ISSN: 3066-1730

Research Article

Journal of Electrical and Computational Innovations

Securing Digital Communications: Quantum and Post-Quantum Cryptography

Kiransairam Muntha[1] and Adewale Ashogbon[2*]

[1]*Graduate Student at the Department of Computer and Information Sciences, Walker School of Business and Technology, Webster University, USA.*

[2]*Assistant Professor of Cybersecurity at the Department of Computer and Information Sciences, Walker School of Business and Technology, Webster University, USA*

[*]Corresponding Author
Adewale Ashogbon, Assistant Professor of Cybersecurity at the Department of Computer and Information Sciences, Walker School of Business and Technology, Webster University, USA.

Submitted: 2025, Aug 01; **Accepted:** 2025, Sep 02; **Published:** 2025, Sep 15

Citation: Muntha, K., Ashogbon, A. (2025). Securing Digital Communications: Quantum and Post-Quantum Cryptography. *J Electr Comput Innov, 2*(2), 01-10.

Abstract

As quantum computing advances toward practical use, classical cryptography is at a serious risk of being compromised, especially with the use of quantum algorithms like the Shor algorithm, which can break RSA in polynomial time, as well as Elliptic Curve Cryptography (ECC). This research paper highlights the urgent need to protect electronic communications against quantum attacks by leveraging two novel approaches: Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). The study aims to evaluate the effectiveness, scalability, and integration possibility of these technologies separately and in mixed combinations, to achieve long-term resilient cybersecurity. This research is a mixed-methods study that combines literature analysis, expert surveys, and performance benchmarking to determine the strength of encryption, compatibility with the network, and feasibility in the real world. First-hand information was gathered through structured surveys among cybersecurity professionals and scholars. In contrast, second-hand information was retrieved from peer-reviewed journals and official standards of institutions, such as NIST. It has been found that QKD offers unparalleled information-theoretic security, founded on quantum mechanics, yet has limitations in terms of scale and cost. PQC algorithms, however, especially lattice-based cryptography, are simpler to integrate into a classical infrastructure but present a performance issue on hardware with limited capabilities. Based on the study, a hybridized cryptographic model appears to be the best solution to the current approach of implementing the secure key exchange properties of QKD and the universal properties of PQC, without compromising either.

Keywords: Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), Quantum-Resistant Security, Hybrid Cryptographic Framework

1. Introduction

Quantum computing is a branch of computer science that has received considerable investment in recent years as the world braces for the exascale era. The rapid evolution of quantum computing creates a cybersecurity gap for both digital and communication assets. Classical cryptographic algorithms, such as RSA and Elliptic Curve Cryptography (ECC), are not considered secure in light of quantum algorithms like Shor's, which are designed to efficiently solve the complex mathematical problems upon which these systems depend [1]. Furthermore, as quantum capabilities improve, the confidentiality and integrity of communication networks, financial systems, and critical infrastructure are at risk of compromise [2]. Quantum key distribution (QKD) is based on quantum principles, such as superposition and the no-cloning theorem, whose capability for theoretically unbreakable key exchange depends on providing a theoretical proof [3]. However, real-world usage is constrained by high costs of implementation, limited range, and dependence on trusted relaying nodes, which present security problems [4]. To overcome these challenges, new routing methods and network designs are being developed that

aim to guarantee zero-trust security, utilize rotating key exchange paths, and employ moving target defense strategies, along with adaptive recovery mechanisms that strengthen QKD networks [3]. The software-defined network (SDN) paradigm provides flexibility and security due to the dynamic resource allocation, which would ultimately reduce cost and enhance scalability, achieved in Time-Division Multiplexing (TDM)-based Quantum Key Distribution (QKD) networks with shared infrastructure [5,6].

Post-quantum cryptography (PQC) aims to resist both classical and quantum computational key attacks using or based on mathematical problems that are computationally intractable, including lattice-based, error-correcting code-based, and multivariate polynomial equation-based problems. PQC algorithms demonstrate scalability and can be feasibly integrated into existing digital infrastructures without requiring new hardware, thereby facilitating a practical transition to quantum-resistant encryption methods [4].

Lattice-based cryptography is one of the many methods of PQC. It has shown great promise in protecting sensitive data in transit and securing vital infrastructure in the post-quantum era, based on the use of computationally challenging problems such as the Shortest Vector Problem (SVP) and Learning with Errors (LWE) [7]. The paper evaluates the current quantum key distribution (QKD) and post-quantum cryptography (PQC) technologies to propose a hybrid cryptographic solution that supports digital ecosystems in the modern context. This way, it aims to provide the following question: How does QKD guard against quantum attacks? What challenges arise when scaling QKD for many users? How can post-quantum algorithms work with current security systems? What mix of QKD, and PQ tools ensures lasting security in encryption? This paper synthesizes advancements in quantum networking, software-defined infrastructure, and post-quantum algorithms to help organizations achieve quantum-secure, resilient communications and long-term data protection. Additionally, it contributes to global efforts to safeguard critical information systems against emerging quantum threats and to maintain digital trust in the future.

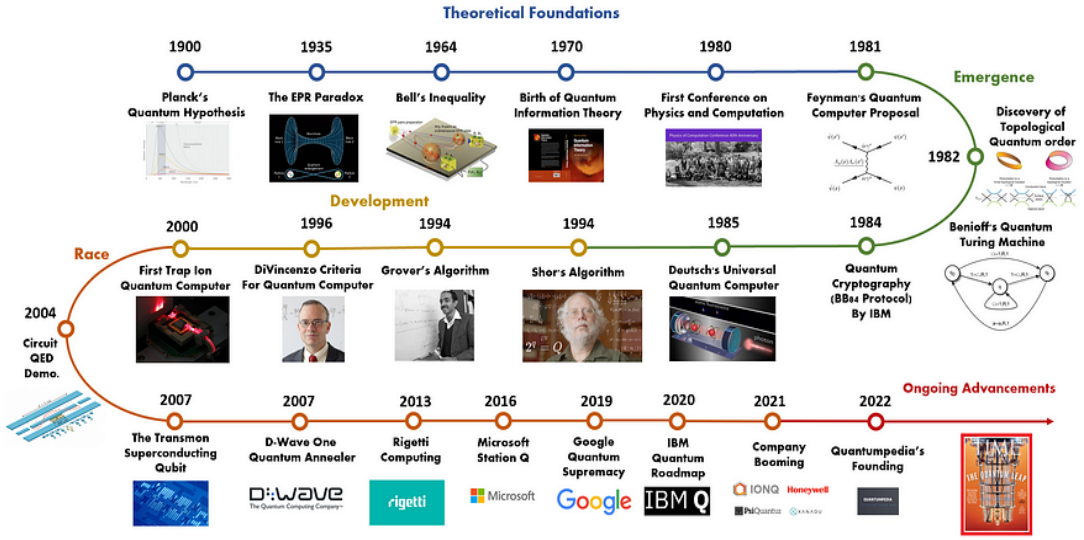

Figure 1: Quantum Computing [8]

2. Literature Review

Cryptography has been the backbone of digital communication security for decades, supporting various means such as intrusion detection systems (IDS), system authentication, and zero-trust security [5,9]. Nevertheless, the threat of new developments in quantum computing poses a significant risk of rendering standard cryptography completely ineffective. Algorithms such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) form the critical constituent of Public Key Infrastructure (PKI), which is exclusively based on the intractability of problems, including but not limited to integer factorization and discrete logarithms. This dependence is, in turn, used to decipher these encryption schemes in quantum algorithms, of which the best-known is Shor [10].

2.1. Evolution of Cryptography and Vulnerabilities of Classical Encryption

Public-key cryptography, introduced by Diffie and Hellman in 1976, enabled secure key exchange without the need for shared secrets. This led to the development of RSA and ECC, which rely on mathematical complexities such as prime factorization and discrete logarithms [11]. RSA and Diffie-Hellman (DH) are robust against classical threats, but security is fundamentally compromised under quantum computing due to the inherent limitations of these mathematical foundations. Shor's algorithm, introduced in 1994, altered the cryptographic landscape by enabling quantum computers to solve these problems exponentially faster than classical ones [12]. As a result, RSA and ECC are likely to face eventual obsolescence.

Quantum computing poses an immediate and critical threat to public-key algorithms. Systems built on RSA and ECC, currently securing everything from banking to defense, would become ineffective in a post-quantum era [13]. This threat is compounded in the harvest-and-decrypt-later model, where adversaries harvest encrypted data today to allow themselves to decrypt it at some point in the future when quantum computing becomes available [14]. Coming to implementation, however, this remains a significant obstacle because legacy systems in finance, government, and healthcare are ill-suited to rapid changes, typically due to their complex nature and associated costs. These industries are particularly vulnerable, given that they rely on outdated cryptographic systems. Retrofitting of RSA-based systems exposes vulnerabilities unless it is accomplished thoroughly through upgrades. Sahu and Mazumdar emphasize that interoperability and compliance are crucial for a seamless transition to a complete system, which should reportedly preserve the effectiveness of PQC [1]. Thus, research must pivot toward practical migration frameworks that address cryptographic changes alongside architecture redesign, regulatory alignment, and workforce readiness, which post-quantum transitions may introduce more risk than protection [15].

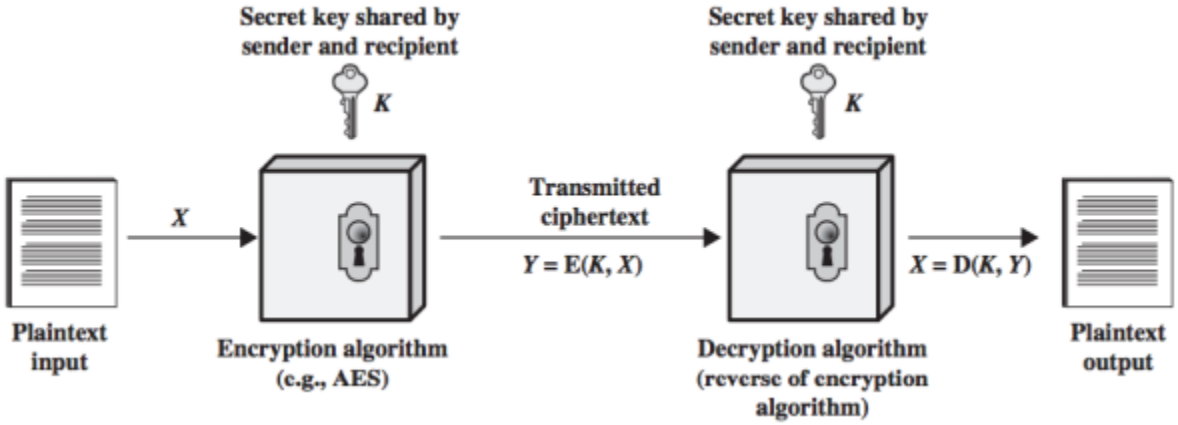

Figure 2: Classical Encryption Techniques (https://notes.shichao.io/cnspp/ch2/)

2.2. Quantum Key Distribution (QKD) Challenges

Information-theoretic Security in QKD is commonly touted as having this security because two quantum properties are impossible to achieve: the no-cloning theorem and quantum superposition. Quantum violations of information security enabled the BB84 protocol to demonstrate that monitoring a quantum channel can introduce measurable disturbances [16]. Nevertheless, although it has several advantages, QKD is hardly practical for real-life applications. The problem with its implementation is that it requires specialized communication channels in quantum communication, namely, fiber optics or satellites, which are costly to install and scarce. QKD also suffers from environmental interference and distance limitations.

Additionally, it cannot achieve scalability due to hardware irregularities, particularly in one-photon detectors. According to GSMA and Diamanti et al., the lack of uniformity in standards and validation procedures is a significant impediment [17,18]. As the next step, industry and academia should initiate the development of certification systems, implementation packages, and cost-effective infrastructure of QKD. An interesting way to justify the significant investments required to establish Quantum Key Distribution Networks (QKDNs) is through the sharing of resources between QKD transceivers in optical switches and a central Software-Defined Networking (SDN) controller. Optical switches enable the routing and reconfiguration of quantum channels by sharing devices at the QKD layer. However, they often cause signal losses that reduce key generation capacity. Due to distance limitations in quantum channels, trusted relays are commonly used in current QKDN deployments, as quantum repeaters are still in their early stages of maturity [6]. SDN has transformed network management by consolidating control and improving adaptability, which is crucial for QKD networks that require a dynamic management plane to monitor and control their quantum resources from a single controller node [5].

2.3. Post-Quantum Cryptography (PQC) and Standards

PQC, in its turn, provides a more easily implementable solution. It also utilizes classical infrastructure and relies on the complexities of quantum-resistant cryptography, which may involve lattices, codes, and multivariate polynomials [19]. One of the most promising candidates for post-quantum cryptosystems (PQC) is lattice-based cryptography (LB-cryptosystems), which is based on the assumption of a computationally intractable mathematical problem, Learning with Errors (LWE) [7]. In 2016, the National Institute of Standards and Technology (U.S.) started a PQC standardization program. It was vetted stringently, and only key encapsulation (CRYSTALS-Kyber) and three digital signatures (CRYSTALS-Dilithium, Falcon, and SPHINCS+) were chosen as finalists in 2022. These became formalized in FIPS in August 2024 [20].

Nevertheless, implementations of PQC do have problems. Specific algorithms are demanding in terms of processing power and memory, and therefore cannot be used in mobile and IoT environments. Also, they are susceptible to the side-channel attacks, which analyze time or power. Mamatha et al. recommend studying lightweight, low-area secure post-quantum cryptography (PQC) that incorporates measures to deal with constrained environments within its design [21]. In the context of the Internet of Vehicles (IoV), where intelligent, connected vehicles rely on latency-sensitive cloud services transmitted over inherently insecure wireless communication channels, security and privacy concerns are becoming increasingly critical. To mitigate the threats posed by malicious entities and the anticipated challenges of quantum computing, a lattice-based, secure, and efficient multi-cloud authentication and key agreement scheme has been introduced for quantum key distribution (QKD)-enabled Internet of Vehicles (IoV) systems. This scheme leverages lattice-based lightweight signature mechanisms in conjunction with quantum authentication keys and is supported by a Quantum Security Service Cloud (QSC), which facilitates centralized authentication management. The proposed approach effectively reduces computational complexity and decreases the number of required authentication rounds, thereby enhancing the overall efficiency and resilience of Internet of Vehicles (IoV) security frameworks [22].

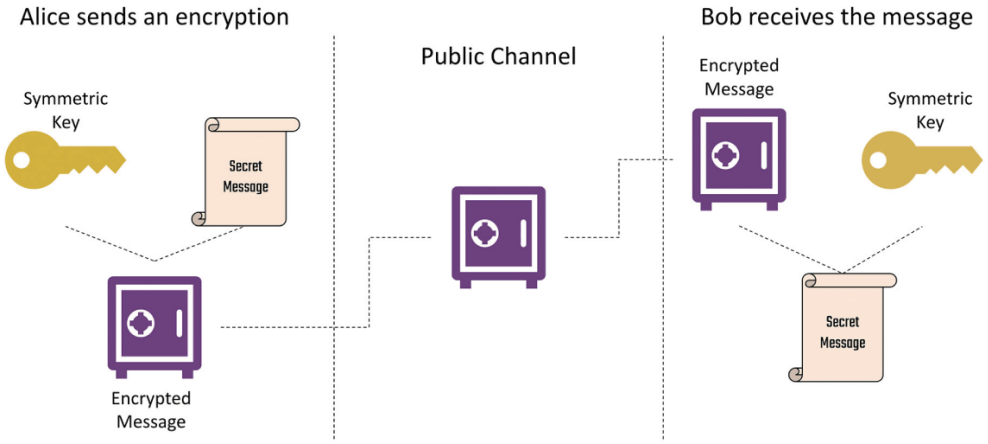

Figure 3: Post-Quantum Cryptography Action [23]

3. Research Method and Design Framework

This study employs a mixed-methods, systematic design to examine the growing weaknesses of RSA and ECC encryption systems in the face of the modernization of quantum computing-based activities. The objective of this work is to assess how Quantum Key Distribution (QKD) and post-quantum (PQ) cryptographic algorithms can be utilized to build scalable and secure digital communication networks. The design adopts a multidimensional approach to the study, establishing its theoretical and empirical foundations to make the study responsive to the serious concerns expressed in the problem statement. Its research foundation is based on quantum information theory, cryptographic algorithms, and network security architecture. This integrated design enables a holistic understanding of quantum threats and the development of secure cryptographic responses in a post-quantum world. To guide this inquiry, the study proposes the following research questions:

1. How does Quantum Key Distribution (QKD) better protect digital systems from quantum-based attacks?
2. What technical problems occur when expanding QKD networks to many users?
3. What combination of QKD and post-quantum (PQ) tools offers a lasting security method for encryption systems?

3.1. Data Collection Strategy and Sources

This study employs a systematic and structured approach to data collection, addressing five essential aspects: what data is needed, where it is located, how it will be obtained, what limitations exist, and how it will be interpreted. The research draws on both primary and secondary data sources to build a robust and credible knowledge base. Primary data is collected through structured surveys directed at cybersecurity experts, academic researchers, and postgraduate students specializing in quantum cryptography [24]. The survey is administered via Google Forms /Microsoft Forms to ensure accessibility and respondent anonymity. It comprises several combinations of multiple-choice, Likert-scale, and open-ended questions designed to gather measurable information and elicit enriched qualitative views on how QKD and the PQ algorithms will be implemented. Among the sources of secondary data, one may note journal articles reviewed by other scholars, industry-related publications, technical reports, and official publications by institutions such as NIST and ETSI. This material presents current and relevant facts regarding the performance of such a system, strategic assessments, and the ongoing evolution of quantum-safe cryptographic systems [24,25]. The data collection stage is planned to ensure that it meets the requirements of privacy and integrity. The sampling size of 30-40 participants, representing the chosen demographic groups, was invited through an email message and allowed 2 weeks to complete the survey. I think that it will take 1015 minutes. The survey answers were stored in a secure environment and downloaded in an anonymous form for

further analysis. The sample size is appropriate, as it is neither too high to conduct in-depth research nor too low to be workable.

3.2. Evaluation and Analysis of Cryptographic Solutions

The research employs a combination of technical benchmarking and strategic evaluation to assess the effectiveness of QKD and PQ cryptographic tools. Performance benchmarking measures include encryption speed, key exchange efficiency, accuracy, and operational behavior across different test environments [26]. These metrics allow for comparative analysis between quantum-safe algorithms and conventional cryptographic systems. Security analysis evaluates the robustness of these cryptographic tools against classical and quantum attacks. This includes examining algorithmic resistance to quantum computing techniques such as Shor's and Grover's algorithms and the mathematical complexity that underpins the cryptographic methods [10]. Additionally, integration assessments test the compatibility of PQ algorithms with existing digital systems, with a particular focus on standard communication protocols such as TLS and IPsec [26]. The study adheres to the principles of validity and reliability to ensure the authenticity of the research results. This strategy is observed in ensuring validity through the establishment of transparent and goal-oriented survey questions that cover all technically and strategically relevant domains [27]. The uniformity of protocol testing will ensure the reliability, inter-rater agreement in qualitative coding, and repeatable measures of time. Coupled together, these evaluation methods enable a sound and technically grounded assessment of the researched cryptographic solutions.

3.3. Limitations and Ethical Considerations

Although its methodology is comprehensive, various limitations have been recognized in the research. Another major limitation is that there is only limited real-world implementation of QKD networks, which limits access to substantial operational data. Additionally, several PQ cryptographic algorithms are still in the standardization process, which results in a scarcity of implementation and interoperability benchmarks. Although a sufficient sample of 30-40 was used due to the exploratory nature of the study, generalization is limited. To uphold ethical integrity, the overall research practice was entirely transparent, and the participants' privacy was always respected. Prior to participation, they were informed in depth about the study's aims and procedures and requested to provide informed consent. No personal data on the patients was received, and all information was stored in an anonymized way.

4. Results and Analysis

This study critically examines the mounting threats posed by quantum computing to classical encryption systems, particularly those relying on RSA and ECC algorithms. As quantum systems advance toward executing Shor's algorithm for efficient factorization, the foundational security of public-key cryptography is facing a severe compromise. In response, this analysis assesses the potential of Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) in defending against quantum attacks. Key areas include the scalability of QKD, integration strategies for PQC, and the development of hybrid models to fortify modern cryptographic systems.

4.1. Quantum Threats to Encryption

The emergence of quantum computing poses a significant threat to conventional cryptographic systems worldwide. At the core of this threat are quantum algorithms that can compromise the mathematical problems on which classical encryption is built. Shor's algorithm, introduced in 1994, enables the efficient factoring of large integers and the solving of discrete logarithms, the fundamental basis of RSA and ECC encryption. Once quantum computers reach a sufficient scale and fault tolerance, public key infrastructure (PKI) relying on these schemes will become obsolete [28]. Symmetric encryption, such as AES, is also affected, but to a lesser extent. Grover's algorithm can accelerate brute-force attacks, reducing the security of AES-128 to just 64 bits. To counteract this reduction, transitioning to AES-256 is now considered necessary [29].

Name	Pre-Quantum Security Level	Function	Post-Quantum Security Level	Impact
AES-128	128	Block cipher	64	Cracked by Grover's algorithm
AES-256	256	Block cipher	128	Cracked by Grover's algorithm
SHA-256	256	Hash function	128	Cracked by Grover's algorithm
RSA-3072	128	Encryption	Broken	Cracked by Shor's algorithm
RSA-3072	128	Signature	Broken	Cracked by Shor's algorithm
256-bit ECDH	128	Key exchange	Broken	Cracked by Shor's algorithm
256-bit ECDSA	128	Signature	Broken	Cracked by Shor's algorithm

Source: Li et al [30]

Table 1: Impact of Quantum Computing on Common Encryption Methods

4.2. Effectiveness of QKD in Security

The novelty of Quantum Key Distribution (QKD) lies in its security, which is grounded in quantum physics, rather than relying on computational complexity. Its concepts include the no-cloning theorem and measurement disturbance to determine whether there are any eavesdropping attempts on key transmission, thus

offering information-theoretical security that even an enemy with unlimited computational power cannot break [31]. In contrast to classical and post-quantum algorithms, the advantage of QKD is that it leverages the physical properties of quantum particles, rather than relying on specific mathematical assumptions. Nevertheless, the hardware of the QKD may be susceptible to implementation vulnerabilities, such as side-channel attacks; thus, it is essential to thoroughly design the hardware and system [32]. Significant developments have been achieved regarding the practical application of QKD. As shown in the article, researchers demonstrated the feasibility of a 128 km fiber optic QKD connection, generating a stable key over 28 days despite optical losses [33]. Additionally, the implementation of a QKD-secured backup network in Cambridge confirmed the general usefulness of quantum key distribution in securing critical infrastructure against future quantum threats. Although these achievements have been made, QKD continues to face challenges, including limited line length, expensive equipment, and integration difficulties. These are the impediments to QKD adoption that should be addressed before its implementation in more comprehensive communication systems.

Attack Vector	QKD Vulnerability Level	Mitigation Measures	Implementation Complexity
Eavesdropping	Low (theoretical)	Quantum mechanics ensures detection of interception	specialized quantum hardware)
Denial of Service (DoS)	High	redundancy, ML-based detection	High (complex detection/response needed)
Man-in-the-Middle	Medium-High	Strong authentication of classical channel	Moderate (requires secure authentication protocol)
Implementation Attacks	Medium-High	audits, side-channel mitigation	High (specialized hardware and ongoing research)
Channel Tampering (e.g., Amplification)	Medium	attack classification, postselection	High (advanced detection algorithms)
Insider Threats/Trusted Relay Compromise	Medium	Physical security, trusted node management	High (requires secure facilities, trusted personnel)
Local Oscillator Attacks (CV-QKD)	Medium	Multiplexing, local oscillator generation at receiver	High (precision hardware and calibration)

Source: Christoph [31]

Table 2: QKD Security Analysis against Different Attack Vectors

Parameter	Quantum Key Distribution (QKD)	Quantum-Resistant Algorithms
Cost	High (requires specialized hardware)	Low (software-based implementation)
Scalability	Limited (effective over short distances)	High (easily deployable across networks)
Infrastructure Needs	Requires dedicated quantum hardware and fiber links	Leverages existing classical infrastructure
High-Sensitivity Suitability	Very strong (ideal for high-security sectors like government and defense)	Suitable for general purposes and enterprise use

Source: Gitonga [32]

Table 3: QKD Pros and Cons Analysis

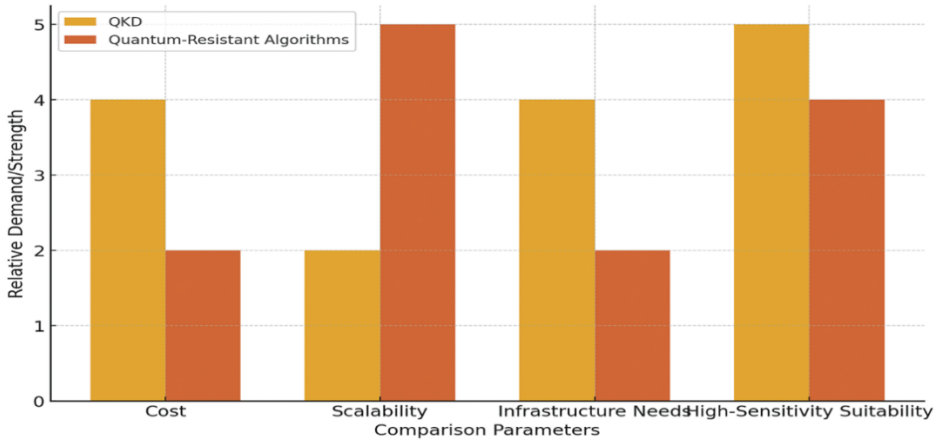

Figure 4: QKD viability analysis [32]

4.3. Performance and Scalability of PQC

An alternative technique is Post-Quantum Cryptography (PQC), which offers smooth integration into existing infrastructure because it leverages a problem that has not been solved in terms of existing computationally intractable mathematical problems, assumed to be secure against both classical and quantum attacks. Three PQC standards (CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+) completed the final stages of the NIST evaluation process in February 2025 [34]. The CRYSTALS-Kyber (including its Kyber-768 version) is as secure as AES-192 and protects against known quantum-based threats [35]. SPHINCS, an advanced hash-based signature algorithm, offers high levels of digital signature security; however, it has the disadvantage of requiring larger key sizes. This is the main difference between PQC and QKD, as it can be easily deployed on classical computing systems without the need to prepare specialized quantum hardware, unlike QKD. PQC algorithms, however, require more memory, computational power, and keys in many cases, which are often wider than those used in traditional cryptography, potentially affecting the performance of low-resource devices [32]. The key elements for successful PQC scalability are compatibility with current communication protocols, the presence of adequate computing resources, and the infrastructure's capability to support increased memory and bandwidth demands. Notwithstanding these difficulties, PQC is generally the more imminent and feasible scheme for securing systems prior to the widespread adoption of quantum computers.

Algorithm	Key Size (KB)	Encryption Time (ms)	Decryption Time (ms)	Signature Generation Time (ms)	Signature Verification Time (ms)
CRYSTALS-Kyber	1.5	1.05	0.98	N/A	N/A
SPHINCS+	32	N/A	N/A	14.5	9.25
McEliece	64–135	2.8	2.45	N/A	N/A
RSA (2048-bit)	0.26	0.8	0.85	0.9	0.75
ECC (256-bit)	0.07	0.7	0.65	0.65	0.6

Source: Gitonga [32]

Table 4: PQC Algorithm Performance Metrics

4.4. Hybrid Approaches for Future Security

With the current setbacks of QKD and PQC devices when applied individually, a hybrid cryptography system is proving to be a potential solution. They integrate the information-theoretic security of QKD with the layered protection levels of PQC, enabling simultaneous protection against multiple technologies, both current and future. Under a hybrid configuration, QKD swaps secure keys among key nodes with high confidentiality and integrity. Subsequently, such keys enable PQC algorithms to encrypt and verify messages over broader networks, representing a wise trade-off between impressive protection and feasible performance, which addresses QKD scalability and the long-term resilience of PQC [17]. The hybrid model allows flexible implementation. Organizations can start by integrating PQC into existing systems and gradually deploying QKD where possible. Standardized APIs enable PQC integration with minimal disruption, supporting incremental transitions. This dual approach provides robust quantum threat protection while also accommodating technical readiness and budget constraints. This framework addresses key challenges:

a. Secures both current and future data.

b. Enables phased deployment across complex infrastructures.

c. Minimizes single points of failure by combining the strengths of each method.

As quantum computing becomes increasingly viable, hybrid solutions will likely form the foundation of long-term cryptographic defenses.

Feature	PQC	QKD	Hybrid (PQC + QKD)
Security	Conjectured	Proven	Stronger combined security
Distance	Unlimited	Limited	PQC extends QKD reach
Cost	$$	$$$	Balanced cost-performance
Authentication	Included	Needs initial setup	PQC supports QKD setup
Certification	NIST draft	ETSI/ISO draft	Broader standards coverage
Integration	Software-based	Hardware-based	Flexible and layered
Implementation Security	Needs secure design	Needs secure design	Reduced risk with both
Security Assurance	Needs real-world testing	Needs real-world testing	More robust evaluation

Source: Erven [36]

Table 5: PQC vs QKD vs Hybrid: Comparative Analysis

Category	Challenge	Potential Solution / Mitigation	Applies To
Technical Performance	Distance Limitation (Fiber)	Quantum Repeaters (R&D); Satellite QKD	QKD
	Low Secret Key Rates (SKR)	Hardware R&D (Sources/Detectors); Advanced Protocols (e.g., TF-QKD)	QKD
	Hardware Imperfections (Sources/Detectors)	Improved Hardware Design; Decoy States; Error Correction	QKD
Practical Deployment	High Cost	Cost Reduction via Manufacturing Scale/Integration; Simpler Protocols	Both
	Integration Complexity	Hybrid Architectures; SDN Control; Standardized Interfaces/APIs	Both
	Lack of Skilled Workforce	Education & Training Programs	Both
Security Vulnerabilities	Implementation vs. Theory Gap	Rigorous Testing & Certification; Secure Hardware Design	Both
	Detector Side-Channels (Blinding, Timing, etc.)	Countermeasures (Filters, Monitors, Self-Test)	QKD (mostly)
	Trojan Horse Attacks	Optical Isolators; Monitoring; Filtering	QKD
	Photon Number Splitting (PNS)	Decoy State Protocols; True Single-Photon Sources	QKD
	Lack of Inherent Authentication	PQC Signatures; Pre-Shared Keys; Secure Auth Protocols	Both
	Denial-of-Service (DoS) Risk	Network Resilience Strategies; Protocol Robustness; Redundancy	Both
Standardization/Maturity	Immature Repeater or Hardware Tech	Continued R&D in Quantum Memories, Entanglement Swapping/Purification	QKD
	Lack of Mature Standards	Active Development in ETSI, ITU-T, ISO/IEC (QKD); NIST PQC Standards	Both
	Need for Certification Frameworks	Methodologies (e.g., Common Criteria PP)	Both

Source: Kumar [37]

Table 6: Overview of Significant Challenges in Quantum Cryptographic Deployment

4.5. Case Studies and Real-World Applications

QKD and PQC demonstrate their capacity and complex deployment limitations when delivering practical solutions to large-scale implementation. Several case research findings show that quantum-resistant systems provide essential components for creating modern infrastructure communication networks with safeguarded systems.

Case Study 1: Orange's Paris Region QCI Project

Orange, in collaboration with ID Quantique and CryptoNext, deployed a hybrid QKD-PQC system on the Île-de-France fiber network. QKD secured key exchanges while PQC protected relay points and authentication, demonstrating seamless integration into existing telecom infrastructure [38].

Case Study 2: Trident HSM – Quantum-Safe Hybrid Key Distribution

The Trident Hardware Security Module (HSM) by i4p combines QKD-generated keys with PQC encapsulation, offering secure cryptographic key storage. Compliant with ETSI guidelines, it represents an early commercial application of hybrid quantum-safe encryption [39].

Case Study 3: PSNC & GÉANT's Transatlantic Hybrid Network

A collaborative quantum-classical network was established between PSNC, GÉANT, and Internet2, connecting facilities in Poland and the U.S. QKD secured local links. At the same time, PQC enabled encrypted transatlantic communication,

demonstrating the practicality of hybrid systems for international research [40].

5. Conclusion

The results suggest that it is crucial to abandon classical cryptography in general, as it becomes increasingly vulnerable to quantum attacks, as demonstrated by the work of Shor and Grover. QKD also offers unrivaled theoretical security, but presents challenges related to cost, scalability, and infrastructure. PQC is more convenient to implement in existing systems, and entails performance and key-size trade-offs. An intermediate strategy involving secure key distribution using QKD and encryption using PQC models the optimal combination of the two methods. This is in concord with the laws of information theory, and it is a real-world limit. Failure to adopt might make important industries, such as finance, defense, and healthcare, very susceptible to interruptions. A synergy between QKD and PQC can provide more secure cybersecurity compared to using either method separately. Together, they strengthen protection against long-term threats such as "harvest now, decrypt later," which keeps data safe both in the present and in the future. Nevertheless, QKD and PQC may not be feasible for everyone due to their infrastructure requirements and might overburden low-resource systems. Thus, a hybrid approach is not a universal solution, but rather one that is versatile and accommodating.

5.1. Future Research in Quantum-Resistant Security

The direct adaptation of quantum-resistant technologies into existing systems, as well as the development of new ones, should be the primary research priority. Although the development of algorithms is on the rise, there is still a need to deploy them with effective methods that guarantee their safe implementation with minimal interference. The areas of focus will be improving the cross-compatibility, enhancing operational efficiency, and making implementation practical. QKD still has problems, such as limited transmission distances and expensive and low-key rates. These advances in quantum repeaters, integrated photonics, and satellite based QKD can help address the barriers. Future studies should also examine the economic, legal, and social implications of transitioning to more quantum-resilient systems on a broader scale. There is a need to research evaluating costs, rule gaps, and the effects on digital privacy. Moreover, there is a need to develop standardized testing models and interoperability standards that enable uniform global adoption. Such attempts will facilitate the safe, scalable, and unified integration of QKD, PQC, and hybrid frameworks across industries and between nations [41-58].

References

1. Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: applications and future prospects. *Frontiers in Physics, 12*, 1456491.
2. Ganeshkar, V., & Kulkarni, M. (2024). Quantum cryptography for a secure communication. *International Journal of Research In Computer Applications and Information Technology (IJRCAIT), 7*(1), 17-29.
3. Ghourab, E. M., Azab, M., & Gračanin, D. (2025). A Quantum Key Distribution Routing Scheme for a Zero-Trust QKD Network System: A Moving Target Defense Approach. *Big Data and Cognitive Computing, 9*(4), 76.
4. Franke, L. (2025). *Quantum Key Distribution vs. Post Quantum Cryptography*. Utimaco.
5. Hadi, H. S., & Obaid, A. J. (2025). Quantum key distribution (QKD) for wireless networks with software-defined networking. *Internet Technology Letters, 8*(2), e547.
6. Hernandez-Hernandez, J. C., Larrabeiti, D., Calderon, M., Soto, I., Cimoli, B., Liu, H., & Monroy, I. T. (2025). Designing optimal Quantum Key Distribution Networks based on Time-Division Multiplexing of QKD transceivers: qTDM-QKDN. *Future Generation Computer Systems, 164*, 107557.
7. Shekhawat, H., & Gupta, D. S. (2024). A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era. Concurrency and *Computation: Practice and Experience, 36*(14), e8080.
8. Encyclopedia, Q. (2023). A brief history of quantum computing. *Quantumpedia – The Quantum Encyclopedia*.
9. Ashogbon, A., Ukpere, O. (2025). Evaluating the Application of Zero Trust Architecture (ZTA) Implementation in Nigeria's Banking Industry. *Journal of Electrical and Electronic Engineering, 13*(3), 131-142.
10. Ivezic, M. (2025). *SHOR's algorithm: A quantum threat to modern cryptography*. PostQuantum – Quantum Computing, Quantum Security, PQC.
11. Thales, G. (2023). *A brief history of encryption* (*and cryptography*). Thales Group.
12. Marchenkova, A. (2023). *How far away is the quantum threat*? BTQ.
13. Tibbetts, J. (2019). *Quantum computing and cryptography: Analysis, risks, and recommendations for decisionmakers* (No. LLNL-TR-790870). Lawrence Livermore National Laboratory (LLNL), Livermore, CA (United States).
14. National Institute of Standards and Technology. (2024). *What is post-Quantum cryptography*? NIST.
15. Hanspal, L. (2022). *The history of cryptography*. DigiCert.
16. Jackson, P. G., Thakur, A., & Kaur, K. (2024). Quantum Cryptography. *Available at SSRN 4916293*.
17. GSMA. (2024). IG.18 opportunities and challenges for hybrid (QKD and PQC) scenarios.
18. Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information, 2*(1), 1-12.
19. Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
20. Amadori, A., Attema, T., Bombar, M., Duarte, J. D., Dunning, V., Etinski, S., Lequesne, M., Schoot, W. V. D., & Stevens, M. (2023). *The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography*. AIVD | CWI | TNO.
21. Mamatha, G. S., Dimri, N., & Sinha, R. (2024). Post-quantum cryptography: Securing digital communication in the quantum

era. *arXiv preprint arXiv:2403.11741*.
22. Yang, Z., Shi, Q., Cheng, T., Wang, X., Zhang, R., & Yu, L. (2024). A security-enhanced authentication scheme for quantum-key-distribution (QKD) enabled Internet of vehicles in multi-cloud environment. *Vehicular Communications, 48*, 100789.
23. Crypto Quantique (2025). An Introduction to Post-Quantum Cryptography.
24. Hassan, M. (2025). *Data collection – Methods, types, and examples*. ResearchMethodology.org.
25. Terra, J. (2025). *Data collection methods: A comprehensive view*. Caltech.
26. Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., ... & Alperin-Sheriff, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process.
27. Kumar, J. (2025). Quantum cryptography: An analytical report on principles, opportunities, impact, and challenges. *LinkedIn*.
28. Brubaker, B. (2024). Thirty years later, a speed boost for quantum factoring. *Quanta Magazine*.
29. Ivezic, M. (2025). Grover's Algorithm and Its Impact on Cybersecurity. *PostQuantum – Quantum Computing, Quantum Security*, *PQC*.
30. Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., ... & Xiong, N. (2023). Post-quantum security: Opportunities and challenges. *Sensors, 23*(21), 8744.
31. Christoph, M. (2023). *Implementation attacks against QKD systems*.
32. Gitonga, C. K. (2025). The impact of quantum computing on cryptographic systems: Urgency of quantum-resistant algorithms and practical applications in cryptography. *European Journal of Information Technologies and Computer Science, 5*(1), 1-10.
33. NDFF. (2022). Case Study: Long-Distance Quantum Key Distribution Secures Multi-Homed Data Backup. *NDFF*.
34. Boutin, C. (2025). NIST Releases First Three Finalized Post-Quantum Encryption Standards. *NIST*.
35. Schwabe, P. (2020). *Kyber*.
36. Erven, C. (2021). Cutting through the hype – Post-quantum cryptography vs quantum key distribution. *TECHUK*.
37. Kumar, P. (2025). *Addressing reliability and validity in survey instrument design*. Public Administration Institute.
38. Dux, S. (2024). Orange completes quantum key test on existing fibre. Mobile Europe.
39. Kristof. (2023). Quantum key distribution and post quantum key encapsulation with Trident HSM. *I4P*.
40. PSNC. (2024). Distributed hybrid quantum-classical computing in a post-quantum cryptography world. *Poznan Supercomputing and Networking Center* (PSNC).
41. Academy, E. (2024). *What are the challenges associated with the practical implementation of QKD protocols, and how do these challenges affect the security analysis*? EITCA Academy.
42. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505-510.
43. Copil, R. (2023). *What Are the Differences between Classical, Quantum, and Post-Quantum Cryptography*? Quantropi.
44. Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education, 2*(2), 25-36.
45. Dodd, P. (2024). *An unprecedented 100 km – researchers set new distance record with Quantum Keys*. SciTechDaily.
46. Emmanni, P. S. (2023). The Impact of Quantum Computing on Cybersecurity. *Journal of Mathematical & Computer Application, 2*(2), 1-4.
47. IBM. (2023). IBM quantum roadmap.
48. Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., ... & Fedorov, A. K. (2018). Quantum-secured blockchain. *Quantum Science and Technology, 3*(3), 035004.
49. Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics, 8*(8), 595-604.
50. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. *IEEE Security & Privacy, 16*(5), 38-41.
51. Mosca, M., & Piani, M. (2023). *Quantum Threat Timeline Report*. Global Risk Institute.
52. Patil, K. (2024). What you need to know about "harvest-now, decrypt-later" attacks. *AppViewX.*
53. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. *Advances in optics and photonics, 12*(4), 1012-1236.
54. Sharma, N. T., Shivangi, N., & Sharma, N. R. (2025). Post-Quantum Cryptography for Navigating Challenges and Exploring Opportunities. *International Journal of Research and Review in Applied Science, Humanities, and Technology, 2*(1), 14-21.
55. The White House. (2025). *Executive Order 14144—Strengthening and promoting innovation in the nation's cybersecurity*. Office of the Federal Register, National Archives and Records Administration.
56. Timans, R., Wouters, P., & Heilbron, J. (2019). Mixed methods research: what it is and what it could be. *Theory and society, 48*(2), 193-216.
57. Ursin, R. (2025). Quantum Key Distribution (QKD) vs. Post-Quantum Cryptography (PQC). Quantum Industries.
58. Williams, B. (2025). *Applying Thematic Analysis to Open-Ended Survey Responses*. INSIGHT.