydeger et al., 2024). In addition, hybrid cryptosystems are also used to perform multi-cryptographic paradigms so as to enhance the security exploitation of the joint strengths (Garms et al., 2024). New categories are also suggested, with the deployment environments in mind, and these include the IoT, cloud computing, and cyber-physical systems. As an example, the lightweight designs of PQC are customized to devices with the resources that are scarce resources, and data centers and high-throughput applications can be performed with high-performance PQC designs (Liu et al., 2024). These types of classification, which are based on the environment, assist in choosing the right algorithm with respect to the requirements and constraints of the system. Table 1 shows that different PQC schemes are classified by the mathematical problem on which they are based, and can be traded off between security and efficiency.

Table 1: Classification of Post-Quantum Cryptographic Schemes

Scheme Type	Underlying Hard Problem	Key Size	Advantages	Limitations
Lattice-based	LWE, SVP	Medium	Strong security, versatile, efficient	Moderate computation overhead
Code-based	Syndrome decoding problem	Very large	Proven long-term security	Large key sizes
Hash-based	Hash preimage/collision resistance	Small–medium	Simple, highly secure	Large signatures, state management issues
Multivariate	Polynomial equation solving	Large	Fast computation	Structural vulnerabilities
Isogeny-based	Elliptic curve isogeny problems	Small	Compact keys	Emerging security concerns

In summary, the PQC scheme classification gives a systematic system on which to gauge the applicability of the schemes in various permutations. It demonstrates the trade-offs among security and performance and the complexity of implementation to ensure that informed decisions are made as far as the implementation of PQC is concerned as part of secure computing systems. More room is available to this classification landscape in terms of new hybrid schemes and

optimized schemes, which will probably be created as more research is conducted.

6. Basics of Lattice-Based Cryptography and LWE

One of the most promising blocks of post-quantum cryptography is the lattice-based cryptography due to the high

theoretical foundation and the effectiveness in practice. Their security is primarily dependent on the hardness of lattice problems, such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE) problem. The problems are discussed to resist classical as well as quantum attacks and can even be extended to the next-generation cryptography (Demir et al., 2025). In lattice-based cryptography, the LWE issue is in the middle ground of the new field. It is solving noisy linear equations, which is computationally infeasible when there are large parameters. The following are the properties that can be generated using this property: secure cryptographic primitives, e.g., encryption, digital signature schemes, and key exchange protocols. Kyber and FrodoKEM are lattice-based schemes, which have extensively been proposed, implemented, and analyzed in terms of their performance and security-related properties in a range of settings (Abbasi et al., 2025).

Lattice-based cryptography is not restricted to a specific type, and this is one of the merits of this approach. The lattice constructions, in contrast to a few other methods of PQC, are usable in a large variety of functions, such as homomorphic encryption and secure disaggregate computation. They are particularly attractive in systems whose cryptographic requirements are advanced, such as cloud computing and data analysis with privacy concerns (Wang and Ismail, 2025). They have also been adopted in the standardisation activities because of relatively efficient implementation as compared to other PQC schemes. Regardless of these advantages, lattice-based cryptography still has certain limitations, in particular, when it comes to the processing load and resource utilization. They have also discovered research on embedded systems and resource-constrained systems demonstrates that the application of lattice-based algorithms can result in the realization of higher latency and energy consumption, which could restrict their usability in some situations (Dong and Wang, 2024). Real world execution can be optimized, e.g., by using hardware acceleration and improved algorithms.

The other consideration in lattice based cryptography is that it is energy efficient. It has also been found by research that even though these schemes are very secure, it can be extremely more local power consuming, in comparison with the classical cryptographic methods. This statement is related to the IoT and mobile devices, particularly in the sphere where energy-related problems turned into a big concern (Roma et al., 2021). Security and performance are tradeoffs, which must be compromised to handle such issues, which are usually a combination of parameter tuning and system level optimization. Recent advances have been spiced with the improvement of the performance of lattice-based schemes into practice. Optimization feasibility studies prove that it is possible to undertake it with the help of a pool of parallel processors and specific hardware (Abbasi et al., 2025). In addition, studies are also being carried out regarding hybrid solution with lattice-based cryptography with other PQC systems to enhance the performance as well as the security of the complete system.

7. Alternative and Code-Based PQC

Code-based cryptography is one of the oldest and most developed techniques of post-quantum cryptography. It can resist the attacks using the mathematical complexity of decoding random linear codes, which has long been deemed impossible in both classical and quantum attacks. This security guarantee, over time, makes code-based schemes an attractive scheme to high reliability applications. However, a significant drawback of such schemes is that their public key sizes are huge and might be a hindrance to their application in a storage-constrained and bandwidth-restricted environment (Borges et al., 2020).

In addition to code-based systems, some other alternative PQC methods have been created in order to overcome particular performance and deployment issues. Cryptographic schemes based on hash, such as are well known, are simple and offer high security assurances. These protocols can be based just on the preimage resistance and collision resistance of hash functions, rendering them very resistant to quantum adversaries. Even though they have the benefits that they can be stateful and have large signature sizes, hash-based signatures do have drawbacks, including that they can require stateful management because the stateful versions only work with stateful versions(Fathalla and Azab, 2024). The other important category is multivariate cryptography that is based on the determination of solutions to nonlinear systems of equations in a finite field. These schemes normally provide rapid calculation of signature generation and verification, and thus are applicable in high-speed applications. They, however, might also possess some issues related to the structure vulnerability and key size which ought to be taken into account entirely in implementation (Wang and Ismail, 2025). This permits their use in specialist applications where speed of the process being calculated is more significant than other factors in the computer industry.

Isogenous cryptography Systems A cryptography system called isogenous cryptography is less advanced than other PQC systems, but possesses small key sizes. The calculations are made on the complexity of searching for isogenies between elliptic curves and form the basis of the plans. Though it is theoretically good, recent cryptanalysis findings uncovered certain frailties in certain of the constructions based on the isogeny, and it remains uncertain whether it is practical over the long term. This means that research on this area is being made, with a focus on making it more secure and more productive (Demir et al., 2025). One of the alternatives that are being investigated as a workable method of transcending the classical systems to post-quantum systems is hybrid cryptography. These methods apply a hybrid of traditional cryptographic algorithms which are founded on PQC in order to provide redundant security. The hybrid protection against quantum threats (hybrid systems) and backward compatibility of the hybrid systems in especially large and prompt systems and in legacy systems are particularly useful (Garms et al., 2024). Also, hybrid encryptions have been suggested to maximize the performance by sharing cryptographic operations among a variety of different schemes (Majumder et al., 2026). In Figure 1, PQC algorithms are examined using performance evaluation framework that correlates with benchmarking, measuring metrics, and comparing the solution with other alternatives to achieve the best solutions.

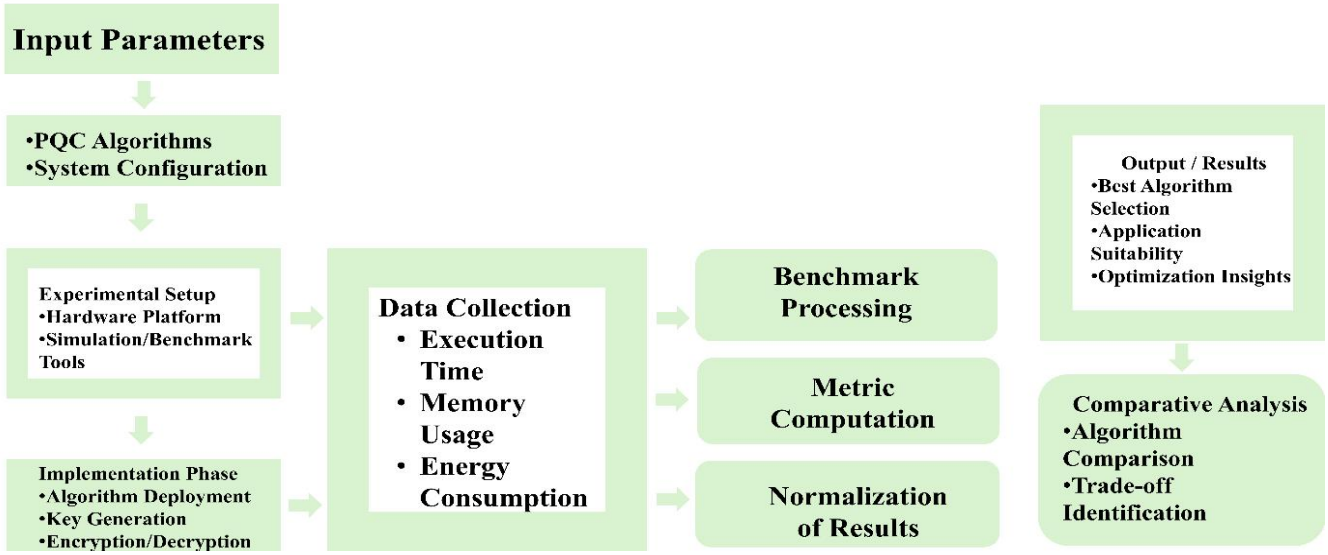

Figure 1: Performance Evaluation Metrics for PQC Systems

Adapted application-specifically, PQC is increasing in significance. An example is PQC which is re-engineered to emerge as an identity management system in order to offer long term authentication security (Aramide, 2022). In the same manner, CP systems need specialized cryptographic solutions that do not jeopardize security but meet the real-time operating limits (Paul et al., 2022). The realizations of this application specific form highlights the significance of flexible and customizable PQC designs. Overall, the set of solutions to quantum-resistant security on code-based and alternative PQC approaches offers a wide range of solutions. These two techniques trade-off in different ways, with their key size, computational performance, and implementation complexity. The current enhancement of hybrid and application-specific solutions will likely play a major part in making the usage of PQC in extensive variety of computing settings popular.

8. Integrity with the Security Computing Architecture

The implantation of post-quantum cryptography in secure computing architectures is a highly important step towards ensuring that it can resist quantum attacks. This is achieved through the integration of PQC algorithms into the existing systems, protocols, and infrastructures and normalizing them to be compatible, efficient, and secure. One of the key challenges in this integration is, in general, reconfiguring existing architectures built to deliver cryptographic primitives and tailored to apply classical cryptography, to address the increased computational and storage requirements of PQC algorithms (Demir et al., 2025). One of the earliest applications of PQC would be to secure

communication protocols, including Transport Layer Security (TLS). Post-quantum TLS can be implemented, both in terms of latency and bandwidth costs; it has been proven that it can be a part of handshake mechanisms. They have also built up performance evaluation designs that have enabled the ideal assessment of these influences and maximized protocol setups (Montenegro et al., 2025). These findings are required to attain seamless internet-level applications. Further complications with IoT devices and embedded systems relate to the lack of guarantee of robust computation and energy efficiency. Experiments have been conducted to assess the performance of PQC on embedded systems, wherein it was found that the choice of algorithms and optimization are crucial in reaching an acceptable level of performance (Dong and Wang, 2024). Hardware acceleration techniques are required in most of these deployments to facilitate the effective use of PQC. In addition, IoT-related literature states that it is necessary to strike a balance between security and the power use and latency needs (Hanna et al., 2025). PQC should also be integrated with cloud and virtualized platforms. Virtual machines add extra overhead, which may influence the performance of cryptographic algorithms. Studies have shown that these challenges can be partly reduced by optimizing the resources and utilizing parallel processing (Kasbi et al., 2025). Such measures are essential to maintain performance in large-scale distributed systems.

The blockchain technology is another field of PQC integration application. A digital signature is the cryptographic primitive that is particularly important to blockchain systems' security. PQC will be forced to be embedded in blockchain to protect against quantum attacks to transaction authentication and consensus system. Research on hybrid solutions has been done between classical signatures and post-quantum signatures in which both are secure and compatible (Castiglione et al., 2024). In addition to the technical issues, there are organizational and strategic factors that add to the integration of PQC. The migration schedules, system interoperability, and risk management must be put into consideration in the transition strategies. Studies note the significance of the gradual introduction and hybrid cryptography appliances to help in a gradual migration of the classical to post-quantum systems (Aydeger et al., 2024). Institutional approaches further highlight the need for policy frameworks and standardization efforts to support widespread adoption (El Bizri et al., 2026). PQC integration is concerned with multiple layers as illustrated in Figure 2, i.e., application, protocol, cryptographic, and hardware, which can engage to ensure secure communication.

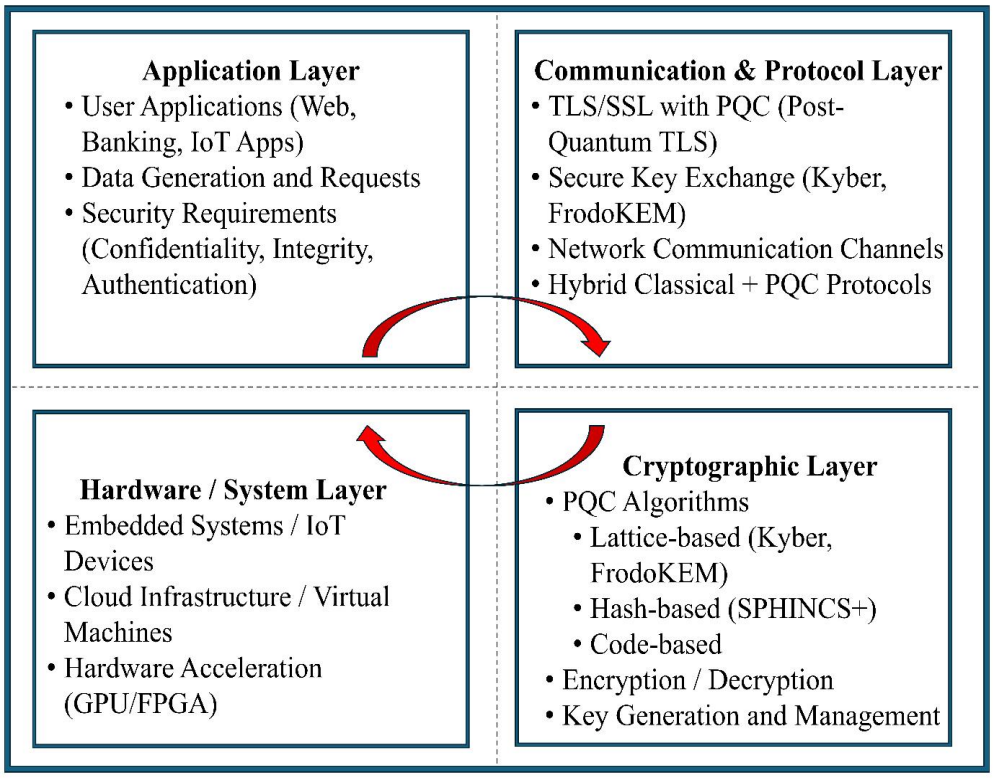

Figure 2: Integration of PQC in Secure Computing Architectures

PQC is also being integrated with emerging applications like the intelligent transportation system and AI-enabled IoT networks to improve security. The systems require formidable cryptographic operators capable of facilitating the use of huge volumes of data and live activities. PQC implementation in such environments would not only improve the functionality of broadbanding but also ensure security in the long-term (Al Mamun et al., 2026; Saeed and Alqahtani, 2026). Overall, introducing PQC into secure computing systems is a multifaceted effort, which includes technical, operational, and strategic components. It requires a list of optimized algorithms, system-level optimization, and transition plans to be able to implement it successfully. These coordinating efforts will play a significant role as the research moves towards building quantum-resistant security infrastructure.

9. Measures of PQC Systems Assessment

The post-quantum cryptographic systems must be tested on a set of performance measures to assess their feasibility to be applied in the real world. Unlike the classical cryptographic schemes, PQC schemes are generally more computationally complex, have larger key sizes, and incur higher communication overheads. Consequently, performance appraisal is very important in establishing their applicability in various computing conditions. Execution time, memory usage, bandwidth use, energy use, and scalability are the most common metrics, all being helpful in understanding how the system would be oriented under various circumstances (Abbasi et al., 2025).

One of the most popular measures to measure PQC algorithms is execution time. It is the time required to run cryptographic key generation, encryption, and decryption, signing, and verification functions. Studies have pointed to PQC algorithms typically being latency-limited as compared to their classical counterparts, particularly under resource-constrained environments. As an illustration example, embedded system performance studies reveal that the cryptography operations consume huge amounts of time; thus, they should be optimized (Dong & Wang, 2024). These are necessary in applications that require real-time applications. The other consideration is the use of memory, especially to gadgets that have minimal storage capacity. Core-based and lattice-based algorithms (PQC schemes in particular) can demand bigger key size, and larger intermediate data structures. This increased memory demand can impose some restrictions on the system performance and limit its application in limited systems such as IoT devices. The performance measurements of PQC deployments to embedded systems have shown that the achievement of feasible throughput requires effective memory management (Tasopoulos et al., 2022).

Ciphertext and key sizes are closely related to bandwidth usage. The bigger the cryptographic parameters, the higher the requirements in the way data is transmitted which can have an impact on network performances. This is particularly true when a communication protocol such as TLS is being used, and the size of the handshake messages can easily grow significantly in the event that PQC algorithms are used. Performance assessment models of TLS based on the post-quantum performance have been useful in determining the impact of these factors on the network latency and throughput (Montenegro et al., 2025).

Power saving is a major value, especially in devices powered by batteries as well as in large-scale distributed systems. PQC algorithms may use many more computational resources, resulting in an increase in energy consumption. Energy efficiency surveys have shown that, when comparing parameters of the algorithm to the acceleration of hardware, it is possible to attain a significant reduction in power consumption (Roma et al., 2021). Measures like these have to be taken when implementing the IoT and mobile environment sustainably. The other metric that is important is the scalability, especially when the systems are being used on a high volume of data or at a high rate of transactions. The PQC algorithm has to be able to achieve good performance as the size of the system and the workload grow. Research on heterogeneous computing scenes depicts that the currently utilized parallel computing and distributed computer architecture may enhance the significance of scalability, enabling computationally-intensive cryptographic functions to be effectively handled (Abbasi et al., 2025). Table 2 shows that such performance parameters as the execution time, memory usage, and energy efficiency play a critical role in deciding whether or not PQC systems are viable in practice.

Table 2: Performance Evaluation Metrics for PQC Systems

Metric	Definition	Impact on System	Measurement Method	Application Relevance
Execution Time	Time for cryptographic operations	Affects latency	Benchmark testing	Real-time systems
Memory Usage	Storage required for keys and operations	Limits deployment	Memory profiling	Embedded/IoT systems
Energy Efficiency	Power consumption during execution	Impacts battery life	Power analysis tools	Mobile and IoT devices
Bandwidth	Data transmitted during communication	Affects network performance	Network simulation	TLS, cloud systems
Scalability	Ability to handle increased workload	Determines system expansion	Stress testing	Large-scale distributed systems

In gauging such metrics across platforms, benchmarking studies are critical. Comparative studies of PQC algorithms enable both researchers and practitioners to make the correct decision concerning the schemes, bearing in mind the potential flaws and advantages of the algorithms. These benchmarks usually take into consideration several measurements at the same time, providing a comprehensive picture of the performance of algorithms (Demir et al., 2025). In summary, metrics of performance evaluation play a very important role in determining the feasibility of post-quantum cryptography. By analyzing the different factors, such as the execution time, memory usage, bandwidth usage, power use, and scaling, researchers can discover the optimal solutions to secure a computing environment. These tests give a chance to make a wise decision and to create an effective and scaled application of PQC.

10. Comparison of the best PQC Algorithms

It is important to compare the most recent algorithms of post-quantum cryptography to understand their relative merits and demerits, and their use in different areas of application. The security assumptions, computational efficiency, and implementation complexity of PQC schemes differ drastically. Consequently, there is a need to undertake systematic comparisons to help select the right algorithms to use in secure computing systems. The benchmarking studies could give useful information about these differences due to their performance assessment in a variety of environments (Abbasi et al., 2025). Lattice-based schemes are some of the most popular PQC schemes, imaginatively known as Kyber and FrodoKEM. The algorithms are highly tested in terms of security and have comparatively good performance, and hence make them ideal contenders in any standardization exercise. However, different parameter sets and design methodologies exhibit different trade-offs between the level of security, the size of the key, and computational overhead. Comparative research has seen that Kyber is faster in performance, and that FrodoKEM is less costly, when considering security assumptions (Demir et al., 2025).

Code algorithms, however, being very secure, are usually large in size, and thus may not be practical. This notwithstanding, they remain a secure enough alternative in the applications which factor is security. Performance comparisons show that code-based schemes can be better than other PQC algorithms in particular situations, especially when compiled using hardware-specific optimizations (Borges et al., 2020). These results accentuate the role of context-specific evaluation. The power and the simplicity of the hash-based signature schemes are familiar. They provide a lot of security; however, some operations are costly to compute and have a large signature. Comparative analysis has shown hash-based algorithms to be particularly effective when long-term security is required, such as in digital data archives and updates to firmware (Fathalla and Azab, 2024). They provide a secure choice because of the predictability of their security properties.

Multivariate and hybrid schemes of cryptography are more controlled both in terms of performance and security. Multivariate schemes are generally quick to compute, but may have key size and structural security problems. Hybrid applications based on classical and post-quantum algorithms can be used to create best-of-both-worlds solutions, a gradual transition, and enhanced security. It has also been established that hybrid systems have the ability to deliver better performance after capitalizing on the capabilities of more than one cryptographic paradigm (Garms et al., 2024; Majumder et al., 2026). Application-specific comparisons are yet another way that depicts the heterogeneity of the performance of PQC. Embedded systems and IoT adapt lightweight algorithms due to the limitations of resources

available; high-performance schemes are more adept on college and data center systems. The analysis of IoT devices has shown that the effectiveness of the system (i.e., latency and consumption) can largely depend on the algorithms used (Hanna et al., 2025). Similarly, blockchain applications require such algorithms to be able to balance the security, scalability, and transaction throughput (Campbell, 2025). As Table 3 shows, the third-best PQC algorithms differ in their key size, computing cost, and applicationability, so this would not imply a best solution.

Table 3: Comparative Analysis of Leading PQC Algorithms

Algorithm	Category	Key Size	Security Level	Computation Cost	Suitable Applications
Kyber	Lattice-based	Medium	High	Low–Moderate	General-purpose, TLS
FrodoKEM	Lattice-based	Large	Very High	High	High-security environments
SNTRUP761	Lattice-based	Medium	High	Low	Efficient communication systems
Classic McEliece	Code-based	Very large	Very High	Moderate	Long-term secure storage
SPHINCS+	Hash-based	Small keys	High	High	Digital signatures

A second big problem when making comparisons in PQC is the presence of signature schemes. The performance analysis of PQC signature algorithms portrays the differences in signing and verification time, and the sizes of signatures. Such differences are relevant to their use in applications, like authentication and managing digital identities (Opiłka et al., 2024; Raavi et al., 2021). Depending on the application under consideration, the signature scheme will be selected depending on its needs.

11. Limitations and Future Directions

There are a few limitations associated with post-quantum cryptography that have hindered its application in post-quantum cryptography in secure computing environments. PQC algorithms are more complex to compute, have larger key and data size, and consume more energy than classical cryptography schemes, and are not well adapted to resource-constrained systems (IoT and embedded systems, etc.). Neither does it have interoperability with legacy systems and existing protocols, which is likewise a significant challenge and requires complex integration and transition plans. Moreover, not all schemes have undergone much real-world testing yet, and could be susceptible to novel cryptanalytic attacks.

Future research must focus on ways of improving the PQC algorithms in their performance, scalability, and consumption of less energy without interfering with the high security level of the algorithms. Cryptographic solutions with lightweight and hybrid designs will be developed to enable easier transitions. Further standardization, practical benchmarking, and even hardware acceleration tools are needed to ensure feasible and secure deployment in various computing systems.

12. Conclusion

Post-quantum cryptography is a breakthrough move towards implementing and building secure computing systems. The increasing risk, presented by quantum computing, is why the classical cryptography algorithms would need to be substituted with the quantum-resistant ones that would help to guarantee the long-term security of the information. This review began by discussing the history of PQC, its classification, and mathematical foundation, in particular, lattice-based constructions, and it also discusses other constructions and how they can be applied in practice. The integration of PQC within safe structures points out that they have profound challenges in terms of performance, utilisation of resources, and compatibility with the existing system. Evaluation metrics of performance and comparative analysis prove that there is no algorithm that fits in all settings, and it is necessary to choose and deploy it depending on the setting. Alternative applications of IoT, blockchain, and distributed systems that are emerging in recent times also indicate the applicability of flexible and efficient PQC implementations. Despite the limitations, the field is ever-growing with recent studies, the standardization, and plans to optimize it. A more seamless transition can be expected by featuring improved system-level integration and hybrid solutions. Ensuring that post-quantum security mechanisms are robust, scalable, and efficient is also critical in safeguarding the future digital infrastructures against computational threats.

References

1. Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., Liu, Y.-K., Miller, C. A., Peralta, R. C., Perlner, R. A., Robinson, A. Y., Smith-Tone, D. C., & Alperin-Sheriff, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process (NIST IR 8309). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8309
2. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandão, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., … Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5
3. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461
4. Ceschin, F., Pinage, F., Castilho, M., Menotti, D., Oliveira, L. S., & Gregio, A. (2018). The need for speed: An analysis of Brazilian malware classifiers. IEEE Security & Privacy, 16(6), 31–41. https://doi.org/10.1109/MSEC.2018.2875369
5. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography (NIST IR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105
6. Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 56(6), 1–40. https://doi.org/10.1145/1568318.1568324
7. Picek, S., Heuser, A., Jovic, A., & Legay, A. (2017). Climbing down the hierarchy: Hierarchical classification
8. for machine learning side-channel attacks. In M. Joye & A. Nitaj (Eds.), Progress in Cryptology – AFRICACRYPT 2017 (pp. 61–78). Springer. https://doi.org/10.1007/978-3-319-57339-7_4
9. Ciampi, M., Persiano, G., Scafuro, A., Siniscalchi, L., & Visconti, I. (2016). Online/offline or composition of sigma protocols. In M. Fischlin & J.-S. Coron (Eds.), Advances in Cryptology – EUROCRYPT 2016 (pp. 63–92). Springer. https://doi.org/10.1007/978-3-662-49896-5_3
10. Smart, N. P. (2016). Cryptography made simple. Springer. https://doi.org/10.1007/978-3-319-21936-3
11. Bos, J., Costello, C., Ducas, L., Mironov, I., Naehrig, M., Nikolaenko, V., Raghunathan, A., & Stebila, D. (2016). Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 1006–1018). https://doi.org/10.1145/2976749.2978425
12. Loidreau, P. (2017). A new rank metric codes-based encryption scheme. In T. Lange & T. Takagi (Eds.), Post-Quantum Cryptography (pp. 3–17). Springer. https://doi.org/10.1007/978-3-319-59879-6_1
13. Barker, E., & Roginsky, A. (2019). Transitioning the use of cryptographic algorithms and key lengths (NIST SP 800-131Ar2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-131Ar2

14. Commey, D., Appiah, B., Klogo, G. S., Bagyl-Bac, W., Gadze, J. D., Alsenani, Y., & Crosby, G. V. (2025). Performance analysis and deployment considerations of post-quantum cryptography for consumer electronics. arXiv. https://doi.org/10.48550/arXiv.2505.02239
15. Ünsal, S. (2025). A comparative performance evaluation of Kyber, SNTRUP761, and FrodoKEM for post-quantum cryptography. arXiv. https://doi.org/10.48550/arXiv.2508.10023
16. Bae, S., Chang, Y., Park, H., Kim, M., & Shin, Y. (2022). A performance evaluation of IPsec with post-quantum cryptography. In International Conference on Information Security and Cryptology (pp. 249–266). Springer.
17. Montenegro, J. A., Rios, R., & Lopez-Cerezo, J. (2025). A performance evaluation framework for post-quantum TLS. Future Generation Computer Systems.
18. Demir, E. D., Bilgin, B., & Onbaşlı, M. C. (2025). Performance analysis and industry deployment of post-quantum cryptography algorithms. arXiv. https://doi.org/10.48550/arXiv.2503.12952
19. Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. Cryptography, 9(2), 32.
20.
21. Wang, Y., & Ismail, E. S. (2025). A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain and IoT. IEEE Access.
22. Hanna, Y., Bozhko, J., Tonyali, S., Harrilal-Parchment, R., Cebe, M., & Akkaya, K. (2025). A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices. Internet of Things, 33, 101650.
23. Dong, B., & Wang, Q. (2024). Evaluating post-quantum cryptography on embedded systems: A performance analysis. arXiv.
24. Tasopoulos, G., et al. (2022). Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems. In International Conference on Information Security Practice and Experience. Springer.
25. Borges, F., Reis, P. R., & Pereira, D. (2020). A comparison of security and its performance for key agreements in post-quantum cryptography. IEEE Access, 8, 142413–142422.
26. Castiglione, A., et al. (2024). Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. IEEE Transactions on Industrial Informatics, 21(2), 1674–1683.
27. Al Mamun, A., et al. (2026). Post-quantum cryptography for intelligent transportation systems: An implementation-focused review. Vehicular Communications.
28. Roma, C. A., Tai, C. E. A., & Hasan, M. A. (2021). Energy efficiency analysis of post-quantum cryptographic algorithms. IEEE Access, 9, 71295–71317.
29. El Bizri, M., et al. (2026). Institutional approaches to post-quantum cryptography. IEEE Access, 14, 3259–3283.
30. Revathi, K., & Suganthi, K. (2025). Enhancing blockchain security against quantum threats. Computers &
31. Electrical Engineering, 127, 110610.
32. Fathalla, E., & Azab, M. (2024). Hash-based PQC schemes review. IEEE Access, 12, 175969–175987.

33. Paul, S., et al. (2022). Post-quantum security for cyber-physical systems. Journal of Computer Security, 30(4), 623–653.
34. Raavi, M., et al. (2021). Performance analyses of PQ signature algorithms. In ACNS. Springer.
35. Aramide, O. O. (2022). PQC for identity management. Adhyayan Journal.
36. Campbell, R. (2025). Hybrid post-quantum signatures for blockchain. Journal of British Blockchain Association.
37. Micheal, L. (2025). Hybrid PQC and blockchain performance evaluation.
38. Aydeger, A., et al. (2024). Transition strategies to PQC. In IEEE NoF Conference.
39. Garms, L., et al. (2024). Hybrid quantum-safe cryptosystem integration. Advanced Quantum Technologies, 7(4).
40. Majumder, C., et al. (2026). Hybrid PQ encryption frameworks. Journal of International Accounting and Financial Management.
41. Reddy, A. (2025). Evaluating PQC in quantum supremacy era. Famous Journal of Computer Science.
42. Saeed, M. M., & Alqahtani, F. (2026). AI and PQC for IoT security. PeerJ Computer Science.
43. Opiłka, F., et al. (2024). PQC signature performance. Applied Sciences, 14(12), 4994.
44. Kasbi, H. A., et al. (2025). PQC in virtual machine systems. In IEEE ICAISD.
45. Liu, T., Ramachandran, G., & Jurdak, R. (2024). PQC for IoT: Performance survey. arXiv.