IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Post Quantum Cryptography: A Comprehensive Review of Migration Challenges & Strategies

[1]Nisha Bhadauriya Agarwal, [2]Ajeet Kumar Agarwal,

[1]S D Bansal College of Technology, Indore, India
[2]College of Defence Management, Secunderabad, India

Abstract : The advancement of Quantum Computers (QC) and its identification as a possible danger to asymmetric cryptography are becoming more and more significant. To protect traditional cryptographic systems from the dangers of quantum computing, post-quantum cryptography, or PQC, is crucial. Traditional algorithms like RSA and ECC run the risk of becoming outdated as quantum computers develop because of Shor's algorithm. The security and effectiveness of PQC algorithms, including as lattice-based, hash-based, code-based, and multivariate cryptography, are evaluated in this review. It also examines important migration issues such performance overheads, standardization delays, compatibility with current infrastructure, and the requirement for crypto-agility. The shift to quantum-resistant systems necessitates careful preparation to prevent interruptions while NIST's PQC standardization process is under progress. While maintaining backward compatibility, organizations must implement hybrid solutions during the transition period. In order to guarantee long-term cybersecurity in the quantum age, this article emphasizes the necessity of PQC adoption and offers guidance on removing migration obstacles. This study examines Post Quantum Cryptography (PQC) as a countermeasure to QC and aims to highlight the difficulties associated with implementing PQC. Post-quantum cryptography (PQC) has to be developed since the emergence of quantum computing threatens traditional cryptographic methods. The concepts of PQC, the several cryptographic algorithms that are being examined, and the difficulties in converting current systems to quantum-resistant cryptographic standards are all covered in this paper.

IndexTerms **- Quantum Cryptography, Post Quantum Cryptography, Migration Challenges, RSA, ECC, Shor's Algorithm.**

1. INTRODUCTION.

Currently, digitization is a worldwide phenomenon that is happening quickly. Information encryption is crucial for storing, transmitting, receiving, and hiding data, especially when done quickly and in more secure ways. Its foundation is the challenge of completing mathematical calculations in the smallest amount of time. Notably, algorithms such as RSA and Diffie-Hellman can be solved in years by a conventional computer, while they can likely be completed in seconds by a quantum computer (QC). Although QC presents new research opportunities, it also poses a risk to the established classical cryptography techniques, as QC may readily defeat their secure algorithms. Many academicians, researchers, and scholars are joining a community that is more committed than ever to developing a quantum-resistant cryptosystem. The European Telecommunication Standards Institute (ETSI) held workshops on "Quantum-Safe Cryptography" in 2013, and shortly after, in 2015, the National Institute of Standards & Technology (NIST) held a workshop on "Cybersecurity in a Post-Quantum World." These efforts have resulted in advancements in the field. It is safe to say that while the development of quantum-resistant devices is accelerating, there is a need for standardization. In essence, it is a race to build large-scale quantum computers, which have the potential to destroy the current classical cryptography setup and give rise to standardized post-quantum cryptography schemes. The majority of post-quantum algorithms currently in use fall into distinct families, each of which is a subset of mathematical problems that are challenging to resolve, even for quantum computers.

The traditional cryptographic systems that support contemporary digital security are under unprecedented threat from the quick development of quantum computing. In order to secure online transactions, communications, and sensitive data, cryptographic algorithms like RSA, ECC (Elliptic Curve Cryptography), and Diffie-Hellman rely on mathematical problems like discrete logarithms and integer factorization, which quantum computers can effectively solve with Shor's algorithm. According to estimates, decades of cryptographic infrastructure may be rendered useless in a matter of minutes if a sufficiently powerful quantum computer were to breach current systems. The creation of Post-Quantum Cryptography (PQC), a novel class of cryptographic algorithms built to resist quantum attacks, has been sped up by this impending weakness.

Lattice-based cryptography, hash-based signatures, code-based cryptography, multivariate polynomial cryptography, and isogeny-based cryptography are some of the mathematical techniques that fall under the umbrella of post-quantum cryptography. These methods are based on computational issues that are thought to be impervious to both classical and quantum attacks, in contrast to classical systems. For example, hash-based signatures use the security of cryptographic hash functions, whereas lattice-based cryptography depends on the difficulty of problems such as the Shortest Vector Problem (SVP) or Learning With Errors (LWE). With the announcement of the first chosen algorithms (CRYSTALS-Dilithium for digital signatures and CRYSTALS-Kyber for key encapsulation) in 2022, the National Institute of Standards and Technology (NIST) has been spearheading the PQC standardization project. But making the switch to PQC is not easy; there are many operational, strategic, and technical obstacles to overcome.

The capacity of systems to quickly accept new cryptographic standards without requiring significant architectural changes is known as crypto-agility, and it is one of the most urgent issues. Since classical cryptography is deeply ingrained in many legacy systems, such as government databases, banking networks, and Internet of Things devices, migration is a difficult, multi-year process. Furthermore, compared to their classical equivalents, PQC algorithms frequently call for bigger key sizes and more processing power. For instance, RSA only requires a few hundred bytes of key material, whereas lattice-based techniques may require kilobytes, resulting in higher bandwidth and storage needs. Adoption may be hampered by this performance penalty in contexts with limited resources, such as 5G networks and embedded systems. Standardization and interoperability are yet another significant obstacle. Even though NIST's PQC standardization process is a big start in the right direction, governments, businesses, and tech companies must work together to ensure its widespread acceptance. Fragmentation may result from distinct sectors prioritizing different PQC methods according to use-case needs. Furthermore, as temporary fixes to reduce risks during migration, hybrid cryptographic systems that combine classical and PQC algorithms are being suggested. However, careful design and testing are necessary to create such systems without creating new vulnerabilities.

Another significant obstacle is security assurance. PQC methods are very new, and their long-term resistance against both quantum and classical attacks is still being examined, in contrast to well-studied classical algorithms. Developments in cryptanalysis have already cracked or weakened several of the suggested PQC options, highlighting the necessity of cautious deployment techniques. The hazards of using algorithms that have not been thoroughly tested must be weighed against the urgency of achieving quantum ready.

Beyond technical difficulties, policy and legal frameworks need to change in order to require the deployment of PQC in vital industries. Governments around the world are starting to release recommendations. For example, the EU is integrating PQC into its cybersecurity resilience plans, while the U.S. has sponsored the Quantum Computing Cybersecurity Preparedness Act. Global security postures may be compromised, though, as compliance schedules differ and certain businesses may not enforce laws as quickly as others. There are logistical and financial issues with the switch to PQC as well. Businesses must determine how much it will cost to update their cryptographic libraries, software, and hardware while minimizing service interruptions. It will be crucial to develop new key management procedures and teach cybersecurity experts PQC concepts. Furthermore, if supply chain risks—like hacked PQC implementations in third-party components—are not adequately addressed, they may jeopardize security initiatives.

Delaying PQC migration is not an option, notwithstanding these difficulties. High-value targets are already at risk from Harvest Now, Decrypt Later (HNDL) operations, in which attackers gather encrypted material now and decrypt it when quantum computers become accessible. Adoption of PQC must be given top priority by governments and businesses that handle long-term sensitive data (such as intellectual property, medical records, or classified information) in order to stop future breaches. This study examines the state of post-quantum cryptography today and evaluates the advantages and disadvantages of the most popular PQC algorithms. It also looks at the various difficulties involved in switching from classical to quantum-resistant systems, providing advice on how to make the move safe and easy. Stakeholders can guarantee that cryptographic infrastructures continue to be robust in the quantum age by tackling operational, technological, and legislative obstacles.

2. POST QUANTUM CRYPTOGRAPHY.

Modern cryptography is based on computational issues that are too complex for traditional computers to solve. Algorithms that have been safe for decades, such as RSA, ECC (Elliptic Curve Cryptography), and Diffie-Hellman, rely on the difficulty of discrete logarithms and integer factorization. The advent of quantum computing, however, poses a danger to this security paradigm.

2.1 The Quantum Threat to Classical Cryptography

Shor's algorithm, a quantum method created in 1994 by mathematician Peter Shor, can solve discrete logarithms and integer factorization in polynomial time. A sufficiently potent quantum computer may potentially crack popular encryption techniques like RSA and ECC in a matter of hours or even minutes, according to this study. Even though Grover's technique isn't as destructive, it can accelerate brute-force attacks and essentially cut the security of symmetric-key algorithms like AES in half. Even while there are currently no large-scale, fault-tolerant quantum computers, the quick development of quantum computing by firms like Google, IBM, and startups indicates that these devices might be available in the next ten to twenty years. Recognizing that cryptography methods need to be improved before quantum computers can scale sufficiently, governments and businesses are already getting ready for this possibility.

2.2 The Birth of Post-Quantum Cryptography (PQC)

Cryptographic techniques created to withstand attacks from both classical and quantum computing are referred to as post-quantum cryptography. PQC is based on mathematical difficulties that are thought to be impervious to quantum algorithms, in contrast to quantum cryptography, which depends on quantum physics (e.g., Quantum Key Distribution). Beginning in the early 2000s, research into quantum-resistant cryptography became more urgent as quantum computers advanced. The National Institute of Standards and Technology, or NIST, started a standardization process in 2016 to assess and choose PQC algorithms for broad use. Finding alternatives to RSA, ECC, and other weak systems before quantum computers make them useless was the aim.

2.3 Key Families of Post-Quantum Cryptographic Algorithms

Cryptographic techniques that are immune to quantum computer attacks are the main focus of post-quantum cryptography (PQC). Different types of PQC Algorithms are as shown in Fig. 1. Among the key families is lattice-based cryptography, which is in the forefront of standardization efforts (e.g., NIST's CRYSTALS-Kyber) and depends on the difficulty of issues such as Learning With Errors (LWE). Classic McEliece is one type of code-based cryptography that makes use of error-correcting codes. Cryptographic hash functions are used by hash-based signatures (like SPHINCS+), whereas multivariate cryptography relies on solving nonlinear equations. Isogeny-based cryptography exchanges keys using elliptic curve isogenies, such as SIKE. Each family influences the development of quantum-resistant encryption by providing distinct trade-offs in terms of security, effectiveness, and implementation complexity. There are four major types of PQC algorithms.

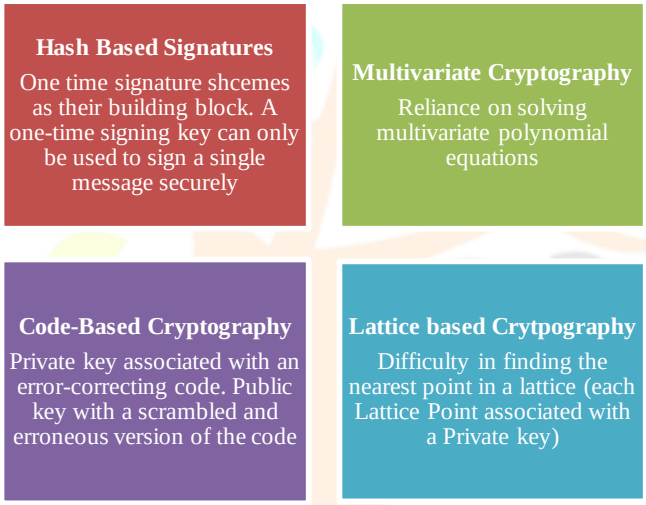

Fig. 1 Types of PQC algorithms

PQC candidates are categorized based on the underlying mathematical structures they rely on:

Lattice-Based Cryptography: Lattice Cryptography is based on the mathematical concept of a lattice in which the geometric structure encodes and decodes messages. A lattice can be thought of as grid of points spaced out regularly and extending to infinity.

- Vector is a point with a set of numbers called the coordinates of the vector. For instance, (2,3) is a 2-D vector as it has 2 coordinates – a lattice is a collection of such vectors, evenly spaced. A vector is called "long" and "short" depending upon distance from origin.
- Basis: Lattices are infinitely stretched and computers have only a finite memory to work with. Basis is a term used to define a lattice – it is a small collection of vectors that can be used to reproduce a point in the lattice.
- Short Vector Problem: A long basis for a lattice L is given and a grid point in L as close to the origin as possible is to be found. In cryptography, the lattices will have nearly 10,000 coordinates and finding a combination of basis vectors that simultaneously makes all 10,000 coordinates small is quite hard even for a quantum computer.
- Closest Vector Problem: A long basis for a lattice L is given and a point P is given – closest point to P is to be found in the lattice space.

Lattices are versatile as they allow one to build variety of cryptographic schemes, they are devoted a bulk of research work when speaking of PQC. They allow for hard math problems which are tough even for a quantum computer. Some of the benefits of Lattice Cryptography[2] are as follows:

- They provide improved security as they are difficult to crack.
- They have faster computation times when compared to other cryptographic algorithms.
- Lattice cryptography allows for lower energy consumption and are easier to implement.

Lattice Cryptography is based on the hardness of problems like **Learning With Errors (LWE)** and **Shortest Vector Problem (SVP)**. Examples include **CRYSTALS-Kyber (Key Encapsulation Mechanism), CRYSTALS-Dilithium**

(Digital Signatures). The advantages if lattice based cryptography are its efficiencyand versatililty. It is also considered one of the most promising PQC approaches.

Hash-Based Cryptography: Hash based Digital signatures serve as an alternative to RSA algorithms which are asymmetric in nature. Unlike other quantum-safe cryptographic algorithms which are "some years away from being standardized, the hash schemes like XMSS and HSS have been approved by the Crypto Forum Research Group (CFRG)" [3]. The Hash functions depend on the collision and preimage resistance of the Hash function. The Preimage resistance implies that it is difficult to find an input x such that y = H(x). Collision resistance implies that given an arbitrary message z1, it is difficult to find another message z2, such that H(z1)=H(z2). Finding quantum algorithms to perform such tasks will be hard which suggests the use of Hash functions in PQC. The only disadvantage that they suffer is that a digital signature can be used only once. It relies on the security of cryptographic hash functions (e.g., SHA-3) and is used primarily for **digital signatures** (e.g., **SPHINCS+**).It has well-understood security, but is limited to signature schemes.

Code-Based Cryptography: **Code-based cryptography** relies on the hardness of decoding random linear codes, a problem believed to resist quantum attacks. The most prominent example is the **McEliece cryptosystem**, which uses binary Goppa codes for encryption, offering strong security but large key sizes. Recent variants like **Classic McEliece** (a NIST PQC finalist) optimize efficiency. **BIKE** and **HQC** are code-based key encapsulation mechanisms (KEMs) using quasi-cyclic codes for smaller keys. While encryption/decryption can be fast, bandwidth overhead remains a challenge. Nevertheless, code-based schemes are among the most mature post-quantum candidates, with decades of cryptanalysis backing their security.

Multivariate Polynomial Cryptography: The basic architecture used is same for all Multivariate Public-Key Cryptosystems (MPKC). **Multivariate polynomial cryptography** is a post-quantum approach based on the difficulty of solving systems of nonlinear polynomial equations over finite fields—a problem known to be NP-hard. These schemes typically use quadratic polynomials to construct public-key encryption, digital signatures, or key exchange mechanisms. Notable examples include **Rainbow** (a NIST PQC signature finalist) and **HFEv-** (used in GeMSS). While multivariate schemes offer fast computation and small key sizes compared to other post-quantum families, they often face challenges in security parameter selection, as some variants have been broken via algebraic attacks (e.g., Oil & Vinegar structure weaknesses). Recent research focuses on enhancing robustness through improved trapdoor designs and hybrid approaches. Despite historical vulnerabilities, multivariate cryptography remains an active area due to its efficiency advantages in low-resource environments.

Isogeny-Based Cryptography: Isogeny-based cryptography is a promising post-quantum approach that relies on the mathematical complexity of computing isogenies (mappings) between elliptic curves. Unlike traditional elliptic curve cryptography, which depends on the discrete logarithm problem, isogeny-based schemes, such as Supersingular Isogeny Diffie-Hellman (SIDH/SIKE), derive security from the difficulty of finding paths between supersingular elliptic curves. These schemes offer compact keys and efficient key exchange but face challenges in performance and side-channel resistance. Although SIKE was initially considered for NIST standardization, a 2022 attack using advanced quaternion algebra weakened its security, prompting a reevaluation. Despite this, research continues into more robust isogeny-based constructions for quantum-resistant cryptography.

2.4 NIST's PQC Standardization Process

The National Institute of standards and Technology (NIST) started a standardization process for new PQC algorithms in December 2016. A total of 69 algorithms were submitted for the NIST PQC competition. After evaluation of the submissions on the basis of Security, Cost and Performance, algorithm and implementation characteristics [6]. The third round of the competition concluded in July 2022 in which 15 algorithms were selected. The family and security levels of these algorithms are specified in Table 1 [6]. NIST's multi-year effort to standardize PQC algorithms has been critical in driving adoption. The process involved:

- Call for proposals (2016): 82 submissions received.
- Multiple rounds of evaluation: Assessing security, efficiency, and practicality.
- First selected algorithms (2022):
    - CRYSTALS-Kyber (Key Encapsulation).
    - CRYSTALS-Dilithium, FALCON, SPHINCS+ (Digital Signatures).
- Fourth-round candidates (2024): Further evaluation of additional schemes.

Table 1. Family and Security Levels of PQC algorithms

Algorithm	Algorithm Family	Security Level
Classic McEliece	Code	5 [64]
Saber	Lattice	1, 3, 5 [64]
Crystals-Kyber	Lattice	1, 3, 5 [64]
NTRU-HRSS	Lattice	1 [64]
NTRU-HPS	Lattice	1,3,5 [65]
Crystals-Dilithium	Lattice	1, 2, 3 [64]
SIKE	Isogeny	1, 2, 3, 5 [65]
SPHINCS+	Hash	1, 3, 5 [64]

2.5 Why PQC Adoption is Urgent: Harvest Now, Decrypt Later (HNDL) Attacks

The fact that opponents are already gathering encrypted data—such as financial records and government secrets—with the goal of employing quantum computers to decipher it later is a serious worry. Sensitive information sent today may eventually be compromised due to this "store now, break later" approach. Because conventional and quantum cryptography are developing so quickly, there is a need for a more dependable and failsafe cryptography. A switch to Post-Quantum Cryptography (PQC) will be necessary for this. Cryptosystems with 112 bits of security are thought to be secure for a substantial amount of time. The shift to post-quantum cryptography presents basic difficulties. PQC is a field of research specializing in creation of algorithms that are robust enough to withstand attacks by QC [1]. Creating mathematical puzzles that are difficult for QC to solve is one way to fend off QC attacks. Hash functions and symmetric algorithms are supposed to be safe from QC.

3. MIGRATION CHALLENGES.

The transition from classical to post-quantum cryptography presents significant technical and logistical challenges as shown in Fig. 2[14], below.

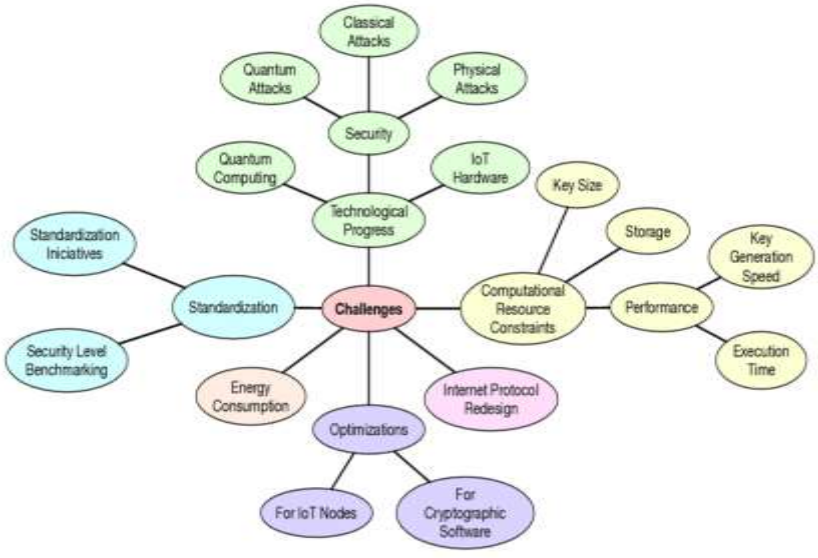

Fig. 2 Migration Challenges [14]

The migration to PQC will need a substantial time and financial investment due to the need to modify current processes, plans, and infrastructure. Everyone would need to work together as the landscape surrounding existing cryptography shifts and we get closer to this new system. Hybrids are one tactic that maintains compatibility with conventional cryptography methods while supporting PQC. It enables the integration of PQC with traditional algorithms. Hybridization would facilitate the switch from PQC to conventional cryptography and existing hardware, but it is not a long-term fix, particularly in low-power devices like smart cards and embedded systems. Due to the heavy reliance on RSA and ECC by older systems (such as government infrastructure, banking, and the Internet of Things), backward compatibility is a significant concern. Including PQC algorithms, which frequently call for bigger keys and greater processing power, could put a strain on the hardware that is already in place, especially in low-power devices like embedded systems and smart cards. Lattice-based systems, for example, require more processing power and bandwidth, which could slow down secure communications. Performance overhead is another issue.

Migration is made more difficult by delays in standardization. Although NIST has chosen preliminary PQC algorithms, organizations are reluctant to commit to widespread use because final standards are still being developed. When there is no universal agreement on the best algorithms, there is a chance that different industries will employ incompatible solutions, leading to fragmentation. Furthermore, hybrid cryptography adds complexity to implementation and key management by fusing classical and PQC techniques as a transitional step. Given that several PQC candidates have been compromised after submission (such as SIKE in 2022), security assurance is still crucial. Early adoption must be weighed

against the possibility of implementing algorithms that turn out to be weak in the future. Government and industry demands for regulatory and compliance frameworks are inconsistent, causing them to lag behind. Lastly, the expense of the migration—upgrading software, hardware, and staff training—is a deterrent, particularly for smaller businesses. Phased rollouts, proactive planning, and crypto-agility are necessary to minimize interruptions and guarantee a safe transition to quantum-resistant cryptography. The following are a few of the suggested hybrids:

3.1 Dual Signature

One digital signature method used in safe electronic transactions, namely in SET (safe Electronic Transaction) protocols, is the dual signature. It allows each party to validate only the pertinent portion of two connected messages, such as order information for the merchant and payment details for the bank. To ensure integrity without disclosing extraneous information, the signer generates a single signature over the two hashed messages. By keeping both parties from obtaining the complete transaction data while maintaining authenticity, this improves e-commerce security and privacy. For digital payments to be trusted by many parties, dual signatures are essential. Signing with different keys means that the data is signed twice: once using a PQC and once using a conventional key. The two signatures are then checked by the verifier for authenticating the data(Fig. 3, Verification of signatures).

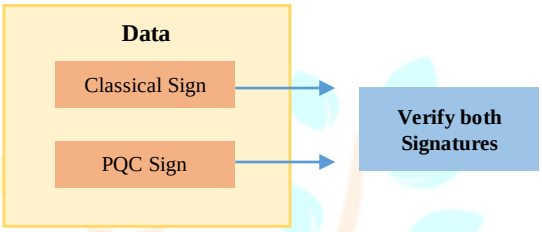

Fig. 3 Verification of signatures

3.2. Key Encapsulation Medium (KEM)

A cryptographic technique called a Key Encapsulation Mechanism (KEM) is made to safely create a shared secret key between two parties via an unprotected channel. A KEM differs from conventional key exchange protocols (like Diffie-Hellman) in that one party creates a ciphertext that is encased in a public key and contains the secret key. The other party then uses their private key to decapsulate the ciphertext. KEMs are essential to post-quantum encryption; two of the most well-known quantum-resistant examples are the code-based Classic McEliece and the lattice-based CRYSTALS-Kyber (NIST-standardized). In hybrid systems, KEMs are frequently used in conjunction with symmetric encryption to provide IND-CCA2 security, which thwarts chosen-ciphertext attacks. Although effective, there are drawbacks, particularly with code-based and isogeny-based methods, such as balancing ciphertext/key sizes and computational complexity. KEMs are essential for protecting communications in the future from quantum attacks. KEM will be a crucial weapon in the fight against quantum dangers. None of the cryptographic APIs currently in use can naturally describe KEM. The three functions that make up KEM are the Key Pair Generation, Key Encapsulation, and Key Decapsulation routines. The key for symmetric encryption is generated in a KEM by feeding the outputs of both algorithms into a key derivation function (Fig. 4, KEM for PQC).

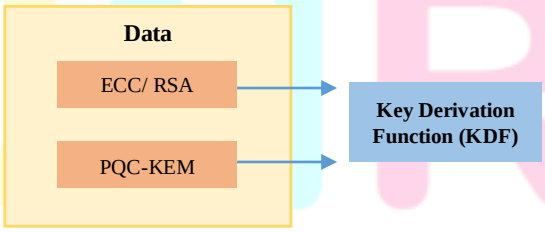

Fig. 4 KEM for PQC

3.3 Major Migration Challenges

3.3.1 Increase in Object Size: As PQC increases the size of cryptographic objects for instance public keys and signatures, therefore embedding/ overlaying a PQC algorithm over a classical algorithm will significantly increase the object sizes of signatures – aim would be to decrease the cryptographic payloads. Adoption of PQC in existing hardware and in the existing ecosystem will prove to be a major challenge. Below is a comparison of classical and some PQC schemes selected during the NIST standardization process [7].

Table 2. Comparison of classical and PQC for QC safety - some schemes from the NIST process

Algorithm Name	Parameter Set Name	Public Key size (bytes)	Ciphertext or Signature size	(S)ignature or (K)EM/KEX	Quantum-safe?
NIST P256	SECP256R1	64	64	K	✗
Kyber	KYBER512	800	768	K	✓
	KYBER768	1184	1088	K	✓
ECDSA	ECDSA_SECP256R1	64	64	S	✗
Falcon	FALCON-512	897	690	S	✓
Dilithium	DILITHIUM2	1312	2420	S	✓
Sphincs+	SPHINCS+-SHAKE256-128S-SIMPLE	32	7856	S	✓
	SPHINCS+-SHAKE256-128F-SIMPLE	32	17088	S	✓

3.3.2 User Data: Assuming that all data is migrated to a PQC platform, it is envisaged that a user can decrypt past communications and that information for future attacks as well.

3.3.3 Analysis of existing protocols: Each application protocol will require a specific analysis. Migration measures can include "limiting authorizations and access token duration time, enforcing a policy for long-term confidential data usage, and revoking past actions performed with classical cryptography" [8].

3.3.4 Complicated Migration criteria for PQC: The conversion to post-quantum cryptography standards is a major hurdle which will not be the easiest to cross.

3.3.5 Rapid Development in Quantum Computing: A major issue would arise if in case QC is developed in all aspects before PQC could be developed thus obviating a lot of effort that has already gone through it and calling for rapid development of PQC.

3.3.6 Record Now, Exploit Later attacks: As most of the private information is shared these days, i.e., in encrypted form, is captured and used after several years by the QC if it is still relevant.

3.3.7 Implementation Considerations: A major hurdle in migration will be the development of an ecosystem that supports PQC without having to rework all the existing paraphernalia surrounding crypto. This would require due weightage to security and performance conditions and their requirements for PQC systems.

4. FUTURE SCOPE & DEVELOPMENTS.

The US government has stated that it will start the transition to post-quantum cryptographic algorithms by 2024, following the completion of standardization, even though it "is currently using the Commercial National Algorithm Suite for protection of information of data up to Top Secret" [9]. Below is a list of some of the post quantum solutions that are currently accessible [10].

• Cloudfare is another company that has demonstrated the use of a post-quantum option for secure tunnels; it combines the elliptic curve based key protocol X25519 with the post-quantum KEMs.
• AliBaba, a multibillion dollar company, has integrated the idea of quantum random number generators to enhance the security of financial transactions. This hybrid protocol is theoretically guaranteed to provide 256-bit security against quantum assaults.
• Google's internal communication networks now employ post-quantum cryptography. They use a hybrid approach that combines X25529 and NTRU-HRSS. Additionally, they are said to have begun developing post-quantum cloud capabilities.
• With its post-quantum venture, IBM is making significant strides. The IBM cloud already offers post-quantum TLS options. The Open Quantum Safe Project community's recommendations served as the foundation for IBM's hybrid algorithms. Additionally, resources for a smooth transition to quantum-safe cryptography are provided via the IBM Quantum Safe project.

In the upcoming years, a number of significant advancements are anticipated in the quickly developing field of post-quantum cryptography. Additional PQC algorithms will be finalized as part of NIST's ongoing standardization process, increasing the number of alternatives for various use cases. For IoT devices, 5G networks, and other resource-constrained contexts, research is also concentrating on optimizing PQC algorithms to lower computational overhead. Transitional deployments will probably be dominated by hybrid cryptographic systems that combine PQC and classical algorithms, guaranteeing backward compatibility while reducing quantum concerns. Future communications will be secured by ongoing developments in post-quantum TLS protocols (such as integration with OpenSSL and BoringSSL) and quantum-resistant blockchain. Crypto-agility, or creating systems that can smoothly transition between cryptographic standards, is another crucial area. As new threats appear and more powerful PQC algorithms are created, this will become crucial. It is anticipated that governments everywhere would impose more stringent PQC compliance requirements, especially for the defense, financial, and critical infrastructure industries. Lastly, PQC schemes will continue to be tested by quantum cryptanalysis, which could result in flaws or breakthroughs. The next generation of quantum-safe cryptography will be shaped by cooperation between academics, business, and policymakers, guaranteeing long-term security in the post-quantum era. Hardware manufacturers are not far behind in making post-quantum cryptography hardware easily accessible;

firms such as Intel, Marvell, and Thales are providing their clients with tools and solutions to evaluate post-quantum readiness using cryptographic agility.

5. CONCLUSION.

Modern encryption has both opportunities and challenges as a result of the development of quantum computing. Post-quantum cryptography (PQC) provides a strong defense, guaranteeing the long-term security of digital infrastructure, while quantum algorithms such as Shor's and Grover's pose existential risks to conventional cryptographic systems [11][13]. This transition has a solid basis thanks to NIST's continuous standardization work and developments in lattice-based, hash-based, and other quantum-resistant algorithms. The switch to PQC is not without its challenges, though. Industry, government, and academic collaboration is required to overcome challenges like performance overhead, interoperability problems, and the requirement for crypto-agility. The imminent threat of "harvest now, decrypt later" assaults, which could eventually compromise critical data, emphasizes how urgent it is to use PQC. In the future, the emphasis should be on utilizing hybrid solutions, strong policy frameworks, and improved algorithms to accelerate PQC integration. The whole community can create a safe, quantum-resistant future by proactively tackling these issues, protecting vital systems from the potentially disruptive effects of quantum computing. In order to safeguard the digital world in the ensuing decades, post-quantum security is a necessary but complicated transition. Although quantum encryption will be a useful tool for safer data exchange, it also encourages research into workable solutions for a post-quantum cryptography scenario. The development of workable and affordable transition technologies to PQC has gained renewed importance as a result of the developments and efforts being made in Quantum Computing. Academic and industry levels are reexamining the switch to a PQC system and the related infrastructure modifications. It may not be difficult to predict that PQC technologies will emerge sooner than QC in the future, ending the situation where QC threatens current cryptographic standards. The threat posed by quantum computing has prompted a major change in cryptographic security known as post-quantum cryptography. Even though NIST's standardization initiatives have sped up development, issues with performance, key sizes, and practical implementation still exist. In addition to being a technological advancement, the switch to PQC is a worldwide cybersecurity necessity to safeguard digital infrastructure in the quantum era.

ACKNOWLEDGMENT

I thank Almighty God, available Online sources and SDBCT for providing me the opportunity and all the support to carry out the work.

REFERENCES

[1] Mailloux, L. O., Lewis II, C. D., Riggs, C., & Grimaila, M. R. (2016). Post-quantum cryptography: what advancements in quantum computing mean for it professionals. IT Professional, 18(5), 42-47.

[2] K. Ahmad, “What is Lattice-Based Cryptography and Why is it Important?” MakeUseOf.com, https://www.makeuseof.com/what-is-lattice-based-cryptography (accessed on 11 Jul 23).

[3] V. Quehen, “Math Paths to Quantum-safe Security: Hash-based Cryptography”, Isara.com, https://www.isara.com/blog-posts/hash-based-cryptography.html (accessed on 14 Jul 23).

[4] A. Rameez, “Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms”, IoT, pp 74-75, Feb 2021

[5] A. Bogdanov, T. Eisenbarth, A. Rupp, C. Wolf, “Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves?” Lect. Notes Comput. Sci., vol. 5154, CHES 2008, Springer (2008), pp. 45-61

[6] L. e. a. Chen, “Report on Post-Quantum Cryptography, NIST Internal or Interagency Report (NISTIR) 8105”, National Institute of Standards and Technology, 2016

[7] R. Bavdekar et al, “Post Quantum Cryptography: Techniques, Challenges, Standardisation, and Directions for Future Research”, pp 9-15, Feb 2022

[8] A. Giron, “Migrating Applications to Post-Quantum Cryptography: Beyond Algorithm Replacement”, Secrypt 2023

[9] J.P. Mattsson, E. Thormarker, “What next in the world of Post Quantum Cryptography?” ericsson.com, https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorithms (accessed on 30 Jul 23)

[10] Taurus Blog, “Quantum Doomsday Planning – the Post Quantum Technology Landscape” taurushq.com, https://www.taurushq.com/blog/quantum-doomsday-planning-2-2-the-post-quantum-technology-landscape/ (accessed on 30 Jul 23)

[11] Nisha Bhadauriya Agarwal, Dr. Deepak Kumar Yadav, 2024, A Comprehensive Analysis of Classical Machine Learning and Modern Deep Learning Methodologies, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 13, Issue 05 (May 2024),

[12] Nisha Bhadauriya Agarwal, Kiran Kumar Makam, Deepak Kumar Yadav, 2025, Quantum Computing and Artificial Intelligence: Progress, Possibilities and Gaps, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 14, Issue 04 (April 2025),

[13] Nisha Bhadauriya Agarwal, July 2023, QUANTUM MEMORY ENHANCED CRYPTOGRAPHY: A NEW FRONTIER IN QUANTUM SECURITY

[14] https://www.researchgate.net/publication/337984796_From_Pre-Quantum_to_Post-Quantum_IoT_Security_A_Survey_on_Quantum-Resistant_Cryptosystems_for_the_Internet_of_Things/figures?lo=1