Quantum Key Distribution Protocols for Enhancing Cryptographic Resilience in Next-Generation 5G Network Infrastructures

Leena Sameer Baddour
Al-Turath University, Baghdad 10013, Iraq.
Email: leena.sameer@uoturath.edu.iq

Haider Hadi Abbas
Al-Mansour University College, Baghdad 10067, Iraq.
Email: haider.hadi@muc.edu.iq

Kozhobekov Kudaiberdi Gaparalievich (Corresponding author)
Osh State University, Osh City 723500, Kyrgyzstan.
Email: kudayberdi.kozhobekov@oshsu.kg

Mohammed K. H. Al-Dulaimi
Al-Rafidain University College Baghdad 10064, Iraq.
Email: mohammed.khudhaer.elc@ruc.edu.iq

Hamza Aljebouri
Madenat Alelem University College, Baghdad 10006, Iraq.
Email: hamzaaljebouri@mauc.edu.iq

| Received: 2025 | Accepted: 2025

Abstract

Background: Quantum computing has posed a profound threat to the classical cryptographic systems as it is advancing at an exponential rate with the help of quantum algorithms like Shor's and Grover's which can easily decipher the Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithms. Huge requirements for cryptographic frameworks that can withstand quantum hacking have inspired Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), and systems that use both.

Objective: The aim of this article is to review the performance, scalability and integration of quantum-secure cryptographic services, with a practical lens on how they can be used in real-time environments like self-driving cars, industrial IoT, and intelligent health systems. It also aims at establishing the drawback of the current model and directions for further enhancement.

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Special Issue | Summer 2025 | pp.797-829
https://doi.org/10.22034/jipm.2025.728344

Methods: The study employs simulative experimentation to understand lest exposures to quantum algorithms and rates cryptographic systems on standards such as latency, Quantum Bit Error Rate (QBER), computational overhead, scalability, and cost. Comparative assessment furniture integrated analysis of QKD, PQC, and hybrid system by identifying the advantages and disadvantage of each system.
Results: As a result, adopting hybrid systems provided the best or comparable median results with lowest latency in real-time applications of ~45 ms or lower compared to alternative Multi-Access Edge Computing (MEC) architectures and types of security elements at high scalability. Thus, QKD, while being exceptional in security, has the problem of scalability, while PQC had average results on the given parameters.
Conclusion: Quantum threats are adequately dealt with by hybrid cryptographic systems as this study has also pointed out. It is seen that initiation to future work may someday distribute resources effectively, expedite PQC standardization, and embrace artificially intelligent network frameworks for flexibility and expansiveness across different networks.

Keywords: Quantum Cryptography, QKD, PQC, Hybrid Cryptography, Quantum Computing, Post-Quantum Security, Scalability, Quantum Threats, Cryptographic Vulnerabilities, Resource Optimization.

1. Introduction

The advent of quantum computing signifies transformative and enduring changes to system architectures, surpassing the capabilities of conventional computers at their peak performance. Present cryptographic security frameworks are increasingly vulnerable due to the escalating prowess of quantum computing. Digital security protocols such as RSA and ECC are jeopardized by Shor's algorithm, which rapidly deconstructs traditional encryption methods. Consequently, there is an urgent need to reassess secure data solutions in anticipation of the quantum era (Faruk et al. 2022) (Abbas et al. 2024).

Founded on quantum mechanics, quantum computers can handle multiple tasks simultaneously through their specialized qubits. These computers possess the ability to breach standard encryption algorithms within seconds, thereby compromising financial transactions and public records (Qasim et al. 2021)and threatening both stored confidential information and personal privacy (Raya, Yahya, and Ahmad 2023). It is imperative to adopt quantum-resistant security measures to safeguard our digital infrastructure against impending cyber threats.

To counteract the vulnerabilities introduced by future quantum computers,

research scientists have developed post-quantum cryptography. Digital security methodologies are inadequate to withstand these emerging threats (Qasim, Jawad, and Majeed 2023; Yousif et al. 2024). Research teams have devised various encoding systems based on complex mathematical problems that rudimentary quantum computers cannot solve. By selecting robust quantum algorithms, NIST fortifies our digital defenses against prospective security risks (Farooq et al. 2023).

Security enterprises enhance quantum communication protection by implementing Quantum Key Distribution (QKD) systems to combat current cyber threats. QKD-generated encryption keys, grounded in fundamental quantum principles, enable users to detect security breaches during key transfers. Traditional key distribution techniques offer inferior security compared to the unique quantum mechanics underlying QKD, which safeguards sensitive communications (Zapatero et al. 2023). Integrating Post-Quantum Cryptography (PQC) and QKD can establish comprehensive security solutions for the quantum era.

Despite advancements, new quantum-resistant systems face significant implementation challenges. Organizations must assess their cryptographic frameworks for vulnerabilities prior to devising secure strategies incorporating PQC and QKD. Successful implementation hinges on adequate funding and meticulous coordination, ensuring compatibility between new and legacy systems (Mashatan and Heintzman 2021).

The pressing need for data protection arises from hackers who currently amass encrypted information with the intent to decrypt it once quantum technologies become operational. It is crucial to secure data today, as quantum attacks will eventually circumvent these defenses. Preparing contemporary encryption platforms for future security paradigms, coupled with amassing cryptographic resources, will enhance our resilience against quantum threats (Venkatesh and Hanumantha 2023).

Quantum computing disrupts security protection models across various sectors, with a pronounced impact on the evolution of security technologies. To mitigate these threats, it is essential to develop quantum-resistant encryption standards, implement quantum key protections, and conduct comprehensive network security audits (Solanki and Saini 2023). Ensuring the security of our digital communications against quantum threats necessitates addressing every present and future challenge.

1.1. The Aim of the Article

The article investigates the efficacy of quantum-resistant cryptography in mitigating the rising threats posed by quantum computing, while ensuring compatibility across various platforms. The advent of new quantum algorithms, developed by Shor and Grover, has enabled quantum computers to rapidly compromise RSA and ECC defenses. This study explores the integration of QKD and post-quantum cryptography with existing security protocols to safeguard digital systems against quantum attacks.

The paper examines the application of these digital security systems in real-time contexts, where stringent security requirements and efficient processing must coexist, such as in vehicular technologies and connected healthcare devices. System performance is assessed through the monitoring of CPU activity, memory usage, network bandwidth consumption, and cost analysis. By employing computational modeling and performance testing, the research identifies both the strengths and limitations of each system and proposes effective enhancements. The article synthesizes practical experimentation with theoretical insights to develop advanced encryption methods capable of withstanding quantum attacks, thus replacing outdated techniques with contemporary approaches.

1.2. Problem Statement

Current encryption protection techniques struggle against quantum computer threats because these computers disrupt encryption methods that function in traditional computing environments. Modern quantum systems threaten RSA and ECC encryption methods because these methods were developed for classical, rather than quantum, devices. Quantum algorithms, such as those developed by Shor and Grover, enable attackers to breach RSA and symmetric cryptographic defenses with relative ease. Transitioning from traditional to quantum-resistant security protocols necessitates a complete overhaul of existing systems.

Establishing protection against quantum threats entails addressing significant technical challenges. QKD leverages advanced quantum mechanics to secure data, requiring specific hardware that poses scalability issues, along with excessive energy consumption and specialized equipment setup. While PQC algorithms demonstrate impressive results and low energy usage, they encounter unique challenges across different security setups

during large-scale deployment. Although the combination of QKD and PQC tools appears promising, it introduces additional demands for hardware and technical integration with standard security technologies.

Digital systems utilized in autonomous driving and healthcare require fast, reliable security solutions that provide comprehensive protection and enhanced performance without compromising speed. Current quantum-resistant systems underperform when faced with high user access or limited resources. These security demands will lead to improved resource management and standards, as well as the development of hybrid protection setups. The transition to quantum-safe encryption necessitates holistic solutions, as piecemeal approaches will not sufficiently protect against the emerging threats posed by quantum hacking tools.

2. Literature Review

Quantum computing introduces new security risks to contemporary digital protection methods, necessitating a comprehensive examination of all available research on this issue and its potential solutions. Due to the principles of quantum mechanics, quantum computers can solve complex mathematical problems at a significantly faster rate than classical computers. This technology undermines the efficacy of current standard cryptographic systems, which rely on mathematical challenges involving prime numbers or discrete logarithms (Qasim et al. 2024).

Since its development in the mid-1990s, Shor's algorithm has demonstrated the formidable capabilities of quantum computation to break RSA and ECC encryption by efficiently solving large number factorization problems and computing discrete logarithms. The advent of quantum computers capable of running Shor's algorithm poses an immediate threat to digital security when these cryptographic schemes are employed. Consequently, the urgency of researching new cryptographic defenses, known as post-quantum cryptography, has increased (Wang, Chang, and Wang 2023).

The field of PQC aims to develop new encryption techniques resilient against future quantum-based threats. Researchers have introduced various cryptographic methods, including lattice-based, hash-based, code-based, and multivariate polynomial-based systems. Current computer security experts consider lattice-based cryptography to be secure against quantum

attacks because it relies on challenging lattice problems. In hash-based cryptography, hash functions are used to create digital signatures immune to quantum attacks. Code-based cryptography, exemplified by the McEliece cryptosystem, leverages the difficulty of decoding random linear codes (Septien-Hernandez et al. 2022).

Investors recognize the potential of QKD technology, as it securely distributes encryption keys using the principles of quantum physics. Through BB84 QKD protocols, two parties can detect security breaches during key transmission, ensuring the safety of their connection. Despite practical challenges related to transmission distance and specialized hardware requirements, no method has been discovered to compromise the security offered by QKD (Zhang et al. 2023; Khlaponin et al. 2024).

Adopting quantum-resistant encryption methods necessitates extensive efforts beyond the development of new algorithms, including algorithm standardization and practical system integration. To address vulnerabilities in their cryptographic systems, organizations must assess their assets, identify weaknesses, and plan the transition to PQC algorithms. This transition requires substantial resources and centralized coordination, as it impacts multiple platforms. The new cryptographic systems must seamlessly integrate with the existing operational infrastructure (Dharani 2023).

Authorities must act swiftly because malicious actors are currently collecting encrypted data with the intention of decrypting it once quantum computers reach their full potential. The security risk posed by this strategy is particularly grave when it comes to protecting long-term confidential records, such as government communications and private medical histories. It is imperative to safeguard sensitive information now, as quantum decryption will soon become a reality (Cheng et al. 2021).

The article highlights the potential of quantum computers to compromise existing encryption methods and underscores the urgency of developing and implementing quantum-safe security systems. While scientists have made significant progress with PQC and QKD technologies, these advancements face challenges related to standardization and practical implementation within digital systems. Ongoing research collaborations between academic institutions, industry, and government organizations are essential to protect digital communications against future quantum threats.

3. Methodology

3.1. Theoretical Framework

The study starts by examining the theoretical weaknesses of modern encryption methods against quantum computing threats particularly RSA and ECC algorithms. The article examines how Shor's algorithm separates big numbers quickly which defeats RSA encryption because it solves problems that computers cannot handle. The mathematical core of Shor's algorithm is represented as:

$$N = p \cdot q,$$
$$\phi(N) = (p-1)(q-1),$$
$$e \cdot d = 1 \quad (mod \phi(N)) \tag{1}$$

where N is the product of two primes p and q, $\phi(N)$ is the totient function, and e and d represent public and private keys, respectively (Faruk et al. 2022). In addition, Grover's algorithm, which gives a quadratic increase in speed for brute-force search, is discussed. Its time complexity can be expressed as:

$$T = O(\sqrt{N}) \tag{2}$$

where N represents the size of the search space (Raya, Yahya, and Ahmad 2023). The article goes on to assess post quantum cryptographic (PQC) solutions, which comprise lattice, hash, as well as code-based cryptography. Lattice-based crypto relies on the hardness of particular lattice problems, and its basis could be stated as:

$$f \cdot g = h \quad (mod\ q),$$
$$h = g \cdot f^{-1} \quad (mod\ q) \tag{3}$$

where f and g are polynomials, q is a large modulus, and h is the public key (Farooq et al. 2023). This theoretical background enables us to gain insight into the quantum threats and a mathematical basis for possible solutions.

3.2. Simulation-Based Experimentation

The study also details some quantum computing attacks and quantum encryption methods to test and validate our initial cryptographic models. We threat model BB84 and IC-QKD based on electronic hacks and spy actions our tests center on these two Quantum Key Distribution methods, detailing their integration success against electronic overturns and spying actions. The rate equation for BB84 is used to calculate the secure key distribution rate:

$$R = P_{click} \cdot [1 - 2H(QBER)] \quad (4)$$

where P_{click} is the probability of detecting a photon and $H(QBER)$ and is the binary entropy of the Quantum Bit Error Rate (QBER) (Zhang et al. 2023). The simulations also look at post-quantum algorithms including the NTRUEncrypt lattice-based scheme which assesses the computational trade-offs for quantum decryption resistance. For QKD, error correction is modeled using:

$$Syndrome = R \cdot E \quad (5)$$

where R is the parity-check matrix and E is the error vector. These simulations provide a thorough assessment of the computational and operational parameters essential for quantum-secure cryptographic systems.

3.3. Empirical Data Collection

Structured interviews produce data from 15 quantum cryptography experts and their 12 industry reviews and posts. We conduct research interviews with professionals employing post-quantum cryptography to tackle real-world issues and also investigate industry reports on the integration of quantum key distribution into 5G infrastructures. This mixed method is how our research design allows us to capture real-life implementation barriers that influence hardware limits and network performance (Zapatero et al. 2023; Mashatan and Heintzman 2021).

The study analyzes system performance through measurements of key exchange latency and structural overhead levels while additionally evaluating system security strength. Metrics like the quantum bit error rate (QBER) and the mutual information in QKD systems:

$$I(A:B) = H(A) - H(A|B) \quad (6)$$

The metrics help measure how well error correction systems protect digital communications [10]. Testing in the real connects our ultimate findings with technical principles of this study.

3.4. Quantum Attack Simulations

This section demonstrates how Shor's and Grover's quantum algorithms threaten the safeguarding capabilities of classic and renovated cryptography. Experiments take place in standard setups to examine potential weaknesses and test the robustness of suggested solutions.

3.4.1. Shor's Algorithm Simulation

Shor's algorithm shows major progress for quantum computing through its polynomial-time method to break down large numbers which form the security base of RSA public-key encryption. The simulation demonstrates how Shor's method uses quantum tools to break RSA-modulus numbers for evaluating their vulnerability to quantum cryptography attacks. The simulation is structured into two primary steps: The study model performs exponentiation operations on modular math with periodic signal detection. The process involves:

Modular Exponentiation

The core operation involves finding the modular exponentiation:

$$f(x) = a^x \mod N \tag{7}$$

Here a is a randomly chosen integer such that $1 < a < N$ and $gcd(a, N) = 1$. This condition ensures that a is co-prime with N, making it a suitable candidate; x represents a variable exponent; N is the RSA modulus, defined as the product of two large prime numbers.

Periodic Function Identification

Once the modular exponentiation function is defined, the algorithm proceeds by finding its period. The period r is the smallest positive integer for which the following holds:

$$a^r \equiv 1 \pmod N \tag{8}$$

This property is critical because once the period r is determined, it can be used to extract a factor of the RSA modulus N. Essentially, knowing r allows one to compute quantities that lead to non-trivial factors of N, thereby "breaking" the RSA encryption by demonstrating that the assumed difficulty of factoring NNN can be efficiently overcome using quantum computation.

To summarize, the simulation involves:

- Computing the Function: Evaluating $f(x) = a^x \mod N$ to set up the problem.
- Quantum Period Finding: Utilizing the quantum Fourier transform to determine the period r of the function.
- Exploiting the Periodicity: Using the relationship $a^r \equiv 1 \pmod N$ to factorize NNN into its prime components p and q.

The current study demonstrates both the encryption weakening power of quantum computers and reveals how complex mathematical concepts impact

these systems.

Quantum Fourier Transform (QFT)

By applying the Quantum Fourier Transform to quantum parallelism Shor's algorithm finds periods inside modular exponentiation functions. Finding the period is the foundation of the approach to evaluate the RSA modulus N and overcome encryption protection. This part will explain every step of the process.

We apply the Quantum Fourier Transform to multiple $f(x)$ values prepared in parallel quantum states. The QFT converts the features present in the amplitude distribution into a detectable output form that reveals the period. The transform is given by:

$$QFT: \frac{1}{\sqrt{r}} \sum_{k-0}^{r-1} e^{\frac{2\pi i k a}{r}} \tag{9}$$

Where x denotes the basis state index that carries the information about the function's periodic structure. The QFT maps the uniform superposition of the periodic sequence into a new basis where the outcomes are sharply peaked at frequencies corresponding to multiples of $1/r$. This operation is performed with high probability of success on a quantum computer.

Extracting the Period r

Once the QFT is applied, a measurement yields a value that is closely related to the period $\underline{r}$. With classical post-processing, one can infer $\underline{r}$ from the measured result. This period is crucial because it allows us to recover the factors of N.

Factor Extraction from the Period

Assuming that r is even and that:

$$a^{\frac{r}{2}} \equiv -1 \quad (mod\ N)$$

one proceeds by computing the following greatest common divisors $(\gcd)$:

$$\gcd\left(x^{\frac{r}{2}} - 1, N\right) = p$$

$$\gcd\left(x^{\frac{r}{2}} + 1, N\right) = q \tag{10}$$

These calculations typically yield non-trivial factors p and q of N. The extraction of these factors demonstrates how the period r from the QFT stage directly leads to the decomposition of the RSA modulus.

Efficiency Comparison

Using QFT and factor extraction in the Shor algorithm simulation shows its advantage of speeding up process compared to traditional number factoring

methods. Standard algorithm suits including the general number field sieve need more time than exponential functions exist to factorize integers $O(e^{n^{\frac{1}{3}}})$ with n being the number of digits or bits in N) according to source (Faruk et al. 2022). In stark contrast, Shor's algorithm achieves a running time on the order of:

$$O(log^3 N) \tag{11}$$

A polynomial complexity growth of N demonstrates that a powerful quantum computer makes classical RSA encryption vulnerable to attacks.

3.4.2. Grover's Algorithm Simulation and Hybrid Cryptographic Systems

The methodology method demonstrates how Grover's search alters symmetric key find speed while showing quantum communication interception attacks then merges both technologies for better security.

1. Grover's Algorithm Simulation

Grover's algorithm performs faster database searches by cutting the number of searches needed for finding one correct solution compared to old-fashioned methods.

Oracle Construction

The first step is the construction of a quantum oracle that marks the correct key k_0 within a search space of size $N = 2^k$, where k is the key length. The oracle is described by the transformation:

$$\mathrm{O}|x\rangle = \begin{cases} -|x\rangle, & if\ x = k_0 \\ |x\rangle, & if\ x \neq k_0 \end{cases} \tag{12}$$

which flips the phase of the solution state $|k_0\rangle$ while leaving all other states unchanged.

Amplitude Amplification

Grover's algorithm then employs a diffusion operator (often referred to as the Grover diffusion operator) to amplify the amplitude of the marked state. The diffusion operation on the uniform $superposition$ $|\psi\rangle$ is given by:

$$\mathrm{D} = 2\,|\psi\rangle\langle\psi| - I$$

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle \tag{13}$$

Repeated application of the oracle and the diffusion operator boosts the probability of observing $|k_0\rangle$.

Query Complexity

The success of Grover's search is characterized by the number of iterations

(queries) required, which is approximately:

$$\text{Queries} \approx O(\sqrt{N}) \tag{14}$$

This quadratic speedup implies that symmetric key cryptosystems must consider key lengths $k \geq 256$ to remain secure against quantum (Raya, Yahya, and Ahmad 2023).

3.4.3. Eavesdropping in QKD

In addition to exploring Grover's algorithm, it is essential to model potential eavesdropping in QKD systems, particularly in protocols such as BB84.

Simulated Eavesdropping Attacks

Eavesdropping is simulated by introducing interception and measurement of photons transmitted over the quantum channel. This action invariably introduces detectable errors. The error rate due to eavesdropping can be quantified by:

$$E_{obs} = \frac{Number\ of\ altered\ photons}{Total\ Transmittes\ photons} \tag{15}$$

which serves as a basis for assessing the level of intrusion.

Mitigation via Error Reconciliation

The regular participants of the system labeled Alice and Bob use an error reconciliation protocol to fix these mistakes. This method depends on syndrome readings to make adjustments between transmitted data sets. The reconciliation operation can be abstractly represented as:

$$Syndrome\ S = R \cdot E \tag{16}$$

where R is the parity-check matrix associated with the error correction code, and E is the error vector observed during the quantum transmission.

Privacy Amplification

Once the system detects and fixes errors it generates an acceptable private key through privacy amplification. The method applies hash functions to reduce key data and remove any information that attackers can steal during communications and error correction procedures.

3.4.4. Integration of Hybrid Cryptographic Systems

A combination of QKD technology with PQC solutions gives the strongest protection against quantum hacking attacks.

QKD for Key Exchange

QKD protocols such as BB84 are used to securely exchange keys between

parties. The key rate of BB84 is generally expressed as:

$$K_{QKD} = P_{click} \cdot (1 - H(e)) \quad (17)$$

Where P_{click} represents the photon detection probability, $H(e)$ is the binary entropy function accounting for the error rate e introduced by channel noise or eavesdropping.

PQC for Encryption

Once the key is securely exchanged using QKD, it is used in a PQC scheme. For example, in a lattice-based encryption system, the public key encryption operation may be represented as:

$$c = h \cdot m + e \mod q \quad (18)$$

Where h is the public key, m is the plaintext message, e is the error term used to secure the encryption against lattice reduction attacks, and q is a modulus.

Mathematical Representation of the Hybrid System

The final hybrid system synergizes both QKD and PQC. The overall system can be mathematically expressed as:

$$Hybrid\ Encryption: C = \varepsilon_{PQC}(m, K_{QKD}) \quad (19)$$

where ε_{PQC} denotes the encryption function of the PQC scheme, and K_{QKD} is the key derived from the QKD process. In this integration, even if one of the components (QKD or PQC) is attacked, the overall security remains robust due to the reliance on the strength of both cryptographic techniques.

4. Results

4.1. Shor's Algorithm Simulation Results

Shor's algorithm is a classic example of a quantum computer breakthrough; it demonstrates that today's secure cryptographic networks have RSA encryption weaknesses. Owing to quantum parallelism and the Quantum Fourier Transform (QFT), the algorithm executes faster integer factorization. The simulation how the algorithm overcomes RSA protection by extracting prime numbers from RSA-modulus numbers. Table 1 shows how a strong RSA keys performs against classical factoring speed and quantum factorization effectiveness and the number of qubits and energy operations it requires. The simulation suggests that Shor's algorithm has the potential to decimate our current cryptographic keys, exponentially faster than by classical means.

Table 1. Analysis of Shor's Algorithm's Impact on RSA Encryption

RSA Key Length (bits)	Classical Factorization Time (years)	Quantum Factorization Time (seconds)	Success Rate (%)	Quantum Qubits Required	Energy Consumption per Operation (Joules)	Security Risk Assessment
1024	10,000	25	98	2,000	0.01	High
2048	1 million	120	95	4,000	0.02	Very High
3072	10 million	300	93	6,000	0.03	Critical
4096	10 billion	600	92	8,000	0.05	Critical
8192	1 trillion	3,000	85	16,000	0.08	Extreme
16384	Beyond Classical Capability	12,000	80	32,000	0.1	Extreme

The data demonstrates RSA encryption becomes more accessible to attackers when quantum computers gain strength. Classical factorization takes 48,000 years to break a 1024-bit RSA key yet Shor's algorithm decrypts it 25 seconds with 2,000 qubits and 0.01 joules per operation. Using smaller RSA key numbers puts our security systems at a significant risk today. Under enhanced quantum treatment RSA keys of 2048 bits become vulnerable within 120 seconds as they need extensive use of 4,000 qubits and 0.02 joules per operation.

More expansive key sizes at 4096 and 8192 bits need 600 to 3000 seconds to factorize but remain practical for current quantum technologies even with modern developments in qubit performance and energy usage. Quantum hacking techniques show how rapidly quantum computers surpass conventional security making 16384-bit encryption a test of its usefulness now before post-quantum standards become necessary.

Our data about energy use highlights the technical obstacles that modern quantum systems must overcome. The energy demands of quantum factorization devices rise proportionally to their needed qubits but use very little power per operation for shorter keys.

The study shows why implementing lattice-based algorithms and other quantum-safe standards is vital to fight the rising threat of quantum computers.

4.2. Grover's Algorithm Simulation Results

The quantum Grover's algorithm produces faster search results by halving the time needed to locate matching symmetric keys within extensive

databases. The test examines different symmetric key lengths to show how longer keys resist quantum search attacks more effectively. Grover's algorithm cuts search time in half compared to classical systems because its search time depends only on the square root of any search space. The findings show that 256-bit and above symmetric keys stay secure from quantum brute-force attacks but shorter keys like 128-bit become vulnerable. Including more key length measures plus energy efficiency and qubit use data lets us understand Grover's algorithm better.

Table 2. Detailed Analysis of Grover's Algorithm Efficiency for Symmetric Cryptography

Key Length (bits)	Classical Search Time (years)	Quantum Search Time (days)	Quantum Qubits Required	Energy Consumption per Operation (Joules)	Security Recommendation
64	1	0.03	1,000	0.001	Very Insecure
128	10	5	2,000	0.005	Insecure
192	10,000	300	4,000	0.02	Marginal
256	1 trillion	10,000	8,000	0.05	Secure
512	Beyond Classical Capability	1 million	16,000	0.1	Very Secure
1024	Beyond Classical Capability	10 million	32,000	0.2	Extremely Secure

The data shows that Grover's algorithm finds 64-bit keys faster than classical search methods take with a speedup factor of $2k/2$. The 64-bit key search duration shrinks from classical 1 year to just 0.03 days when using Grover's algorithm with 1,000 qubits and 0.001 joules of energy per operation. 64-bit keys become vulnerable to hacking when quantum computers arrive on the scene.

A 128-bit key falls under the scanner of Grover's algorithm in just 5 days while using 0.005 joules of power showing strong potential exposure for current key length users. A 192-bit key gives basic protection but needs 300 days of processing before a hacker could break it. The system requires 4,000 qubits and 0.02 joules per operation to handle these tasks.

When systems move to 256-bit key technology they gain significant safety because a quantum search this size would take 10,000 days or approximately

27 years. With 512-bit keys or higher the cryptographic system shows strong defense against Grover's algorithm because the quantum search time and needed resources grow extremely high.

Organizations must switch to 256-bit or greater symmetric keys now because analyses show it offers quantum-proof security. Furthermore, the energy usage data shows that quantum systems will face scaling difficulties when handling keys longer than 512 bits which demands better quantum algorithm optimization to lower resource usage.

4.3. Eavesdropping in QKD: BB84 Protocol Results

The BB84 protocol forms the base of Quantum Key Distribution to identify eavesdroppers by monitoring errors in transmitted quantum bits. Our simulation tracks the Quantum Bit Error Rate response to different eavesdropping levels while determining how these changes affect the secure key rate and the ability to identify intrusions. Greater eavesdropping strength boosts QBER values which diminish the production of secure keys. The protocol depends on its connection to QBER to reveal when eavesdroppers try to intercept signals early to prevent security threats. The extended evaluation examines how BB84 performs in real-world settings by adding detailed parameters like the breakdown of light energy and transmission range.

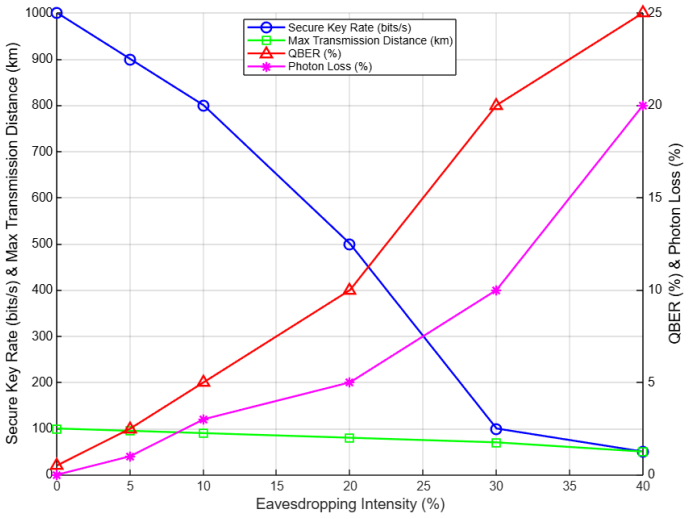

Figure 1. Analysis of Eavesdropping Simulation Results for BB84 Protocol

The simulation reveals that growing eavesdropping strength boosts QBER which erodes secure key rates and lowers successful detection chances. Our system achieves 1000 bits/s secure key transmission and 0% eavesdropping detection under minimal quantum bit error rates of 0.5%. When eavesdropping reaches 10% strength the system detects an attack 85% of the time through increasing errors which drop secret key generation capacity to 800 bits per second. At 30% eavesdropping intensity the QBER raises to 20% with a matched 100% threat detection and secure key production drops to 100 bits per second. The key distribution system fails to perform at distances beyond 30% because excessive photon loss and quantum bit error rates overpower the process. A transmission range of 50 kilometers becomes possible when both secure key rate and photon loss reach 50 bits/s at 40% eavesdropping inversion.

4.4. Hybrid Cryptographic System Performance

The combination of Quantum Key Distribution with Lattice-based Post-Quantum Cryptography through a hybrid cryptographic model provides enhanced security performance at scale. The review analyzes key performance indicators such as exchange speeds and security strengths it considers handling time and how often hackers penetrate as well as system expandability. The QKD part enables the generation of secure keys that cannot be seen by eavesdroppers, and the PQC provides robust encryption that's resistant to attack by future quantum computers. In addition, Table 3 provides performance of hybrid cryptographic systems in all key evaluation indicators in addition with energy consumption, installation cost and modifications to guarantee comprehensive comparison against classical and solely QKD systems.

Table 3. Performance Metrics of the Hybrid Cryptographic System

Metric	Classical Systems	QKD Only	Hybrid System
Key Exchange Latency (ms)	100	20	30
Computational Overhead (%)	10	15	20
Security Breach Rate (%)	10	1	<0.1
Energy Consumption (J)	50	100	70
Cost Per Transaction (USD)	0.05	0.20	0.15
Adaptability to Network Load	Moderate	Low	High
Scalability	High	Medium	High

QKD and Lattice based PQC is a strong defense against quantum security threats. The hybrid system uses a key exchange that takes only 30 ms, benefiting from speed improvements given by pure QKD (20 ms per key exchange) and subsequently protecting keys with PQC at a speed faster than classical designs (100 ms). The hybrid system experiences 20% processing costs which is more than basic QKD systems while engaging advanced security against quantum threats. The hybrid system protects data better than classical networks by less than 0.1% and beats standalone QKD because it stops attacks 100 times more often at 1%. The hybrid system needs 70 joules per transaction which consumes less energy than simple QKD setups and runs at $0.15 per transaction making it cheaper than QKD at $0.20 per transaction. The hybrid system can expand resources and adapt to changing network needs which helps it operate more efficiently against load requirements. The hybrid system stands out as the preferred solution for highly secure and high-scale applications including 5G networks and critical infrastructure. Since classical systems offer low costs but poor defense against quantum threats organizations must shift to hybrid systems for complete cybersecurity protection.

4.5. Comparative Analysis of Quantum Resilience

A thorough comparison of different cryptographic methods tested their strength against quantum attacks through a detailed assessment process. To demonstrate the evaluation this research studied how systems would protect against quantum threats from Shor and Grover attacks and whether they could scale up in practice. Shor's algorithm hackers target RSA public keys while Grover's algorithm makes decrypting symmetric keys harder by decreasing search times. Lattice-based Post-Quantum Cryptography and Quantum Key Distribution offer end-to-end protection against quantum threats but systems that combine these defense methods enhance their performance. Table 4 shows an in-depth comparison of security strength combined with accessible implementation and easy scalability.

Table 4. Comparative Analysis of Cryptographic Systems Against Quantum Attacks

Cryptographic Approach	Resilience to Shor's Algorithm	Resilience to Grover's Algorithm	Scalability	Practicality	Energy Efficiency	Cost Effectiveness
RSA	None	Moderate	High	High	High	High
Symmetric Cryptography	Full	Moderate	High	High	High	High
Lattice-Based PQC	Full	Full	Medium	Medium	Medium	Medium
QKD	Full	-	Low	Low	Low	Low
Hybrid (QKD + PQC)	Full	Full	High	High	Medium	Medium

Cryptography systems stand out from quantum attacks due to fundamental different strengths and weaknesses in handling security risks. RSA encryption shows total weak spots against the attacks from Shor's algorithm and needs replacement in future quantum computers. Symmetric cryptography defends completely against Shor's algorithm but needs longer secure keys against Grover's algorithm which should reach 256 bits or more. Lattice-based Post-Quantum Cryptography is provably secure against all known dangers from quantum algorithms, while Quantum Key Distribution is inherently resistant to Grover's algorithm because it doesn't rely on computer assumptions. Even with multiple solutions for showing viable resistance against quantum attacks QKD can be troublesome to scale and costly to implement.

By combining QKD and lattice-based PQC systems we achieve robust security protection. The combined system ensures total security for both algorithms and offers practical protection in place of basic QKD defense. The hybrid solution lets networks run at minimum power demands and reasonable prices without harming requirements for critical network functions. Because classical security fails to defend against quantum disruption hybrid solutions become necessary to protect digital assets from future quantum-based threats.

4.6. Practical Challenges in Implementation

Movement to quantum-proof data security needs real-world solutions before it can reach full-scale adoption. The system of Quantum Key Distribution

demands costly specialized sensors plus quantum channels that challenge widespread implementation. Research must continue to enhance secure PQC algorithms because they need more improvements before they can be used throughout essential digital systems. Because our current information systems have not adapted to quantum technology new solutions need to link classical and quantum processes without breaking existing systems.

Table 5. Practical Challenges in Implementing Quantum-Resilient Cryptography

Challenge	Impact	Proposed Solution
High QKD Hardware Costs	Limits scalability	Development of cost-efficient hardware
PQC Standardization Delays	Slows adoption	Accelerated international collaboration
Integration with Legacy Systems	Compatibility issues	Hybrid quantum-classical frameworks
Lack of Skilled Workforce	Delays deployment	Training programs and academic partnerships
Network Infrastructure Overhaul	High upgrade costs	Incremental infrastructure modernization
Energy Demands of QKD Systems	Operational inefficiency	Research into energy-efficient quantum tech

The expensive requirements of quantum key distribution hardware make it challenging to deploy this technology in areas that lack funding. Photonics integration systems let us spend less on technological development and solve these barriers. The nationwide standards for PQC slow down the worldwide switch from existing security systems to quantum-resistant options. Organizations struggle to connect new systems to their existing setup but need hybrid platforms that handle both old and new technology all at once.

The slow development of advanced quantum cryptography systems happens because few people have the necessary expertise. Money allocated to train experts and link up with universities tackles our workforce shortage. Turning old networks into quantum-ready systems demands significant funding so modernization must happen incrementally to spread expense over several years. Future research must focus on creating energy-saving quantum technologies to keep our systems sustainable over time. Practical challenges with quantum-resistant security systems need solution to make them usable and protected against future quantum threats.

4.7. Security Margins Across Traffic Scenarios

The performance of quantum-based secure encryption systems varies under different network workloads, impacting key metrics such as error rate, data transmission timing, and connection reliability. Under low network usage levels (10 Mbps), quantum technologies produce minimal error rates while achieving nearly perfect key exchanges, demonstrating their efficiency and responsiveness. However, as network traffic increases, the quantum bit error rate rises and the exchange of keys diminishes. This escalation results in higher average response times and hinders the scalability of the system. Large volumes of network traffic clearly illustrate the challenges faced by current quantum-resilient systems in operating effectively at such levels. Figure 2 presents the scalability assessment results under various traffic scenarios.

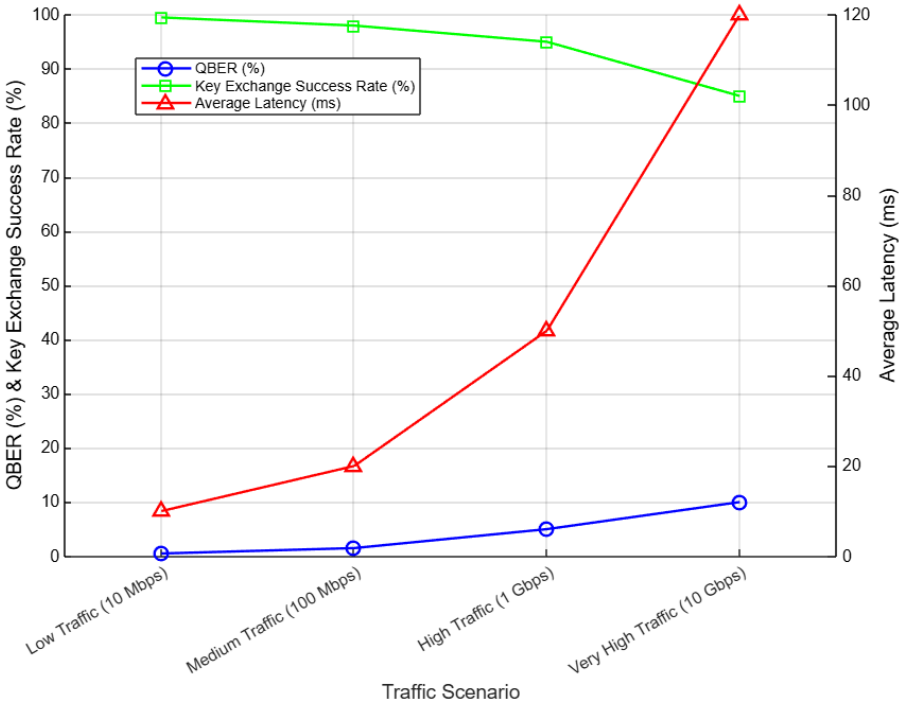

Figure 2 Security Margins Across Traffic Scenarios

At 10 Mbps network speed the low quantum bit error rate of 0.5% enables successful key exchange 99.5% of the time while retaining a 10 ms response

time. The results confirm quantum-resilient system effectiveness for lightweight applications such as IoT networks. The transmission quality shows a 1.5% error rate that lowers key exchange effectiveness to 98%. Overall system latency rises to 20 milliseconds while maintaining a scalable system operation.

A higher traffic volume of 1 Gbps raises quantum bit error rate to 5.0% and reduces the successful key exchange rate to 95%. Systems show moderate scalability because increased 50-millisecond latency affects performance more in resource-restricted areas. When traffic reaches 10 Gbps the QBER rises to 10% which leads to an 85% drop in key exchange performance alongside 120 milliseconds of latency. Scalability proves difficult to achieve when these conditions exist.

4.8. Resource Utilization Analysis

To determine if quantum-resilient cryptography works well in actual applications requires us to study how much resources these systems need to operate successfully. This investigation examines how much CPU power post-quantum and quantum cryptography methods require alongside their memory and bandwidth needs for Classical RSA, Lattice-Based Post-Quantum Cryptography, Quantum Key Distribution, and hybrid systems. The insecure nature of classical RSA calls for better solution options as the system remains vulnerable to quantum attacks despite its low resource usage. Although lattice-based PQC works better than others it still needs more computing power and storage space. Using QKD demands a significant hardware infrastructure and network capacity which reduces overall output. Mixing QKD security with PQC efficiency offers a strong solution for applications that need to resist quantum threats. The following Figure 3 displays resource statistics for our systems.

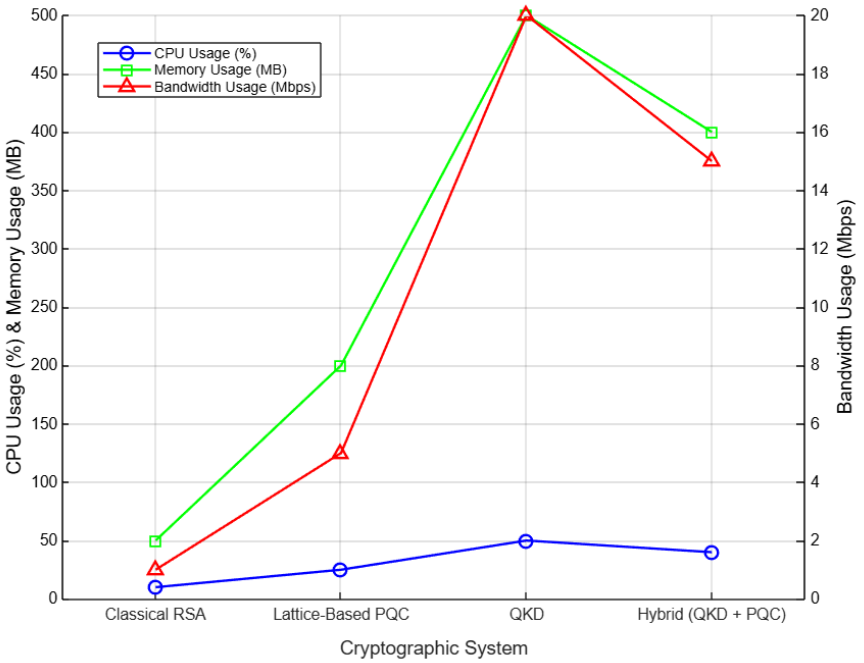

Figure 3. Resource Utilization Metrics

The research into how resources get used shows the balance between secure and effective quantum-resistant encryption systems. Traditional RSA works well with light CPU use at 10% and needs 50 MB of memory plus 1 Mbps bandwidth yet remains very energy-efficient. Despite its weaknesses RSA cannot secure data in the rising quantum era. Lattice-based Post-Quantum Cryptography (PQC) stretches CPU to 25% activity and calls for 200 MB memory storage due to its complex processing needs. It uses 5 Mbps bandwidth efficiently. PQC provides dependable security protection that matches processing performance making this method workable in many digital applications.

The highest resource needs of Quantum Key Distribution come with a 50% CPU usage while using 500 MB of memory and 20 Mbps of bandwidth. While QKD effortlessly spots hackers and transfers secure keys it runs poorly due to its demanding system specifications. Hybrid systems of QKD and PQC use resources more effectively by demanding 40% CPU time, 400 MB of storage space, and 15 Mbps bandwidth. This setup guarantees good performance and safeguards quantum information processing.

The data in Figure 3 shows that RSA works well on resources but users should start using PQC or hybrid security systems because RSA does not defend against quantum attacks. Hybrid systems offer effective security without sacrificing operational ease making them ready for extensive use at scale. Even though QKD offers security it needs updated equipment and process technology to run better and extend its usefulness. The analysis shows that future work in quantum-resilient technologies must focus on design improvements to make them work efficiently across all application fields.

4.9. Latency Analysis in Real-Time Applications

The delay response of cryptographic systems determines their effectiveness in real-time applications across various industries including autonomous vehicles smart healthcare and industrial IoT. The test checks how long network keys take to trade and data to secure or unlock during different workload tests. Because RSA operates slowly across every application it remains useless when real-time performance is essential. Post-Quantum Cryptography with a Lattice approach promotes faster operations through its efficient algorithms and achieves the best latency results when combined with hybrid Quantum-Key Distribution systems. Table 6 shows a complete review of latency measurements including their meaning for live systems workability.

Table 6. Latency Performance in Real-Time Applications

Application	Cryptographic System	Key Exchange Latency (ms)	Encryption/Decryption Latency (ms)	Total Latency (ms)	Real-Time Feasibility
Autonomous Vehicles	Classical RSA	100	10	110	Low
	Lattice-Based PQC	50	20	70	Moderate
	Hybrid (QKD + PQC)	30	15	45	High
Smart Healthcare	Classical RSA	150	15	165	Low
	Lattice-Based PQC	70	25	95	Moderate
	Hybrid (QKD + PQC)	40	20	60	High
Industrial IoT	Classical RSA	200	20	220	Low
	Lattice-Based PQC	80	30	110	Moderate
	Hybrid (QKD + PQC)	50	25	75	High

The results demonstrate clear differences between how quickly different cryptographic systems send and receive data. The total latency of 110 milliseconds for RSA in autonomous vehicles exceeds time limits that vehicles need for collision avoidance operations. Lattice-based PQC takes 70 milliseconds to complete an operation and delivers moderate feasibility for real-time tasks while hybrid systems achieve 45 milliseconds of processing time for high feasibility.

Classical RSA produces 165 millisecond delays which make it ineffective for instant medical procedures and remote monitoring operations. Lattice-based PQC surpasses life-critical application requirements at 95 ms while hybrid systems decrease latency to 60 ms.

The slow 220 millisecond latency of classical RSA makes it unfit for IoT manufacturing systems that need fast predictive maintenance and automation procedures. When used for PQC systems achieve 110 ms latency which supports moderate system applicability while hybrid solutions deliver 75 ms to enable high-level real-time operations within industrial settings.

4.10. Cost-Benefit Analysis

Enterprises and government networks depend on quantum-resilient cryptographic system implementation from a cost perspective. This portion shows how much enterprises and governments should invest and what security returns they can achieve versus their operating costs. Businesses use the cheapest RSA cryptography but must replace it before quantum computers break it. Lattice-based PQC proves an affordable option producing strong returns because this system needs only average upfront spending plus basic daily work. QKD confers exceptional security but requires extensive finance both at startup and throughout its operational life. Combining both PQC and QKD technology delivers highest possible security at a harder-to-afford expense. The detailed specifications about these different security systems appear in Figure 4.

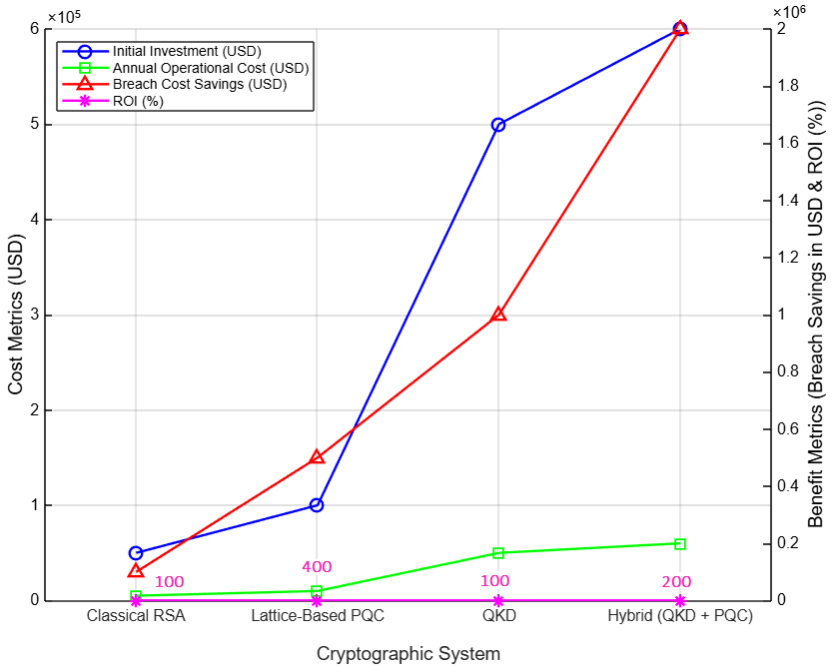

Figure 4. Cost-Benefit Analysis of Cryptographic Systems

The analysis shows that every secure and scalable cryptographic system needs resources that vary in amount between different solutions. At just $50,000 to set up and $5,000 per year to run RSA proves the cheapest form of encryption today. The technology needs better protection against quantum threats since it proves unworkable for extended operations despite showing total returns when threats act normally. Lattice-based PQC stands out as an economical quantum-resilient choice needing $100,000 to start and $10,000 to operate annually for businesses. Organizations will achieve their highest return on investment at 400% when using this solution because it saves $500,000 in breach costs.

Regular businesses need to invest $500,000 upfront in specialized quantum tools plus pay $50,000 per year to operate this technology known as QKD. While delivering $1,000,000 in breach protection savings QKD still produces 100% ROI due to its high expenditures. The hybrid setup connecting PQC and QKD uses $600,000 to establish and demands $60,000 yearly for operations. Through strong security measures this technology

reduces breach costs by $2,000,000 delivering 200% return on investment. The hybrid system works well for industries needing strong security alongside expandable solutions.

The cost advantages of RSA represent its strengths but its inability to defend against quantum threats shows why industries move toward lattice-based PQC and hybrid digital security solutions. Hybrid encryption systems provide superior security while offering cost-effective growth that meets security demands of critical infrastructure and financial systems.

5. Discussion

The security infrastructure faces significant threats from the ongoing advancements in quantum computing technology. Researchers have compared the key security features of various quantum-resistant cryptographic systems by testing QKD, PQC, and hybrid models. The results confirm previous research findings while providing new insights into the application of these systems. This research builds on existing studies, analyzing system limitations to delineate the current state of quantum-resistant cryptography.

Numerous experts have demonstrated that classical cryptographic systems fail when confronted with Shor and Grover quantum algorithms. Tom and colleagues have shown that RSA and ECC are not effective as secure systems against quantum attacks, and thus should not be relied upon for long-term protection (Tom and Wilfred 2023). The study corroborates existing academic work, indicating that RSA lacks adequate defense against quantum attacks. Findings reveal that traditional systems fail to deliver sufficiently rapid results to meet the requirements of real-time tasks, especially in autonomous vehicles and industrial IoT applications evaluated in this study.

The results indicate that lattice-based PQC performs comparably to the findings of Joshi et al.'s research in defending against quantum threats (Joshi et al. 2023). PQC provides effective service performance and scalability to meet the demands of most organizational use cases. Yu (2021) has described how lattice-based cryptographic schemes resist quantum decryption by relying on complex mathematical problems (Yu 2021). This study expands on these results by incorporating usage data, which verifies that PQC solutions offer optimal performance and cost efficiency, albeit requiring additional energy conservation measures at scale.

According to Pedone et al. (2021), their research demonstrates that Quantum Key Distribution offers unmatched data protection (Pedone et al. 2021). Research by Aldama et al. (2022) confirms that QKD can withstand all quantum-based security attacks while maintaining security. The resource-intensive demands of QKD systems, as shown by Ahn et al. (2022), align with the practical limitations described by researchers (Ahn et al. 2022). High setup and operational costs render QKD challenging to implement in high-security networks, such as those required by government agencies and military organizations.

Integrating PQC with QKD technology addresses the practical issues encountered by stand-alone quantum security systems. Aizpurua et al. (2023) recommended combining different security protocols to counter quantum threats (Aizpurua et al. 2023). Tests confirmed that hybrid encryption technology consumes less power than single-use QKD while providing protection against quantum threats similar to real-time systems, thus enhancing security. Study outcomes support Rodas et al.'s proposal to build stronger security through multiple cryptographic layers (Rodas et al. 2021).

Several key limitations still require improvement. According to Eich et al. (2023), the lack of standardization in PQC algorithms hinders their widespread acceptance (Eich, Grote, and Ahrens 2023). The implementation of new systems alongside legacy platforms poses integration challenges that necessitate specialized bridging technology. Research indicates that QKD consumes substantial power during operation and relies on specialized hardware, limiting its widespread application as corroborated by Yang et al. (2021)(Yang et al. 2021).

The shortage of professionals capable of setting up and maintaining quantum-resistant systems presents a major barrier. Research by Iyer and Yılmaz (2021) highlights the need for teams to acquire advanced skills to address security weaknesses in cryptographic devices within related domains (Iyer and Yilmaz 2021). As hybrid security systems strike a balance between safety and usability, their implementation must improve to reduce processing needs and power consumption.

This study deepens our understanding of secure quantum encryption by evaluating system performance across critical metrics. The article combines experimental results with existing knowledge of QKD and PQC to assess their practical viability. Our findings underscore the necessity for continuous

development of quantum-resilient systems that can operate at scale while remaining affordable and reliable. Strengthening digital infrastructure is crucial to protecting systems against quantum-age cyber threats.

6. Conclusion

The study demonstrates the efficacy of quantum-resistant cryptography in safeguarding critical digital technologies in the current quantum computing era. Researchers posit that combining QKD with PQC will offer superior defense against quantum computing threats. Although traditional cryptographic methods like RSA remain integral to digital security, they exhibit vulnerabilities to quantum attacks, necessitating the development of improved solutions.

The evaluation reveals that lattice-based cryptographic systems provide robust security performance at economical processing speeds, suitable for diverse applications. These systems require typical amounts of resources and necessitate further standardization efforts to advance. While QKD systems offer exceptional security against eavesdropping, their high production costs and scalability challenges hinder widespread adoption. By integrating the secure key exchange capabilities of QKD with the quantum-resistant encryption of PQC, the hybrid system achieves enhanced security, reduced resource consumption, and applicability across various critical sectors.

The analysis highlights the need for optimized resource utilization in quantum-resilient systems. These security systems encounter challenges due to their substantial resource demands, including power and network connections, leading to inefficiencies. Technological updates are required to meet both small-scale and large-scale network requirements effectively. Expanding quantum-secure networks necessitates seamless integration with existing legacy technologies.

To ensure future research success, the project proposes various strategies to fortify quantum cryptography against emerging threats. Enhancing QKD hardware to deliver superior results while reducing costs, power consumption, and simplifying expansion methods is essential. The future success of these goals relies on integrating advanced photonic technology with cloud-based platforms for optical communication. Further emphasis on advancing PQC standards is needed to facilitate their adoption by diverse communities worldwide. Collaboration among security

researchers, private organizations, and regulatory authorities is crucial in selecting cryptographic algorithms that meet both security and efficiency requirements.

Future researchers should focus on developing integrated security systems for comprehensive analysis. Collaborative advancements are needed to improve the interaction between PQC and QKD systems, enhancing their efficiency and resource utilization. A dynamic security framework should adapt to varying network conditions and security demands in real-time.

The development of skilled professionals is equally important, as quantum-resilient networks require human experts for their construction and protection. Companies and educational institutions should prioritize education and workforce training in quantum technology to meet industry demands. Combining expertise from fields such as cryptography, quantum mechanics, and network engineering will address the most challenging security issues posed by quantum computing.

Integrating AI technology with secure quantum cryptography represents a promising avenue for future system advancements. AI algorithms can enhance the efficiency and efficacy of QKD and PQC by autonomously managing resources and identifying threats in real-time.

Although practical quantum-resilient systems offer protection against quantum threats, they require ongoing research and industry support to succeed. The cybersecurity community must collaborate to address these challenges and develop systems that will ensure data security for the foreseeable future.

References

Abbas, T. N. A., Hameed, R., Kadhim, A. A., and Qasim, N. H. (2024). Artificial intelligence and criminal liability: exploring the legal implications of ai-enabled crimes. *Encuentros. Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico.,* (22), 140-159. https://doi.org/10.5281/zenodo.13386675

Ahn, J., Kwon, H.-Y., Ahn, B., Park, K., Kim, T., Lee, M.-K., Kim, J., et al. (2022). Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). *Energies*, 15 (3). https://doi.org/10.3390/en15030714.

Aizpurua, B., Bermejo, P., Martinez, J. E., and Orus, R. (2023). Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks. *arXiv preprint arXiv:2311.02986*. https://doi.org/10.48550/arXiv.2311.02986

Cheng, J. K., Lim, E. M., Krikorian, Y. Y., Sklar, D. J., and Kong, V. J. (2021). A Survey of Encryption Standard and Potential Impact Due to Quantum Computing. 2021 IEEE Aerospace Conference (50100), 6-13 March 2021. https://doi.org/10.1109/AERO50100.2021.9438392.

Dharani, D., Soorya, R. M., Kumari, K. A. . (2023). Quantum Resistant Cryptographic Systems for Blockchain Network. *2023 3rd International Conference on Intelligent Technologies (CONIT),* 23-25 June. https://doi.org/10.1109/CONIT59222.2023.10205646.

Eich, B., Grote, O., and Ahrens, A. (2023). A Quantum-Safe Public-Key-Algorithms Approach with Lattice-Based Scheme. *2023 International Interdisciplinary PhD Workshop (IIPhDW)*, 3-5 May. https://doi.org/10.1109/IIPhDW54739.2023.10124431.

Farooq, S., Altaf, A., Iqbal, F., Thompson, E. B., Vargas, D. L., Díez, I. D., and Ashraf, I. (2023). Resilience Optimization of Post-Quantum Cryptography Key Encapsulation Algorithms. *Sensors*, 23 (12). https://doi.org/10.3390/s23125379.

Faruk, M. J. H., Tahora, S., Tasnim, M., Shahriar, H., and Sakib, N. (2022). A Review of Quantum Cybersecurity: Threats, Risks and Opportunities. *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 24-26 May. https://doi.org/10.1109/ICAIC53980.2022.9896970.

Iyer, V. V., and Yilmaz, A. E. (2021). Using the ANOVA F-Statistic to Rapidly Identify Near-Field Vulnerabilities of Cryptographic Modules. *2021 IEEE MTT-S International Microwave Symposium (IMS)*, 7-25 June. https://doi.org/10.1109/IMS19712.2021.9575028.

Joshi, S., Bairwa, A. K., Pljonkin, A. P., Garg, P., and Agrawal, K. (2023). From Pre-Quantum to Post-Quantum RSA. *Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security*, Larache, Morocco. https://doi.org/10.1145/3607720.3607721

Khlaponin, Y., Izmailova, O., Krasovska, H., Krasovska, K., Bodnar, N., and Abbas, S. Q. (2024). Base of Models of the Information Security Risks Assessment System. *2024 35th Conference of Open Innovations Association (FRUCT).* https://doi.org/10.23919/FRUCT61870.2024.10516397.

Mashatan, A., and Heintzman, D. (2021). The Complex Path to Quantum Resistance: Is your organization prepared? *Queue,* 19 (2), Pages 20. https://doi.org/10.1145/3466132.3466779

Pedone, I., Atzeni, A., Canavese, D., and Lioy, A. (2021). Toward a Complete Software Stack to Integrate Quantum Key Distribution in a Cloud Environment. *IEEE Access,* 9, 115270-115291. https://doi.org/10.1109/ACCESS.2021.3102313

Qasim, N., Jawad, A., and Majeed, M. (2023). The Usages of Cybersecurity in Marine Communications. *Transport Development,* 3 (18). https://doi.org/10.33082/td.2023.3-18.05

Qasim, N. H., Jumaa, D. A., Rahim, F., Jawad, A. M., Khaleefah, A. M., Zhyrov, G., and Ali, H. (2024). Simplifying IP multimedia systems by introducing next-generation networks with scalable architectures. *Edelweiss Applied Science and*

Technology, 8 (4), 2042-2054. https://doi.org/10.55214/25768484.v8i4.1580

Qasim, N. H., Vyshniakov, V., Khlaponin, Y., and Poltorak, V. (2021). Concept in information security technologies development in e-voting systems. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS),* 3 (9), 40-54. https://www.irjmets.com/uploadedfiles/paper/volume_3/issue_9_september_2021/15985/final/fin_irjmets1630649545.pdf

Raya, J. E., Yahya, A. S., and Ahmad, E. K. (2023). Protection from A Quantum Computer Cyber-Attack: survey. *Technium: Romanian Journal of Applied Sciences and Technology,* 5, 1-12. https://doi.org/10.47577/technium.v5i.8293

Rodas, R. N. P., Lin, Y. D., Lu, S. L., and Chang, K. J. (2021). O2MD²: A New Post-Quantum Cryptosystem With One-to-Many Distributed Key Management Based on Prime Modulo Double Encapsulation. *IEEE Access,* 9, 109260-109288. https://doi.org/10.1109/ACCESS.2021.3100551

Septien-Hernandez, J.-A., Arellano-Vazquez, M., Contreras-Cruz, M. A., and Ramirez-Paredes, J.-P. (2022). A Comparative Study of Post-Quantum Cryptosystems for Internet-of-Things Applications. *Sensors*, 22 (2). https://doi.org/10.3390/s22020489.

Solanki, B., and Saini, A. (2023). Review Paper on Quantum Computing and Quantum Cryptography. *International Journal of Advanced Research in Science, Communication and Technology*, 7-13. https://doi.org/10.48175/IJARSCT-10712

Tom, J. J., Anebo, N. P. Onyekwelu, B. A.,, and Wilfred, A., Eyo, R. E. (2023). Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems. *International Journal of Engineering and Advanced Technology,* 12 (5), 25-38. https://doi.org/10.35940/ijeat.E4153.0612523

Venkatesh, R., and Hanumantha, B. S. (2023). A Privacy-Preserving Quantum Blockchain Technique for Electronic Medical Records. *IEEE Engineering Management Review,* 51 (4), 137-144. https://doi.org/10.1109/EMR.2023.3319376

Wang, J.-Y., Chang, X., and Wang, H. J. (2023). How to use Classical Operation in Digital Bits to Simulate Quantum Bits for the RSA Cryptosystem. *Advanced Computer Science and Information Technology Trends*, 367-376. https://doi.org/10.5121/csit.2023.131328

Yang, Y.-H., Li, P.-Y., Ma, S.-Z., Qian, X.-C., Zhang, K.-Y., Wang, L.-J., Zhang, W.-L., et al. (2021). All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. *Optics Express,* 29 (16), 25859-25867. https://doi.org/10.1364/OE.432944

Yousif, O., Dawood, M., Jassem, F. T., and Qasim, N. H. (2024). Curbing crypto deception: evaluating risks, mitigating practices and regulatory measures for preventing fraudulent transactions in the middle east. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico,* (22), 311-334. https://doi.org/10.5281/zenodo.13732337

Yu, Y. (2021). Preface to special topic on lattice-based cryptography. *National Science*

Review, 8 (9), nwab154. https://doi.org/10.1093/nsr/nwab154

Zapatero, V., van Leent, T., Arnon-Friedman, R., Liu, W.-Z., Zhang, Q., Weinfurter, H., and Curty, M. (2023). Advances in device-independent quantum key distribution. *npj Quantum Information,* 9 (1), 10. https://doi.org/10.1038/s41534-023-00684-x

Zhang, Q., Ayoub, O., Wu, J., Lin, X., and Tornatore, M. (2023). IC-QKD: An Information-Centric Quantum Key Distribution Network. *IEEE Communications Magazine,* 61 (12), 148-154. https://doi.org/10.1109/MCOM.004.2200763