SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V13I6P102

Volume 13 Issue 6, 12-20, June 2026

Original Article

Comparative Analysis of Existing Quantum Security Algorithms: PQC and QKD Protocols

Rashmi Kuksal[1], Sumit Chaudhary[2], Ashish Bhatt[3]

[1,2,3]*Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India.*

[1]*Corresponding Author : rashmikuksal@gmail.com*

Received: 24 April 2026 Revised: 27 May 2026 Accepted: 11 June 2026 Published: 28 June 2026

Abstract *- Quantum computing poses a challenge as well as an unprecedented opportunity to current cryptography. The algorithm by Shor and Grover shows that popular classical cryptosystems, including Rivest-Shamir- Adleman (RSA) and Elliptic Curve Cryptography (ECC), are susceptible to a quantum attack, and quantum-safe security designs should be created. The paper gives a comparative analysis of the current quantum security algorithms, including Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). Their trade-offs in working, their strengths, weaknesses, performance, and practical considerations are analyzed. Based on the comparative analysis provided below, hybrid cryptographic systems, in turn, a combination of PQC algorithm and QKD protocol, may be considered a good opportunity to make communication systems secure in the post-quantum era. The findings underline that PQC can be deployed practically in an already existing communication network environment, yet QKD is only subject to unconditional security, but needs dedicated quantum hardware and communication systems.*

Keywords *- BB84 Protocol, Post-Quantum Cryptography, Quantum Key Distribution, Quantum Security, Lattice-based Cryptography, Shor's Algorithm.*

1. Introduction

The expeditious development of quantum computing has created severe worries about the security of modern communication systems. Classical cryptographic algorithms depend on algorithmic intractability hypotheses, such as Integer Factorization (RSA) or Discrete Logarithms (ECC)[1]. However, quantum algorithms such as Shor's algorithm and Grover's search algorithm can efficiently break these assumptions. Consequently, researchers have focused on designing cryptographic algorithms that can withstand quantum attacks, collectively known as Post-Quantum Cryptography, as well as physical approaches like Quantum Key Distribution [2].

The National Institute of Standards and Technology (NIST) has led a multi-year standardization effort that has selected lattice-based schemes such as CRYSTALS-Kyber and CRYSTALS-Dilithium for broad adoption. QKD, in contrast, achieves information-theoretic security for key exchange by exploiting physical properties of quantum systems, such as no-cloning theorem and the disturbance introduced by measurement, rather than relying on unproven computational assumptions.

Although PQC and QKD have received substantial individual attention in the literature, fewer studies systematically compare the two paradigms with respect to deployment feasibility, computational and infrastructural overhead, and resistance to emerging cryptanalysis. This gap leaves practitioners with limited guidance on how the approaches might be combined within a single security architecture rather than evaluated in isolation.

The present paper addresses this gap by providing a structured comparative analysis of PQC and QKD, examining the underlying mathematical and physical security assumptions, key-size and performance trade-offs, and practical deployment constraints of each approach, and by identifying the conditions under which a hybrid PQC-QKD architecture may offer the strongest available defense against quantum-enabled attacks.

2. Methods

2.1. Post-Quantum Cryptography (PQC)

PQC algorithms are practical on classical hardware and are made to withstand breaches from both classical and quantum attackers [3-5]. The PQC standardization process has been overseen by the National Institute of Standards and Technology (NIST), which has chosen hash-based and lattice-based algorithms for implementation. Below, we discuss the main families of PQC.

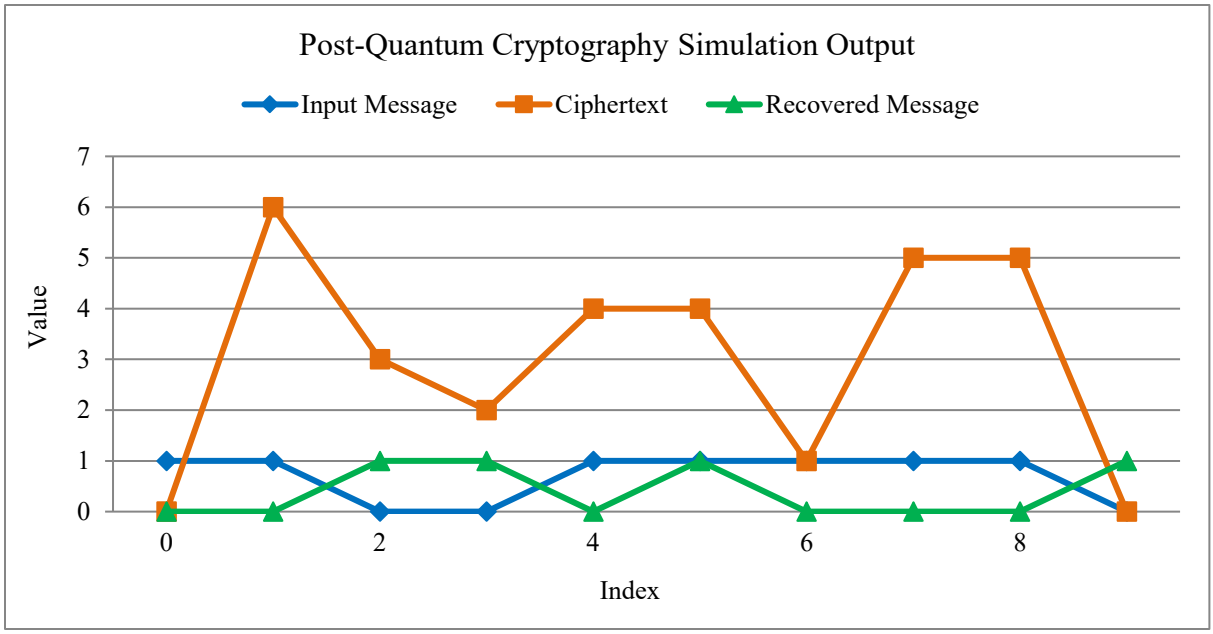

Fig. 1 Conceptual workflow of a system for post-quantum cryptography

Figure 1 displays the simulation results of the post-quantum cryptography system. The simulation results show the input message, the encrypted ciphertext, and the recovered message at different indices. The input message is represented as a binary sequence, whereas the ciphertext shows much larger and non-uniform values due to the addition of noise and complex modifications typical of post-quantum encryption schemes [6-8]. This behavior suggests a resistance to both classical and quantum cryptanalytic attacks. The extracted message is very much similar to the original input, therefore assuring the precision and dependability of the decryption process [9-10]. In a nutshell, the figure illustrates the basic PQC property of turning simple input data into computationally hard ciphertexts and also ensures accurate and safe recovery at the receiver end.

Fig. 2 Block diagram of a post-quantum cryptography system

Figure 2 presents the workflow of a Post-Quantum Cryptography (PQC) system. The process begins with the generation of public parameters and cryptographic keys. A controlled noise component is incorporated during the encryption stage, which forms the basis of several PQC schemes and contributes to their resistance against both standard and quantum attacks. The input message is represented as a binary sequence and is subsequently encrypted using the generated keys and noise parameters. During decryption, the corresponding secret key is applied to recover the original message. As shown in the figure, the recovered message matches the input message, demonstrating the correctness of the encryption – decryption process. The figure illustrates the fundamental stages involved in a PQC framework, including key generation, noise incorporation, encryption, and message recovery.

2.2. Lattice-based Cryptography

CRYSTALS-Kyber and CRYSTALS-Dilithium (signatures) are the most promising ones. They are grounded on the difficulty of the Learning with Errors shortcomings, and there are powerful security guarantees.

Figure 3 represents the performance of a lattice-based post-quantum cryptography system, which is a Learning With Errors (LWE) model. The input message has been represented as a binary sequence, and the value associated with the ciphertext is significantly higher and not uniform as a result of the intentional insertion of lattice noise in the encryption mechanism [11-13]. This distortion is an example of the security aspect of the scheme, as the ciphertext will not reveal the form of the original message.

The decryption operation is able to retrieve the original binary message with very good precision, even in the presence of noise, as can be seen by the fact that the overlap between the input message plot and the recovered message plot is very great. The results assure that the mechanism of lattice-based encryption is right and strong, highlighting its suitability to secure communication in a post-quantum setting.

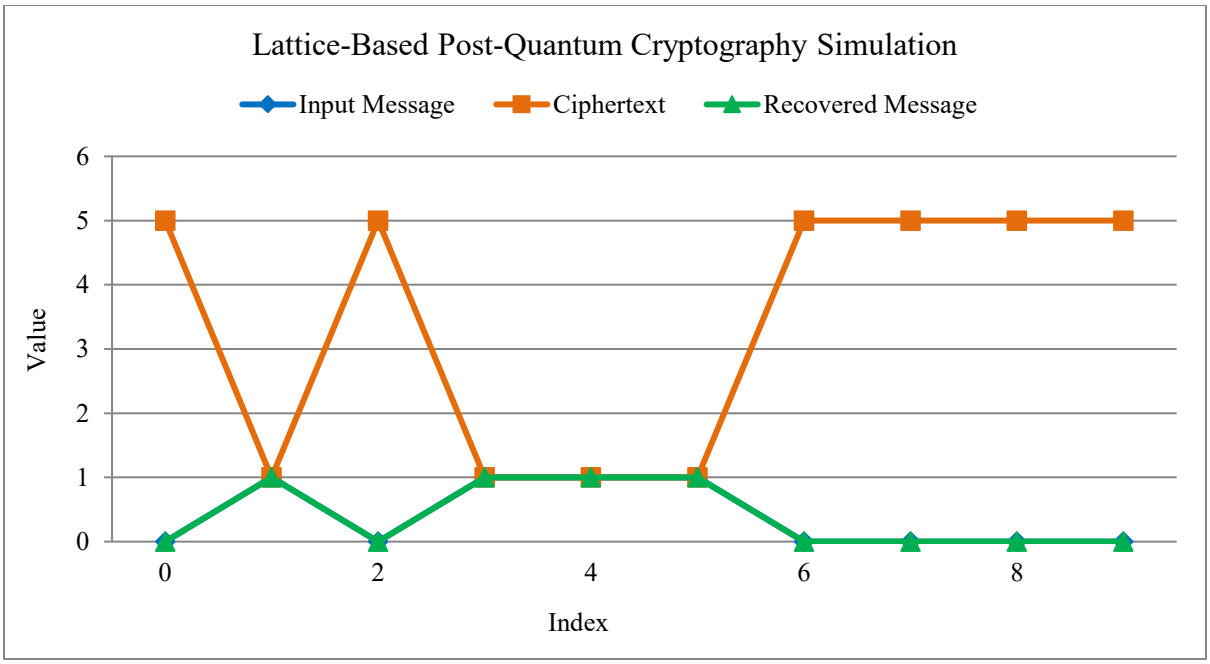

Fig. 3 Noisy lattice-based secure encryption and reliable decryption

2.3. Code-based Cryptography

Classic McEliece has recourse to the hardness of decoding random linear codes. It possesses huge public keys yet established security [14-15].

As mentioned in Figure 4, the performance of a code-based post-quantum cryptography method [16]. The process of enciphering purposefully distorts the encrypted message and is unscholarly in the process of producing a distorted ciphertext. This careful sound, even if the decoding process will correctly reconstruct the original message. This shows the self-correcting capabilities and the trustworthiness of the cryptosystem that includes a code. The results ensure the safety and accuracy of the scheme.

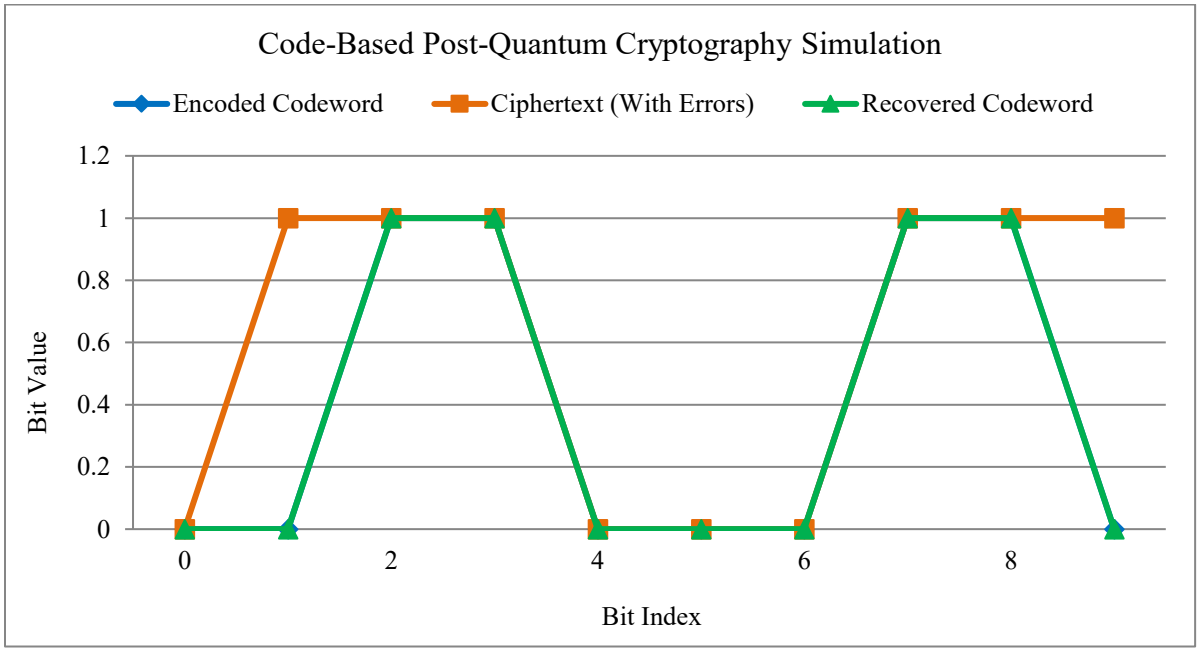

Fig. 4 Post-quantum encryption and decryption performance in code

2.4. Hash-based Cryptography

SPHINCS+ is a stateless hash-based signature protocol offering strong security assuming only hash function strength[13].

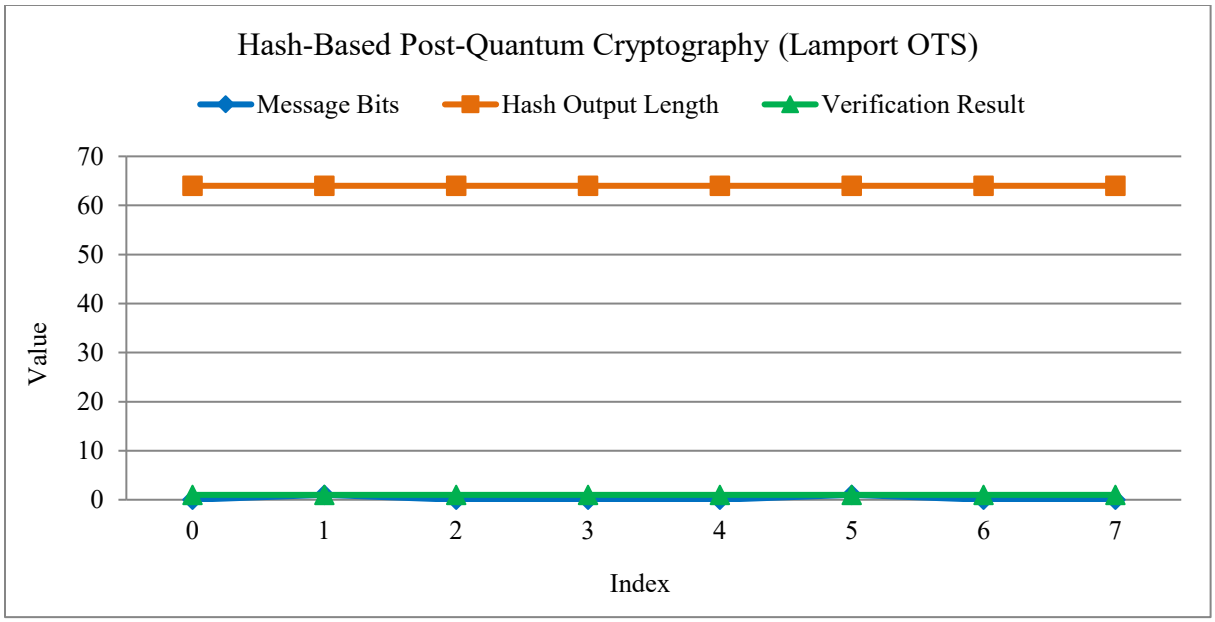

Fig. 5 Secure signing of messages in a hash-based cryptographic system

Figure 5 depicts how well a hash-based post-quantum cryptographic scheme performs when employing the Lamport One-Time Signature (OTS)[14-15]. Using fixed-length hash outputs, the binary message bits are signed, illustrating the constant-size and deterministic characteristics of cryptographic hashing. The successful verification of all indices confirms the integrity, authenticity, and reliability of the hash-based signature mechanism.

2.5. Multivariate Cryptography

Relies on solving systems of multivariate quadratic equations. Rainbow was a candidate but has been broken by attacks[16].

The Figure 6 depicts the behavior of a multivariate post-quantum cryptographic scheme that is based on evaluating quadratic polynomials over a finite field.

The signature and message vectors are shown as elements modulo q, whereas the verification value is obtained from evaluating the multivariate quadratic function.

The uniformity of the verification output validates the accuracy and structural integrity of the multivariate signature mechanism.

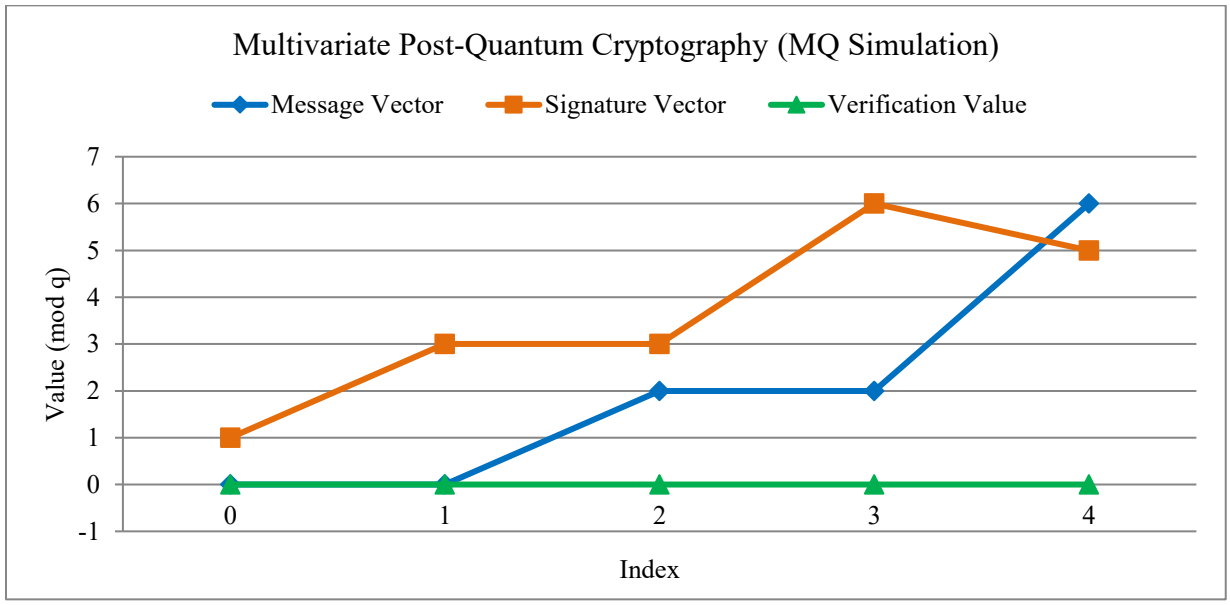

Fig. 6 Efficiency of a multivariate quadratic (MQ) post-quantum scheme

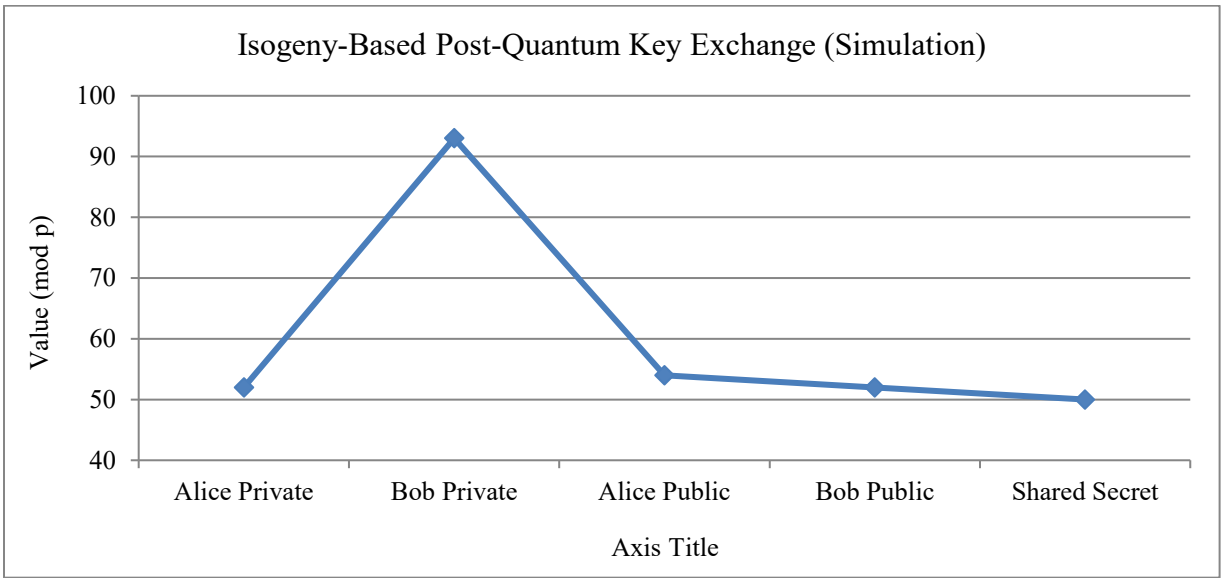

Fig. 7 Isogeny-oriented key exchange demonstrating precise shared secret computation

2.6. Isogeny-based Cryptography

Schemes like SIKE offered very small key sizes, but recent attacks have made them insecure[17].

An isogeny-based simulated key exchange procedure intended for the post-quantum era is shown in Figure 7. The same shared secret is calculated by both parties modulo p, and independent private keys produce equivalent public parameters.

The agreement of the shared secret validates the accuracy and consistency of the isogeny-based key establishment technique.

3. Quantum Key Distribution (QKD)

In contrast to PQC, QKD offers information-theoretic safe key exchange by utilizing quantum mechanics. To identify eavesdropping attempts, protocols like BB84 and E91 use concepts like superposition and entanglement. Despite its potential, QKD has drawbacks, including integration, cost, and distance restrictions.

3.1. BB84 Protocol

Encoding qubits in non-orthogonal states is the foundation of the first and most extensively researched QKD protocol.

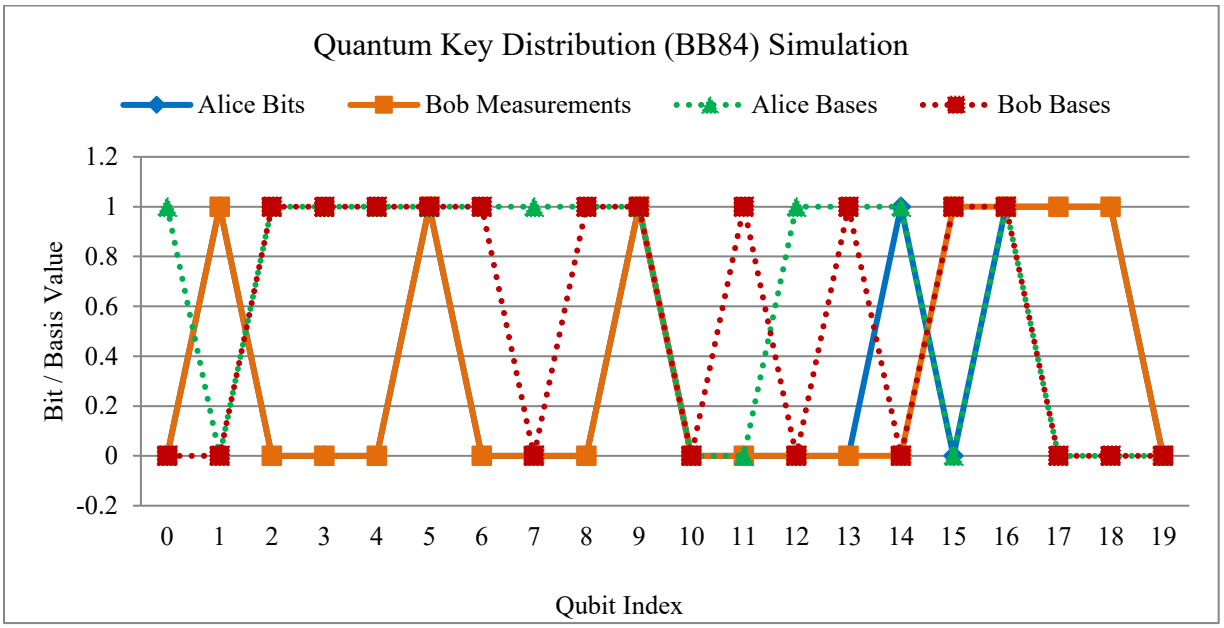

Fig. 8 Results of the BB84 QKD simulation

The simulated BB84 Quantum Key Distribution (QKD) procedure is shown in Figure 8, along with Bob's measurement results and randomly selected bases, as well as Alice's qubit bits and bases. Alice's and Bob's successful key generation instances are determined by the alignment of their bases. The measured bits coincide and form the sifted key when both parties select the same bases; otherwise, the results are discarded. The simulation illustrates the probabilistic nature of quantum measurement and the basis-dependent behavior that is fundamental to QKD security.

3.2. E91 Protocol

An entanglement-based scheme provides stronger theoretical security guarantees.

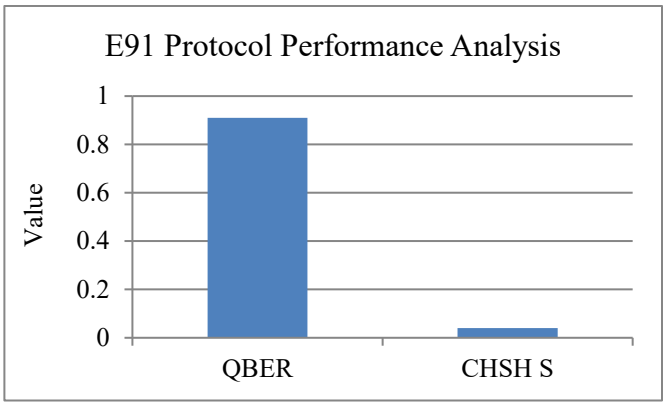

Fig. 9 E91 protocol performance analysis (QBER and CHSH Parameter)

The CHSH Bell parameter and QBER performance of the E91 protocol are shown in the figure 9. While the Bell parameter surpassing the classical limit(S>2) verifies entanglement and guarantees protocol security, the low QBER suggests few transmission failures.

4. Mathematical Analysis of Quantum Security Algorithms

In this part, we will evaluate the computational complexity, security assumptions, key sizes, and practical performance characteristics of important quantum-safe cryptographic techniques. The emphasis is on understanding the mathematical aspects that affect security and implementation efficiency, rather than on giving individual algorithmic equations.

4.1. Security Assumptions

Various quantum-secure algorithms obtain their security from unique, complex mathematical issues. The foundation of lattice-based cryptography is the Shortest Vector Problem and Learning with Errors, both of which are thought to be computationally impossible even for quantum computers. Code-Based Cryptography secures itself through the challenge of deciphering random linear error-correcting codes. Hash-Based Cryptography leverages the collision resilience and preimage resilience characteristics of cryptographic hash functions. The difficulty of solving systems of multivariate quadratic equations is exploited by multidimensional cryptography. The challenge of identifying isogenies amongst supersingular elliptic curves is used in isogeny-based cryptography. Quantum Key Distribution (QKD) obtains its security from quantum mechanical principles, including the no-copy theorem and measurement disturbance. PQC security is based on computational complexity - an attacker is unable to reverse the function effectively even with quantum algorithms.

Given y=f(x), find x is computationally infeasible, represented as equation (1)

$$y = f(x) \tag{1}$$

4.2. Computational Complexity Comparison

The computational demands of the examined methodologies vary considerably. Lattice-based approaches are capable of efficient key generation and encryption, which is suitable for practical implementation. Code-based solutions provide strong security but require much bigger public keys. Hash-based signatures offer strong security guarantees but are restricted to use as digital signatures. Multivariate methods allow for quick signature generation. Isogeny-based schemes have small key sizes but require high computational cost. Quantum Key Distribution requires dedicated infrastructure for quantum communication.

Here, we extract secret vectors which are given by the following equation (2). The problem of noisy linear equations is the Learning With Errors (LWE) problem.

$$b = As + e(modq) \tag{2}$$

4.3. Key Size and Scalability Analysis

Storage requirements and transmission overhead directly depend on the size of the key. Lattice-based systems tend to require moderate key sizes, whereas code-based approaches require substantially bigger public keys. Hash based and Multivariate systems are in the middle. Isogeny-based cryptography offers the smallest key sizes among post-quantum candidates, but recent cryptanalytic advances have eroded confidence in its security. As shown in equation (3), the encoding of a random error vector and its decoding. The security is based on the difficulty of mistake-correction decoding. It offers extremely high levels of security, yet the keys are extremely large when compared to lattice systems.

$$c = mG + e \ , \ s = HcT \tag{3}$$

4.4. Security Evaluation against Quantum Attacks

The resilience of each method against quantum assaults might be evaluated based on presently recognized algorithms: Shor's algorithm poses a significant threat to conventional RSA and ECC systems.

Lattice-based, code-based, and hash-based systems currently exhibit no known polynomial-time quantum vulnerabilities. Multivariate methods continue to withstand established quantum attacks; however, certain architectures have been compromised via classical cryptanalysis. Numerous isogeny-based strategies have been undermined by recent assaults, diminishing their practical feasibility. Quantum Key Distribution (QKD) offers information-theoretic security when executed properly. The security is only assured by the hash collision resistance. Quantum computers do not attack any algebraic structure besides the search (offering only quadratic speedup) by Grover. Therefore, very trusty but mostly restricted to digital signatures and verified as in equation (4).

$$y = H(x)\,, H(m) = yi \tag{4}$$

4.5. Comparative Discussion

The analysis shows that lattice-based cryptography has the best symmetry between security, efficiency, and ease of implementation, and hence has been incorporated into the NIST post-quantum cryptography guidelines. Code-based systems have strong security in the long run, but are typified by large key sizes. Hash-based signatures have good security but are designed for certain purposes. Multivariate and Isogeny-based techniques have interesting properties, but are not practical and have security problems. Quantum Key Distribution (QKD) provides strong theoretical security guarantees but requires specialized quantum communication infrastructure, limiting its wide deployment.

The comparison demonstrates that there is no single quantum-security mechanism that is always better, but the decision is application-dependent, considering the processor power, communication constraints, and security goals.

$$Pi(x1, \dots, xn) = \sum aijkxjxk + \sum bijxj + ci \tag{5}$$

The NP-hard problem of solving systems of nonlinear polynomial equations is essential to security. Larger keys and certain structural attacks undermine confidence, but fast signatures do the same as equation (5).

4.6. Security and Complexity Analysis Isogeny-Based Cryptography

Isogeny-based encryption secures itself through the computational challenge of identifying isogenies amongst supersingular elliptic curves. A primary advantage is the utilization of tiny key sizes in comparison to alternative post-quantum cryptography methods. Nonetheless, the computational expense linked to isogeny computations is considerably more than that of lattice-based and code-based approaches.

Elliptic Curve: $E: y2 = x3 + ax + b$
Isogeny mapping: $\phi: E1 \rightarrow E2$

Shared secret: $j(E_{AB}) = j(E_{BA})$ (6)

Finding the concealed curve mapping, or isogeny, is essential to security. Although it has the smallest key sizes, its practical confidence is lower, and its calculation complexity is considerable from the above equation (6). Despite initial optimism regarding isogeny-based approaches as viable alternatives for post-quantum security, recent cryptanalytic attacks have diminished trust in their long-term feasibility.

Consequently, despite their communication efficiency, their practical implementation is constrained in comparison to NIST-standardized lattice-based algorithms. The analysis shows that the isogeny-based cryptography delivers better key-size economy, but suffers from the challenges in terms of computational overhead and security assurances.

4.7. Performance analysis of Quantum Key Distribution

It is important to note that QKD is fundamentally different from the post-quantum cryptography methods discussed above, in that its security is based on the fundamentals of quantum mechanics rather than assumptions about the difficulty of computing. The effectiveness of a QKD system is usually measured by the Quantum Bit Error Rate(QBER), which is the reliability of the dispatched quantum states.

Key error rate: $QBER = \frac{error\ bits}{total\ bits}$

Secret key rate: $R = 1 - 2H(QBER)$ (7)

Security is set by quantum measurement disruption, not mathematics as in (7). If someone is viewing the channel, the error rate increases.

An increase in QBER could be a symptom of channel noise, hardware malfunction, or the presence of an eavesdropper. The higher the error rate is, the lower the achievable secret key rate is, which in turn reduces the effectiveness of secure communication. Hence, a low Quantum Bit Error Rate (QBER) is necessary for successful key generation. Compared to computational cryptography techniques, QKD provides stronger theoretical security guarantees. However, it requires the specific quantum communication infrastructure, which increases expense and complexity.

4.8. Comparative Analysis of BB84 Quantum Key Distribution Protocol

One of the most popular methods for distributing quantum keys is the BB84 protocol because of its conceptual simplicity and practical feasibility. Security is provided by the random selection of measurement bases. Any attempt at interception results in detectable changes to the quantum states being communicated.

Key Sifting: $Ki = \{bi, \emptyset, \theta A = \theta B, \theta A \neq \theta B$

Quantum States:
$|+\rangle = |0\rangle + |1\rangle/\sqrt{2}\ ,\ |-\rangle = |0\rangle - |1\rangle/\sqrt{2}$ (8)

The security comes from the fact that measuring on the wrong basis will disturb the photon and will indicate the presence of eavesdropping. This is expressed in equation (8). The protocol is quite robust against eavesdropping attacks and requires relatively less quantum hardware as compared to the entanglement-based protocols. However, channel losses, detector inefficiencies, and ambient noise could reduce the communication efficacy. Comparative analysis shows that BB84 provides the best compromise between security, implementation complexity, and cost; it is the most practical QKD scheme for the current real-world applications.

4.9. Comparative analysis of E91 Entanglement-Based Protocol

Entangled Bell state: $|\psi-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$
Bell inequality: $|S| \leq 2$ (classical), $|S| = 2\sqrt{2}$(quantum) (9)

Security indicated in equation (9) is confirmed by Bell inequality violations, theoretically more secure than BB84, but more difficult to implement in practice. The E91 protocol uses quantum entanglement to provide secure communication and proves security by showing violations of Bell inequalities.

E91 has better theoretical security guarantees and is more robust against sophisticated attacks than BB84. However, it needs entangled photon sources and more complicated quantum apparatus, thus increasing the complexity and cost of implementation. Consequently, E91 provides superior security; yet, it is less feasible for contemporary large-scale implementations compared to BB84.

5. Results and Discussion

5.1. Comparative Analysis

The table1 provides a comparative summary of PQC and QKD approaches in terms of key metrics such as assumptions, key size, performance, and maturity.

Table 1. Quantum and post-quantum cryptography systems are compared

Algorithm Family	Security Basis	Key/Signature Size	Performance	Maturity
Lattice-based	LWE hardness	Moderate (KBs)	Fast	NIST standardized (Kyber/Dilithium)
Code-based	Code decoding	Very Large (MBs)	Moderate	Backup candidate (McEliece)
Hash-based	Hash security	Large signatures	Moderate/slow	Standardized (SPHINCS+)
Isogeny-based	Isogenies (broken)	Small	Compromised	Not recommended
QKD	Quantum no-cloning	N/A	Hardware dependent	Experimental deployments

Table 1 compares the main families of post-quantum cryptography according to their deployment maturity, performance traits, and underlying hardness assumptions. Due to their strong security-performance trade off, lattice-based schemes that are based on LWE hardness are currently at the forefront of standardization efforts. Large key sizes are a drawback of code-based systems, notwithstanding their conservative security. Strong security proofs with a higher signature overhead are offered by hash-based signatures. Recent cryptanalytic breaks have made isogeny-based systems, which were once appealing for tiny keys, unsuitable. On the other hand, QKD offers information-theoretic security by utilizing quantum mechanical perspectives like the no-cloning theorem; nonetheless, it still requires specialized hardware and is primarily experimental.

6. Future Scope

Quantum security is an evolving field. In the near future, hybrid systems combining classical and PQC algorithms will dominate secure communications. QKD will likely see adoption in high-security sectors with dedicated infrastructure. Further research is required in quantum-resistant primitives, side-channel resistance, and integration of PQC into existing standards.

7. Conclusion

This paper presented a thorough comparative analysis of different existing quantum security algorithms. With lattice, code, and hash-based systems, post-quantum cryptography offers workable short-term solutions, but QKD offers long-term information-theoretic assurances but presents substantial implementation difficulties. Using both PQC and QKD together could provide the strongest defense against quantum threats.

Funding Statement

There was no specific grant from any governmental, private, or nonprofit funding organization to support this work.

Conflicts of Interest

The authors state that none of the work presented in this study could have been impacted by any known competing financial interests or personal relationships.

References

[1] Cédric Pilatte, *Unconditional Correctness of Recent Quantum Algorithms for Factoring and Computing Discrete Logarithms*, Forum of Mathematics, Pi, Cambridge University Press, vol. 14, pp. 1-25, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[2] Olli Ahonen, Mikko Möttönen, and Jeremy L. O'Brien, "Entanglement-Enhanced Quantum Key Distribution," *Physical Review A*, vol. 78, no. 3, pp. 1-44, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[3] Giovanni Amedeo Cirillo et al., "Advances in Molecular Quantum Computing: from Technological Modeling to Circuit Design," *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Limassol, Cyprus, pp. 132-137, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Naser Mohammadzadeh, Mehdi Sedighi, and Morteza Saheb Zamani, "Gate Location Changing: An Optimization Technique for Quantum Circuits," *International Journal of Quantum Information*, vol. 10, no. 3, pp. 1-15, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[5] Artyom M. Grigoryan, and Sos S. Agaian, "3-Qubit Circular Quantum Convolution Computation using the Fourier Transform with Illustrative Examples," *Journal of Quantum Computing*, vol. 6, no. 1, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Hiral B. Patel et al., "The Future of Quantum Computing and its Potential Applications," *Journal for Basic Sciences*, vol. 23, no. 11, pp. 513-519, 2023. [Google Scholar]

[7] Chi-Chuan Hwang, Chu-Yuan Tseng, and Cheng-Fang Su, "Quantum Circuit Design for Computer-Assisted Shor's Algorithm," *TechRxiv*, pp. 1-27, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Vaishali Bhatia, and K.R. Ramkumar, "An Efficient Quantum Computing Technique for Cracking RSA using Shor's Algorithm," *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, Greater Noida, India, pp. 89-94, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Anocha Yimsiriwattana, and Samuel J. Lomonaco Jr, "Distributed Quantum Computing: A Distributed Shor Algorithm," *Quantum Information and Computation II*, vol. 5436, pp. 360-372, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[10] Shuangcheng Jia, "Comparison of Performances for Quantum and Conventional Algorithms: Shor's Algorithm and Boson Sampling," *Highlights in Science, Engineering and Technology*, vol. 38, pp. 493-501, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Aidan Dang, Charles D. Hill, and Lloyd C.L. Hollenberg, "Optimising Matrix Product State Simulations of Shor's Algorithm," *Quantum*, vol. 3, pp. 1-9, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Andrew W. Cross et al., "Open Quantum Assembly Language," *arXiv Preprint*, pp. 1-24, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] Hoa T. Nguyen, Muhammad Usman, and Rajkumar Buyya, "iQUANTUM: A Toolkit for Modeling and Simulation of Quantum Computing Environments," *Software: Practice and Experience*, vol. 54, no. 6, pp. 1141-1171, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Daniel J. Bernstein et al., "Classic McEliece: Conservative Code-based Cryptography," *NIST Submissions*, vol. 1, no. 1, pp. 1-25, 2017. [Google Scholar]

[15] Ward Beullens, "Breaking Rainbow takes a Weekend on a Laptop," *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022*, Santa Barbara, CA, USA, vol. 13508, pp. 464-479, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Wouter Castryck, and Thomas Decru, "An Efficient Key Recovery Attack on SIDH," *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Lyon, France, vol. 14008, pp. 423-447, 2023. [CrossRef] [Google Scholar] [Publisher Link]