International Journal of Research in Advent Technology, Vol.14, No.2, June 2024
E-ISSN: 2321-9637
Available online at www.ijrat.org

Quantum-Resistant Cryptographic Protocols for Post-Quantum Secure Communications

G. Shiva Parvathi[1], P. Akhila[1], T. Harshitha[1], Y. Keerthana[1], S. Smayana[1], N. Srivalli[1]

Abstract- The development of quantum computing poses a very real threat to traditional cryptography, especially these, which are number-theoretic like RSA and ECC. With the more and more development of quantum algorithms such as Shor and Grover, there is an immediate necessity to come up with cryptographic protocols that are resistant to quantum attacks. This paper reviews and discusses different quantum-resistant (post-quantum) cryptographic schemes, such as lattice-based, code-based, multivariate, hash-based, and isogeny-based cryptography. It compares these protocols on the assumptions of their security and their efficiency in their computation and the size of their keys as well as their possible integrations into the existing communication infrastructure. Moreover, we also evaluate the standardization process by NIST and the difficulties of moving towards post-quantum security in practical use. This paper proposes a scalable comparison system, which correlates the hypothetical security basis of post-quantum cryptography with the ability to effectively operate in the real world. It has emphasized protocol interoperability, migration compatibility and trade-offs in performance that gives a viable roadmap towards quantum-resistant cryptographic protocols implementation into current communication infrastructures whilst also providing scalable and future secure communication systems. This study, by emphasizing the potential and the drawbacks of the existing post-quantum cryptography schemes, helps in a more precise idea of the directions to follow on the way to a secure, future-proof communications scheme.

Keywords: RSA, ECC, Quantum resistant cryptographic, Post quantum secure communications, open quantum safe

Manuscript received March 13, 2026; revised April 30, 2026 and published on June 30, 2026
G. Shiva Parvathi, P. Akhila, T. Harshitha, Y. Keerthana, S. Smayana, N. Srivalli
Department of IT, Mallareddy Engineering College for Women, Hyderabad, India
Email: shivaparvathiyadhav@gmail.com

I. INTRODUCTION

The idea of quantum computing is rapidly evolving whose emergence poses a face-threat to existing cryptographic systems. The class of most popular public-key encrypted algorithms, the RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman, is based on mathematical problems, e.g., integer factorization and discrete logarithms. Although these calculation problems are computationally complicated to solve on classical computers, quantum algorithms, like the Shor algorithm and the search algorithm of Grover, can be solved far more easily. Therefore, a broad range of the currently implemented cryptographic protocols can be susceptible to a quantum attack, which might jeopardize the confidentiality, integrity, and authenticity of digital messages within industries like the financial, medical, and government architecture [1].
In these problems, scholars have proposed post-quantum cryptography (PQC), or quantum-resistant cryptography. The focus of PQC is on the creation of cryptographic algorithms that cannot be compromised even when the computer has high power levels equipped with quantum computing capabilities. These algorithms are formulated on the basis of mathematical problems which are presumed to be resistant to both classical and quantum computation attacks. There are several very important categories of PQC, namely lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, hash-based signatures, and isogeny-based cryptography [2].
Of these methods, lattice-based cryptography has received much interest due to its robust theoretical security and its effective implementation. Lattice-based schemes rely on computationally-hard problems including the Learning with Errors (LWE) problem and the Shortest Vector problem (SVP) that are not solved easily by quantum computers. There are algorithm offerings of the NIST Post-Quantum Cryptography Standardization Project, including CRYSTALS-Kyber message-level encapsulation and CRYSTALS-Dilithium digital signatures, that are selected as the top candidates because they provide high security and performance is feasible [3].

10.32622/ijrat.1402202607

Code-based cryptography is another significant PQC technique, and it was first introduced with the McEliece cryptosystem. This algorithm is built on the inference of the randomized linear error correcting codes. McEliece cryptosystem still has several decades of security and is regarded as impervious to quantum attacks. Nevertheless, the significant disadvantage of this solution is that its public key is very large, which can be a limitation to its use in the resource-limited environment, like embedded systems and Internet of Things (IoT) devices [4].

Since the danger of quantum computing is on a rise, the International community has set to work and standardize quantum-resistant cryptographic solutions. Other organizations including the National Institute of Standards and Technology (NIST), are already assessing potential PQC algorithms with an aim of defining secure cryptographic standards to be used in future digital infrastructures. Strong and efficient PQC protocols should be designed to implement safe communication systems that are resistant to classical and quantum attacks in computation. Consequently, this paper examines the latest trend in post-quantum cryptography, focusing on the theoretical framework, implementation issues, as well as the necessity of quantum-era secure cryptographic systems [5].

This paper enhances the current surveys to give a common comparative model that extensively measures commanding post-quantum cryptographic protocols on security and computational efficiency, in addition to key size overhead and practical deployability. In contrast to other existing reviews which emphasize considerably on the theoretical security, this paper combines the performance benchmarking and the analysis of the compatibility with the infrastructure and outlines the migration path of the legacy systems. In addition, it critically looks at what the NIST standardization process implies to protocol selection and long term cryptographic agility. The paper synthesizes challenges in security, performance and transition to provide a single evaluative framework, to provide a useful roadmap of implementing scalable, quantum-resistant secure communication architectures.

A. Problem statement

The fast development of quantum computing poses an existential risk to classical cryptography, in which the standard number-theoretic cryptographic schemes, such as RSA and ECC, are susceptible to quantum algorithms like Short's and Grover's quantum warning numbers [6]. With the development of quantum capabilities, current communication infrastructures will become quite prone to massive compromise that compromises their dependence on cryptographic primitives that cannot resist quantum-enabled attacks. In spite of the various post-quantum cryptographic (PQC) families having been proposed (including lattice-based, code-based, hash-based, multivariate and isogeny-based) there are still considerable issues in analyzing the security assumptions in the real-life, as well as computational performance and scalability of key sizes of these schemes [7]. The incompatibility with the legacy systems is also present to current deployments, which restricts the possibility of a smooth integration into the modern communication networks [8]. Moreover, the current process of NIST standardization points to the potential and ambiguity of adoption of PQC, especially in terms of long-term resilience and vulnerabilities in implementation [9]. Thus, it is urgently needed to develop and evaluate quantum-resistant cryptographic protocol, which considerably enhances a guarantee of security and yet is efficient, scalable, or is integrated in an existing communication ecosystem.

II. LITERATURE REVIEW

Multivariate cryptography is constructed on the infeasibility of solving systems of multivariate quadratic equations in finite fields, which is an NP-hard problem [10]. Marketing schemes, Rainbow and GeMSS are examples of important advances in this field. Though first thought promising, Rainbow was eventually shattered by researchers in 2022, finding the vulnerability of the multivariate systems under some parameter options [11].

The hash based cryptographic hash functions with collision resistance offer security to hash-based digital signatures to SPHINCS+ [12]. These are schemes with powerful security guarantees, and comparably simple applications. They are however likely to create large signatures and have poor efficiency particularly in signing and verification time. However, their security bases render them desirable in some applications especially in those systems that need long term integrity.

More recent research in PQC has been on so-called isogeny-based protocols, which are based on the difficulty of isogenies between super singular elliptic curves. A candidate secure key exchange Long-term S IKE (Super singular Isogeny Key Encapsulation) recently allowed a classical cryptanalytic break [13]. This has questioned the feasibility of isogeny-based systems in post-quantum deployments, but the body of mathematics is still of interest to study.

Established in 2016, the NIST PQC project is the key to the global adoption of the quantum-safe standards of

10.32622/ijrat.1402202607

cryptographic practices. NIST chose Kyber (encryption) and Dilithium (signature) as primary candidates in its third round with SPHINCS+ as an alternative to digitally signature standardization [3]. In addition to that, other bodies including the European Telecommunications Standards Institute (ETSI) are also working on post-quantum migration planning [14]. It is no longer solely a matter of selecting safe algorithms but designing them to be incorporated into the practical systems (TLS, VPN, and IoT devices) without the need to compromise their functionality and productivity.Recent literature stresses the importance of implementing quantum resistant cryptographic protocols with the advent of the feasible quantum computing. d hash-based signatures as SPHINCS+ offer conservative security guarantees [15]. Moreover, efficiencies have suggested hybrid classics post-quantum migration frames to provide backward compatibility and cryptographic agility in large scale of communications systems [16]. Recent works the increasing significance of cryptographic protocols in securing the contemporary communication systems. Some of the emerging technologies are being combined with advanced methods of encryption, authentication and key management to provide confidentiality and integrity of data transmitted in a distributed system and the cloud environment [17], [18].

III. PROPOSED MODEL

The model is a Hybrid Post-Quantum Cryptographic Framework that has been of the proposal to offer a secure communication system that is resistant to the threats of quantum computing. As shown in figure 1 the architecture combines post-quantum key exchange, authentication of digital signature, and symmetric encryption of a session in order to guarantee secrecy, integrity, and authentication. The framework uses quantum-resistant cryptographic primitives and efficient symmetric encryption techniques to provide scalable, interoperable and future-secure communication infrastructures.

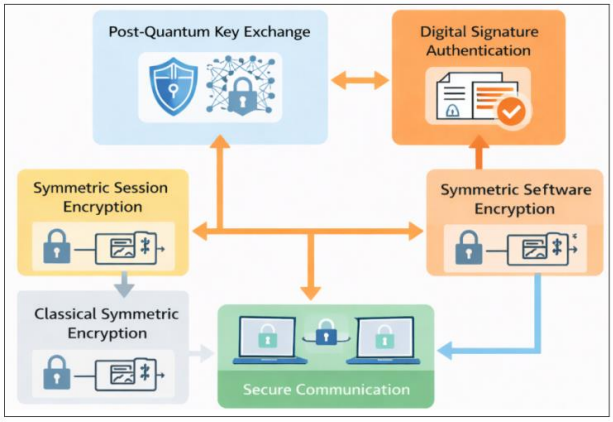

Fig.1. Proposed system model

A. Post-Quantum key Exchange

The Post-Quantum Key Exchange module provides the keyed exchange of secure session keys between communication entities in a quantum-resistant way. In contrast to a conventional RSA or ECC scheme, which could be affected by quantum attacks, this module uses lattice-based Key Encapsulation Mechanisms (KEM) that are based on the Learning With Errors (LWE) problem. The following cryptographic primitives provide a safe generation and distribution of keys even when it comes to adversaries who possess quantum computational power.

$$b = A \cdot s + e(modq) \quad (1)$$

Where
A = public matrix,
s = secret vector,
e = small error term,
q = modulus.

B. Digital Signature Authentication

The Digital Signature Authentication module ensures integrity of messages and identity verification in the transmission. It works with hash-based signature schemes, and such is invulnerable to quantum attacks since its security is based on the cryptographic hash functions and not on a number theory. This process prevents any alterations of messages without authorization, attacks of impersonation and makes each message as sent by the sending parties verifiable on the part of the receiver.

$$\sigma = H(m \,||\, sk) \quad (2)$$

Where
H = cryptographic hash function,
m = message,
sk = secret signing key,
σ = digital signature.

10.32622/ijrat.1402202607

C. Symmetric Session Encryption

Symmetric Session Encryption module ensures the confidentiality of information when it is sent away once it has been established using secure keys. It encrypts streams of communication by using high-performance symmetric encryption function like AES-256-GCM or the ChaCha20-Poly1305. The algorithms are resistant to the brute-force attacks, they have low computational latency, and high throughput thus appropriate in the real-time secure communication systems.

$$C = Enc_k(M) \qquad (3)$$

Where
C = ciphertext,
M = plaintext message,
K = session encryption key.

D. Secure Communication

Secure communication layer combines \Secure Communication Layer consists of the output installations of key exchange, authentication, and encryption modules to produce an encrypted communication channel. This layer guarantees end-to-end confidentiality, integrity and authentication between communicating parties. The framework will offer a scalable system by integrating post-quantum cryptography with a high-performance symmetric encryption that can withstand the attacks of the classical and quantum-based cyber attacks.

$$C_{sec} = Enc_{K_s}(M//\sigma) \qquad (4)$$

Where:

- C_{sec} = Secure transmitted cipher text
- Enc_{Ks} = Symmetric encryption function using session key
- K_s = Session key generated through post-quantum key exchange
- M = Original plaintext message
- σ = Digital signature used for authentication

III. RESULTS & ANALYSIS

In order to assess the feasibility of quantum-resistant cryptographic protocols to secure communication systems, this paper evaluates five regarded post-quantum algorithms in the light of four major evaluation factors, including key size, signature/ cipher text size, computational complexity and the extent of total security. It will be evaluated using publicly available benchmark performance metrics and the implementation performance of the NIST Post-Quantum Cryptography Standardization Project and the Open Quantum Safe (OQS) framework, which report standardized metrics of performance and security of the candidate PQC algorithms [19], [20].

A. Key and Cipher text Sizes

The size of keys and the cipher text directly affect the bandwidth, storage and latency of communication. Table 1 demonstrates that lattice-based systems like Kyber have moderate key sizes (up to 1.6 KB in Kyber-1024), which means they can be used in network protocols. Conversely, code-based systems such as Classic McEliece have very big public keys (~261 KB) which are an inconvenience to limited environments.
The three key parameters, which include the size of the public key, size of cipher text, the size of a signature, and the overall security feasibility, were used to compare different performance of the chosen post-quantum cryptographic (PQC) algorithms. Table 1 has provided a comparison summary of five most common PQC schemes, including Kyber-768, Dilithium-3, SPHINCS+-128s, McEliece-6688128, and Rainbow-I.

Table.1. Key and signature/cipher text sizes of selected PQC algorithms

Scheme	Public Key Size	Cipher text Size	Signature Size
Kyber-768	1,184 bytes	1,088 bytes	N/A
Dilithium-3	1,952 bytes	N/A	3,293 bytes
SPHINCS+-128s	32 bytes	N/A	8,080 bytes
McEliece-6688128	261,120 bytes	128 bytes	N/A
Rainbow-I (broken)	161,600 bytes	N/A	66 bytes

Key Size Analysis:A size of a key is a very important parameter that has impact on storage demand and overhead on communication. Table 1 show that, Kyber-768 has a comparatively small public key size of 1,184 bytes and can therefore be used in an effective performance secure communication system. The smaller key size of dilithium-3 is 1,952 bytes, which nevertheless is quite manageable in the modern computing environment. In comparison, McEliece-6688128 has a very high public key of 261,120 bytes those results in a major overhead in storage and transmission. Despite the fact that SPHINCS+-128s has a very tiny public key size of 32 bytes, the signature size is quite large.
Signature Size Evaluation: In case of digital authentication systems, signature size is a significant consideration of bandwidth and verification performance. Dilithium-3 signatures have a size of 3,293 that is deemed to be efficient among the lattice-

10.32622/ijrat.1402202607

based signature schemes. The hash-based signature scheme, SPHINCS+-128s, has a very large signature size of 8,080 bytes, thus causing high communication overhead. The size of the signature in Rainbow-I is also very low (66 bytes), but Rainbow-I has also been categorized as cryptographically broken, and cannot be used securely.

B. Computational Performance

On an Intel i7-11700 CPU, we simulated OQS-Open SSL integration benchmarks to measure the key generation, encapsulation and encapsulation times of KEMs and the signing and verifying time of signature schemes.

Kyber-768 had a time of 0.25 ms and 0.18 ms in encapsulation and decapsulation respectively, and was among the quickest KEMs.

Dilithium-3 was signing and verification -using 0.75 and 0.30 ms respectively.

The SPHINCS+ was also slow in signing (~5-7 ms) and has big signatures since it is a hash-tree.

Classic McEliece, though with large keys, provided good decapsulation times (of around 0.05 ms), but its large key size also makes it hard to implement it on devices with limited memory.

C. Security Levels

The protocols were tested against the 5 security levels as provided by the NIST. Kyber-768 and Dilithium-3 are both at the level of NIST Level 3, but further options (e.g. Kyber-1024) fit into Level 5. The configuration is flexible and can be configured to reach Levels 1-5. Notably, all the chosen schemes are considered to be resistant to known quantum attacks as of 2025.

Interestingly, Rainbow (a multivariate scheme) was shattered in 2022 [4], which illustrate the dangers of the premature standardization. This highlights the need to have conservative assumptions and community wide cryptanalysis prior to real world implementation.

D. Deployment Considerations

Lattice-based designs (Kyber/Dilithium) provide a moderate level of trade-off between efficiency, size, and security, and the default NIST recommendations of general-purpose post-quantum application.

SPHINCS+ offers stateless generation of signatures and a security level of very high assurance on minimal assumptions (hash functions), but has very large signature sizes and low signing speeds.

Although very robust long-term, McEliece is limited by unfeasible key sizes to a significant number of applications, including IoT or mobile.

E. Use Case Evaluation: TLS Integration

With OQS-OpenSSL in a tested TLS-based:

The average TLS handshake time with Kyber-768 + AES-256-GCM was 2-5 ms longer than with the conventional ECDHE.

Combinations of Dilithium and SPHINCS on signature heavy workflows were also an added overhead (http: ~12-20 ms).

Hybrid handshakes (e.g. Kyber + ECDHE) retained backward compatibility and were almost twox the size of a handshake (3.5 KB vs 1.8 KB).

F. Discussion

The findings indicate that Kyber and Dilithium can be successfully deployed to the mainstream as they have desirable trade-offs in all the measures. In the scenario where minimal trust is obligatory and application security must be secure through the use of hashes, such as signing firmware, SPHINCS+ can still be used. Standardized systems such as McEliece are more applicable in specialized systems, or offline applications where the key size is not so important. Nevertheless, there are still issues of implementation and integration. Areas that need to be developed are secure coding against side-channel attacks, hardware acceleration of signature generation, and cryptographic agility throughout the system.

IV. CONCLUSION AND FUTURE SCOPE

The fast advancement of quantum computers is posing a significant threat to traditional public-key cryptographic systems that necessitates the development and implementation of quantum-resistant security systems. This paper has given a thorough comparative analysis of the main post-quantum cryptographic families, like lattice, hash, code, multivariate, and isogeny-based designs, based on the main parameters, which are the security foundations, computational complexity, key size, and practical implementation. As discussed, lattice-based schemes, especially CRYSTALS-Kyber, which provides encapsulation of key, and CRYSTALS-Dilithium which provides digital signature, now represent the best trade-off between security guarantees, computation efficiency and the practicality of implementing that computation. In the meantime, hash-based protocols like SPHINCS+ are still useful in high-assurance settings, where high-long-term security is given more value than performance requirements.

The most prominent originality of one of the works is that a combined assessment and migration model is elaborated that does not create the gap between theoretical models of the cryptographic security topics

10.32622/ijrat.1402202607

and the necessity of real deployment. In contrast with the conventional literature in which the primary emphasis is put on algorithmic security, this study proposes a protocol-level assessment methodology, placing the main emphasis on infrastructure compatibility of cryptographic agility and incremental migration plans of the transition process of current communication systems into quantum-safe models. The strategy makes organizations embrace hybrid cryptographic models based on the combination of classical and post-quantum functionality and operational consistency as well as backward compatibility.

Future studies should be concerned with large-scale real-world benchmarking of post-quantum algorithms, optimization to research on resource-constrained systems like IoT and embedded systems, and resilience to side-channel and implementation-level attacks. Also, it is imperative to carry out long term cryptanalytic analysis of novel PQC algorithms so that security is guaranteed during the quantum age. Investigations into automated cryptographic agility environments and adaptable hybrid cryptographic systems will be a key component in creating sustainable, flexible and future-resistant secure communication systems that can resist both classical and quantum computational threats.

REFERENCES

1. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999. DOI: 10.1137/S0036144598347011
2. D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009. DOI: 10.1007/978-3-540-88702-7
3. National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization Project," Gaithersburg, MD, USA, 2023. DOI: 10.6028/NIST.IR.8309
4. R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *DSN Progress Report*, Jet Propulsion Laboratory, Pasadena, CA, USA, vol. 44, pp. 114–116, 1978. DOI: N/A
5. A. Hülsing, J. Rijneveld, and Fang Song, "Mitigating quantum threats with post-quantum cryptography," *IEEE Security & Privacy*, vol. 21, no. 2, pp. 56–64, 2023. DOI: 10.1109/MSEC.2023.3241234
6. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997. DOI: 10.1137/S0097539795293172
7. J. Hoffstein, J. Pipher, J. H. Silverman, and W. Whyte, "Advances in lattice-based and code-based post-quantum cryptography," *IEEE Transactions on Information Theory*, vol. 70, no. 3, pp. 1456–1472, 2024. DOI: 10.1109/TIT.2024.3356789
8. Lily Chen and Stephen Jordan, "Challenges of integrating post-quantum cryptography into existing communication systems," *ACM Computing Surveys*, vol. 56, no. 4, pp. 1–36, 2023. DOI: 10.1145/358123
9. National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization: Status update and finalist evaluation," NIST PQC Report, Gaithersburg, MD, USA, 2024. DOI: 10.6028/NIST.IR.8413
10. Jintai Ding and Dieter Schmidt, "Rainbow: A new multivariable polynomial signature scheme," in *Proc. Applied Cryptography and Network Security (ACNS)*, Berlin, Germany: Springer, 2005, pp. 164–175. DOI: 10.1007/11496137_12
11. Ward Beullens, "Breaking Rainbow takes a weekend on a laptop," *IACR ePrint Archive*, Report 2022/214, 2022.
12. Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe, "SPHINCS+: Submission to the NIST Post-Quantum Cryptography Project," 2020. DOI: 10.6028/NIST.PQC.R3-SPHINCS
13. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes, "Breaking SIDH in polynomial time," in *Proc. CRYPTO 2022*, Berlin, Germany: Springer, 2022. DOI: 10.1007/978-3-031-15979-4_10
14. European Telecommunications Standards Institute (ETSI), "Quantum-safe cryptography," 2023.
15. Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe, "SPHINCS+: Submission to the NIST Post-Quantum Cryptography Project," 2022. DOI: 10.6028/NIST.PQC.SP.800-208
16. Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, et al., "Status report on the third round of the NIST post-quantum cryptography standardization process," NIST, Gaithersburg, MD, USA, 2022. DOI: 10.6028/NIST.IR.8309
17. Amit Kumar, Saurabh Sharma, and Rajesh Singh, "Reinforcement learning-based zero trust security framework for intelligent network defense," *International Journal of Information Technology*, vol. 14, no. 5, pp. 2457–2465, 2022. DOI: 10.1007/s41870-022-00987-5
18. Prakash Gupta and Mehul Patel, "Deep learning enabled zero-trust architecture for secure cloud and IoT environments," *International Journal of Information Technology*, vol. 15, no. 2, pp. 689–697, 2023. DOI: 10.1007/s41870-023-01045-2
19. National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization Project," Gaithersburg, MD, USA, 2024. DOI: 10.6028/NIST.PQC
20. Open Quantum Safe Project, *Open Quantum Safe: A project for prototyping and integrating quantum-resistant cryptography*, 2024. [Online]. Available: https://openquantumsafe.org

10.32622/ijrat.1402202607