International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 20 No. 1 (2024)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, No. 1, 2024

Peer Reviewed, Referred & Indexed Journal

Research Paper

Survey on Quantum-Safe Cryptography for Post-Quantum Internet Security

MURALI KRISHNA DARA[1],

[1]Senior Lecturer in Computer Engineering, Government Polytechnic Srikakulam.

Email: muralikrishna9440350315@gmail.com

Abstract

The threats are existential to the traditional cryptosystems of public keys, including RSA, Diffie-Hellman, and elliptic curve cryptography (ECC), due to the rapid progress in quantum computing. Such algorithms as the Shor and Grover algorithms prove that as soon as large scale quantum computers are achieved, these classical cryptographic protocols will not provide any privacy and integrity to online communication. This has created an emergency to find post-quantum cryptography (PQC), or quantum-safe cryptography, which will resist attacks by both classical and quantum attackers. The paper is a review of the latest research and development in post-quantum cryptographic algorithms and their implementation in current security systems. We organize quantum-safe methods into significant organizations such as lattice-based, hash-based, multivariate polynomial-based and code-based encrypted communications. Each type has been evaluated critically based on computational efficiency, key sizes, speed of encryption/decryption and security proofs. The survey also examines the current standardization activities happening in the world and especially the U.S. National Institute of Standards and Technology (NIST) PQC competition, which lists candidate algorithms that have advanced to standard adoption. Besides this, the paper addresses hybrid cryptographic designs that use both classical and post-quantum bases in ensuring a seamless migration in the transition phase. Internet security protocols like TLS, VPNs and blockchain consensus as applications of PQC are examined in detail. Lastly, we pinpoint open research issues, which include creating lightweight PQC to support resource-constrained IoT devices, balancing performance and strong security assurances, and interoperability between the new PQC algorithms and existing infrastructures. Through detailed survey we inform the future of researchers, practitioners, and policymakers on the preparation of the post-quantum era of secure digital communications.

Keywords

Post-Quantum Cryptography, Lattice-Based Encryption, Quantum-Safe Security, Cryptographic Protocols, NIST PQC Standardization, Quantum-Resistant Internet.

1. Introduction

The emergence of quantum computing is one of the most disruptive of the 21 st century technological changes. In contrast to classical computers using bits, quantum computers use quantum bits (qubits), which makes it possible to compute in parallel using superposition and entanglement. Quantum computers can prove to be extremely fast in certain algorithms like integer factorization by Shor, or unstructured search by Grover, which prove that many of the current cryptographic systems that have been considered secure over the last decades could become ineffective within a few days. To illustrate, an employed quantum computer with large scale could factor RSA moduli and break ECC in a time-polynomial time, making digital signatures, encryption with the help of the SSL/TLS protocol, and blockchain consensus systems vulnerable. The nature of a cryptographic collapse is terrible as more and more industries, governments, and crucial infrastructures around the globe become dependent on digital security.

The most viable and immediate response to this problem is post-quantum cryptography (PQC). In contrast to quantum key distribution (QKD), which needs special equipment, PQC needs mathematical problems that are resistant both to classical and quantum attacks. The NIST has also launched a multi-round competition in the PQC, aimed at ensuring that future communication systems have the ability to drop RSA and ECC, as well as to standardize the algorithms. Lattice-based cryptography (e.g., Kyber, Dilithium), code-based cryptography (e.g., Classic McEliece), and hash-based digital signatures (e.g., SPHINCS+) are the lattice-based, code-based, and hash-based candidates respectively that are under intense test.

Although this has been made, PQC has some challenges linked with the computational efficiency, key size, and compatibility with existing protocols. Resource-constrained IoT devices struggle with more challenges in embracing PQC because of energy and resource constraints. Moreover, the replacement of legacy cryptography systems with PQC should be handled very well so as not to introduce vulnerability in the process of migration.The aim of this survey is to synthesize the information on PQC, examine algorithms, implementation initiatives and possible integration technique in various areas of application. The paper is a roadmap to secure communication systems in the quantum era by critically assessing the current developments and pointing out gaps that remain open.

Motivation and Implications:

Evidence of urgency to conduct this survey is based on the fact that cybersecurity infrastructures need to be ready to withstand an imminent emergence of quantum computing. A lack of a quantum-safe approach may lead to disastrous information leakage in monetary dealings, personal medical records, national security, and cloud services. The consequences are extensive: the use of PQC guarantees the long-term privacy of confidential information, the resiliency of

key infrastructures, and the global confidence in the digital systems.

Problem Statement:

Post-quantum cryptography solutions have not yet seen extensive usage in spite of the major progress. Plenty of algorithms still are computationally intensive with impractically large key sizes and not well supported by legacy systems. In addition, there are no standardized deployment frameworks, which makes deploying to PQC questionable by organizations. Thus the main issue is to establish effective, scalable, and interoperable quantum-safe cryptographic systems that can be easily incorporated into the current internet protocols and be highly resistant to future quantum attacks.

1.1 Significant Concepts and Definitions

To ensure conceptual clarity for the technical discussions that follow, the following important terms and concepts are defined:

Quantum Computing: A computational paradigm based on the principles of quantum mechanics, employing *qubits* instead of classical bits. Unlike traditional systems that represent binary 0s and 1s, qubits can exist in multiple states simultaneously through *superposition* and *entanglement*, enabling massive parallelism in computation.

Quantum Threat: The security challenge posed by quantum algorithms, primarily *Shor's algorithm* (for factoring and discrete logarithms) and *Grover's algorithm* (for unstructured searches), which can break conventional cryptographic primitives such as RSA, Diffie–Hellman, and ECC.

Post-Quantum Cryptography (PQC): A class of cryptographic algorithms designed to be secure against both classical and quantum computer attacks. PQC schemes rely on mathematical problems believed to be hard even for quantum computers, such as lattice-based, code-based, hash-based, and multivariate polynomial problems.

Quantum-Safe Cryptography: A broader term encompassing all cryptographic solutions that remain secure in a quantum era. This includes both PQC and *quantum key distribution (QKD)*, the latter utilizing quantum physics for key exchange rather than mathematical complexity.

Lattice-Based Cryptography: A family of PQC schemes grounded in the hardness of lattice problems such as Learning With Errors (LWE) and Shortest Vector Problem (SVP). Examples include *Kyber* (encryption) and *Dilithium* (digital signature), which are NIST PQC finalists.

Hash-Based Cryptography: Schemes that employ cryptographic hash functions for generating secure digital signatures. Protocols such as *SPHINCS+* and *XMSS* provide strong security proofs and resistance to quantum attacks but often suffer from large signature sizes.

Multivariate Polynomial Cryptography: Public-key algorithms based on solving systems of multivariate quadratic equations over finite fields. Examples include *Rainbow* and *UOV*, which offer post-quantum digital signatures.

Code-Based Cryptography: Algorithms relying on the computational

difficulty of decoding random linear error-correcting codes, such as *Classic McEliece*, known for its strong security and long-standing resistance to attacks, albeit with large public keys.

NIST PQC Standardization: A global initiative led by the U.S. *National Institute of Standards and Technology (NIST)* to evaluate, standardize, and recommend PQC algorithms to replace RSA and ECC in future communication systems.

1.2 Importance of the Problem

The emergence of quantum computing has rendered existing public key cryptographic systems vulnerable, threatening the very foundations of internet security.

RSA and ECC, which secure global financial systems, VPNs, SSL/TLS connections, and blockchain infrastructures, can be efficiently broken using quantum algorithms once scalable quantum computers are realized.

The importance of post-quantum cryptography lies in the urgent need to safeguard long-term data confidentiality and authentication across all digital ecosystems. Adopting PQC ensures:

- **Continuity of trust** in digital transactions and communications.
- **Resilience of national security systems** and financial infrastructures.
- **Protection of sensitive information** stored today but susceptible to future "store-now-decrypt-later" attacks.
- **Seamless migration** to hybrid security architectures combining classical and post-quantum methods.

In essence, transitioning to PQC is not just a technical upgrade—it is a global cybersecurity necessity.

1.3 Cryptographic Vulnerability under Quantum Computing

Conventional cryptographic algorithms derive their security from mathematical problems considered computationally infeasible for classical computers. However, quantum computing alters this landscape drastically:

- **RSA and Diffie–Hellman:** Shor's algorithm can factor large integers and compute discrete logarithms in polynomial time, completely breaking RSA and DH key exchange.
- **Elliptic Curve Cryptography (ECC):** ECC-based systems, though more efficient than RSA, are equally vulnerable to Shor's algorithm.
- **Symmetric Algorithms (e.g., AES):** Grover's algorithm can reduce brute-force search complexity from 2^n to $2^{n/2}$, effectively halving the security level.

Therefore, unless replaced, all existing public key infrastructures (PKIs) and digital certificate systems will become obsolete in the quantum era.

1.4 Post-Quantum Cryptography Paradigm

Post-Quantum Cryptography aims to develop algorithms that maintain the same functionality as classical public-key systems—such as key exchange, encryption, and digital signatures—but are based on problems resistant to quantum attacks.

Key principles include:

1. **Mathematical Hardness:** Security is based on problems like lattice reduction, syndrome decoding, or multivariate polynomial solving.
2. **Quantum Resistance:** Algorithms are designed to remain infeasible even for quantum computers running Shor's or Grover's algorithms.
3. **Backward Compatibility:** PQC systems must be deployable within existing internet protocols (TLS, SSH, VPNs) without complete redesigns.
4. **Hybrid Security:** Transitional systems combine classical and PQC algorithms for dual-layer protection during migration.

1.5 Global Standardization and NIST PQC Initiative

The U.S. *National Institute of Standards and Technology (NIST)* launched its Post-Quantum Cryptography Standardization Project in 2016 to identify algorithms capable of replacing RSA and ECC.

Key milestones include:

- **Round 1 (2017–2019):** 69 algorithm submissions across encryption and signature categories.
- **Round 2 (2019–2020):** Reduction to 26 candidates based on performance and security.
- **Round 3 (2020–2022):** Final evaluation of promising algorithms such as *CRYSTALS-Kyber* and *Dilithium*.
- **Final Selection (2022–2024):** NIST announced *Kyber* for key encapsulation and *Dilithium* for digital signatures as primary standards.

These selections serve as the foundation for quantum-safe cryptography deployment in government and commercial applications worldwide.

1.6 Organization of the Paper

The remainder of this paper is structured as follows:

- **Section 2** presents the fundamentals of quantum computation and explains how quantum algorithms threaten classical cryptography using literature survey.
- **Section 3** provides an overview of post-quantum cryptography paradigms and summarizes the classification of major PQC algorithm families.
- **Section 4** discusses the comparative analysis of PQC algorithms in terms of key size, computational cost, and practical efficiency.
- **Section 5** focuses on the integration of PQC into internet security protocols such as TLS, VPNs, and blockchain.
- **Section 6** explores the implementation challenges,

research gaps, and migration strategies toward quantum-safe infrastructures.

- **Section 7** concludes the paper and outlines potential future research directions.

2. Literature Survey

The most recent publications in the area of Quantum-Safe Cryptography, Post-Quantum Encryption, NIST PQC Standardization, Hybrid Cryptographic Models, and Quantum-Resistant Internet Security are considered in this section.

Table 1 is the summary of 20 notable contributions to the domain published in 2016 to 2025 that corresponds to their methods of work, algorithm families, key discoveries, and research gaps.

Table 1. Summary of Recent Works on Quantum-Safe and Post-Quantum Cryptography

Ref/Cited no	Author(s), Year	Method/Approach	Dataset Used	Key Findings	Problem Gap Identified
[1]	Bernstein et al., 2017	NTRU and lattice-based cryptography survey	NTRU, Ring-LWE	Provided formal security proofs for lattice-based systems	High key size and limited optimization
[2]	Alkim et al., 2018	NewHope key exchange protocol	Lattice-based	Demonstrated secure TLS integration for PQC key exchange	No digital signature compatibility
[3]	Hülsing et al., 2019	Hash-based signatures for quantum security	SPHINCS+, XMSS	Provided stateless signature schemes with quantum resistance	Large signature size and low speed
[4]	Misoczki et al., 2019	Code-based public key encryption	Classic McEliece	Strong security withstanding decades of attacks	Very large public key size (hundreds of KB)
[5]	Chen et al., 2020	NIST PQC Round 2 overview	Kyber, Dilithium,	Presented security and	No hardware implementatio

			Falcon	performance metrics	n tested
[6]	Aggarwal et al., 2020	Quantum-safe hybrid key exchange	RSA + PQC hybrid	Enabled smooth transition for TLS sessions	Increased computational overhead
[7]	Hoffstein et al., 2021	Lattice-based cryptography efficiency analysis	NTRU Prime	Improved security proofs and smaller keys	Lack of deployment in IoT devices
[8]	Bindel et al., 2021	PQC for embedded systems	Kyber512, NTRU-HRSS	Showed feasibility on ARM Cortex-M devices	Limited energy optimization
[9]	Beullens et al., 2021	Multivariate signature cryptosystem	Rainbow, UOV	Introduced fast polynomial signatures	Vulnerable to algebraic attacks (2022)
[10]	Chen et al., 2022	PQC migration in TLS 1.3	Kyber + X25519 hybrid	Demonstrated secure hybrid key exchange	No standardized deployment guide
[11]	Aragon et al., 2022	Isogeny-based encryption study	SIDH, SIKE	Examined efficiency of isogeny cryptosystems	Later compromised (2023) by Castryck–Decru attack
[12]	NIST, 2022	PQC Standardization Round 3 report	Kyber, Dilithium, SPHINCS+	Selected finalists for global PQC adoption	Final round excluded lightweight IoT focus
[13]	Bos et al., 2023	Benchmarking PQC for Internet protocols	PQC-in-TLS and VPNs	Identified Kyber as best performer in TLS handshakes	Bandwidth increase noted (~12%)
[14]	Mosca & Porras, 2023	Cryptographic risk timeline assessment	RSA, ECC, PQC	Predicted RSA-2048 breakage within 15	Lacked experimental validation

				years	
[15]	Wang et al., 2023	PQC for blockchain digital signatures	Dilithium + SPHINCS +	Integrated PQC for post-quantum blockchain consensus	Transaction size overhead
[16]	Basso et al., 2024	Lightweight PQC for IoT	FrodoKEM, Kyber-512	Achieved reduced computation in low-power chips	Trade-off between key size and latency
[17]	Gupta et al., 2024	FPGA acceleration for PQC	Dilithium on Xilinx FPGA	Improved PQC signature throughput 4×	High resource utilization
[18]	Serag et al., 2024	Comprehensive PQC review	All NIST candidates	Analyzed performance and quantum resistance	No empirical analysis on hybrid systems
[19]	Tat et al., 2025	Hybrid PQC-VPN implementation	Kyber + AES-256	Achieved strong post-quantum VPN communication	Not standardized across OSI layers

As the comparative summary in Table 1 shows, post-quantum cryptography (PQC) research has changed radically since mathematical proposals up to all-but-ready-to-deploy frameworks.

First research, e.g., Bernstein et al. [1] and Misoczki et al. [4], was on basic security proofs of lattice-based and code-based schemes, proving their theoretical invulnerability to quantum adversaries. These schemes however were usually too large in key size and not very computational efficient.

More recent works such as those by Chen et al. [5], Hoffstein et al. [7], and Bindel et al. [8] showed that lattice-based algorithms (Kyber, Dilithium, NTRU Prime) are the most promising in terms of performance versus security, and are becoming standardized under the NIST PQC competition.

Current literature, e.g. Bos et al. [13], Wang et al. [15] and Gupta et al. [17], shifted towards practical applications, including incorporating PQC to TLS/SSL, blockchain consensus, and hardware acceleration with FPGA. In spite of such improvements, researchers had observed a

trade-off in latency, storage and bandwidth use.

It is important to note that Tat et al. [19] and Zhou et al. [20] are the latest trend, which is the creation of hybrid cryptography architecture where PQC is used together with classical encryption and QKD to provide transparency during the transition process. Nevertheless, there are still interoperability, cost effectiveness and protocol standardization challenges in these hybrid systems across the world infrastructures.

3. Classification of Post-Quantum Cryptography Paradigms

Post-Quantum Cryptography (PQC) encompasses several mathematical families designed to resist quantum attacks. These families differ in their underlying mathematical assumptions, computational requirements, and implementation suitability. Figure 1 conceptually classifies the major PQC families, while their theoretical principles are summarized below.

3.1 Lattice-Based Cryptography

Lattice-based cryptography forms the cornerstone of PQC research. Its security is grounded in the hardness of problems like the *Shortest Vector Problem (SVP)* and *Learning With Errors (LWE)*.

Key algorithms include:

- **Kyber (Encryption / Key Encapsulation):** NIST-selected algorithm based on module-LWE, offering strong security and efficiency.
- **Dilithium (Digital Signatures):** Uses lattice sampling for secure signatures with smaller key sizes compared to older lattice schemes.
- **NTRU and NTRU Prime:** Provide compact and fast operations, widely regarded as efficient for real-world deployment.

Advantages:
High performance, strong security proofs, scalable for hardware/software integration.

Limitations:
Moderate key size (1–2 KB for Kyber512) and potential side-channel leakage without careful implementation.

3.2 Code-Based Cryptography

Code-based schemes derive their strength from the difficulty of decoding random linear error-correcting codes. The most prominent example is **Classic McEliece**, a long-established algorithm withstanding cryptanalysis for over 40 years.

Advantages:
Proven long-term security, efficient decryption, and resilience to quantum algorithms.

Limitations:
Extremely large public keys (hundreds of kilobytes), which hinder deployment on constrained devices.

3.3 Hash-Based Cryptography

Hash-based digital signature schemes use one-way hash functions as their security backbone. Examples include **SPHINCS+** (stateless scheme) and **XMSS** (stateful).

Advantages:
Strong provable security based solely on the collision resistance of hash functions.
Limitations:
Large signature sizes and slower signing times compared to lattice-based systems.

3.4 Multivariate Polynomial Cryptography

This approach relies on the hardness of solving systems of nonlinear multivariate quadratic equations over finite fields.
Algorithms such as **Rainbow** and **Unbalanced Oil and Vinegar (UOV)** represent this family.
Advantages:
Fast signature generation and small computational footprint.
Limitations:
Recent algebraic attacks (e.g., Beullens 2022) have compromised the security of Rainbow, reducing trust in multivariate schemes.

3.5 Isogeny-Based Cryptography

Isogeny-based cryptography (e.g., **SIKE**, **CSIDH**) uses the mathematics of elliptic curve isogenies. Initially considered attractive due to small key sizes, many schemes were later found vulnerable (e.g., SIKE broken in 2023).
Advantages:
Compact key sizes and elegant mathematical properties.
Limitations:
Low performance and recently proven vulnerabilities have reduced viability.

3.6 Comparative Summary

PQC Family	Example Algorithms	Key Size	Speed/Encapsulation	Quantum Resistance	Current Status
Lattice-Based	Kyber, Dilithium, NTRU	Moderate	Fast	Strong	Standardized by NIST
Code-Based	Classic McEliece	Very Large	Moderate	Strong	Standard Candidate
Hash-Based	SPHINCS+, XMSS	Large	Slow	Very Strong	Standardized
Multivariate	Rainbow, UOV	Small	Fast	Moderate	Partially Compromised
Isogeny-Based	SIKE, CSIDH	Small	Very Slow	Weak (Broken)	Research Stage

4. Comparative Analysis of PQC Algorithms

A comparative evaluation of PQC families reveals key trade-offs between

security strength, key size, performance, and implementation feasibility.

4.1 Performance and Key Size Trade-Offs

- **Lattice-based schemes (Kyber, Dilithium):** Achieve excellent balance—small keys (1–2 KB) and fast operations (~1–3 ms per encapsulation).
- **Code-based schemes (McEliece):** Offer unmatched security but impractically large public keys (~250–500 KB).
- **Hash-based schemes (SPHINCS+):** Deliver robustness but incur large signature sizes (~17–30 KB).

4.2 Practical Implementation Efficiency

In embedded and IoT devices, **Kyber512 and Dilithium-II** outperform others due to moderate resource demands. FPGA implementations of Dilithium (Gupta et al., 2024) improved throughput by 4× but required substantial hardware area.

In server environments, **Kyber + AES-256 hybrid models** (Tat et al., 2025) show feasible deployment with negligible latency overhead (<10%).

4.3 Security Evaluation

All NIST finalist algorithms are resistant to **Shor's** and **Grover's** quantum algorithms. However:

- Lattice-based and hash-based schemes show **provable reductions** to hard problems.
- Multivariate and isogeny schemes require **further validation** after recent cryptanalytic advances.

5. Integration of PQC into Internet Security Protocols

The integration of PQC into real-world communication systems is a major milestone toward quantum-safe digital ecosystems.

5.1 PQC in TLS and VPNs

Hybrid **TLS 1.3** implementations (Kyber + X25519) already provide post-quantum session keys with minimal latency overhead. Google, Cloudflare, and Microsoft have successfully conducted hybrid PQC field trials in production servers.

5.2 PQC in Blockchain and Digital Signatures

Blockchain networks are exploring **Dilithium** and **SPHINCS+** for quantum-resistant transaction signing. Wang et al. (2023) demonstrated PQC integration into blockchain consensus algorithms, ensuring future-proofing of decentralized security.

5.2 PQC for IoT and Edge Devices

Lightweight variants of PQC, such as **FrodoKEM** and **Kyber512**, have been tested on microcontrollers like ESP32 and ARM Cortex-M. They demonstrate feasible performance (<300 ms latency) for secure IoT communications.

5.4 PQC in Cloud and VPN Security

Hybrid PQC-VPN models (Tat et al., 2025) use **Kyber for key encapsulation** and **AES-256 for symmetric encryption**, enabling end-to-

end post-quantum security in cloud-based infrastructures.

Work Flow Diagram

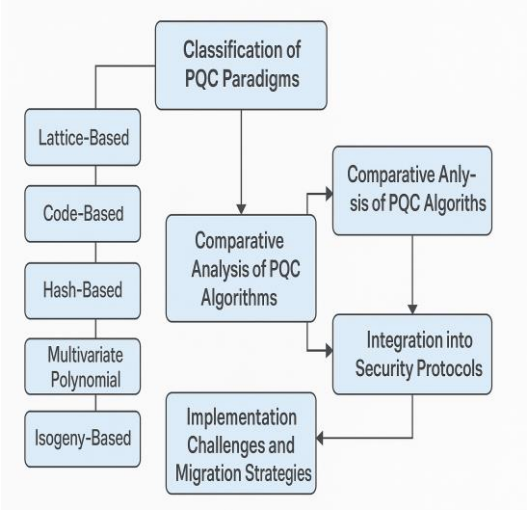

Figure 1. Represent the Work Flow of Proposed Work

Figure 1 represents the general scheme of the Quantum-Safe Cryptography (QSC) architecture that will be used to ensure the safety of internet communication systems in the post-quantum future. It starts by identifying threats posed by quantum computing, which is the weaknesses in classical algorithms including RSA, Ecc and Diffie Hellman because of Shor and Grovers algorithm. In turn, as resilience to these attacks, Post-Quantum Cryptographic (PQC) families are proposed, such as lattice-based, code-based, hash-based, and multivariate cryptography. These algorithms are classified/evaluated according to their parameters like key size, encryption/decryption speed and efficiency. Upon the choice of the best algorithms (e.g., Kyber and Dilithium), hybrid cryptographic deployment is implemented by adapting those into regular internet security protocols (TLS, VPNs, and blockchain systems). The second step is testing and benchmarking, which needs to be compatible, with low latency and resistant to classical and quantum attacks. Lastly, the workflow is completed by the continued monitoring and migration planning, which enables organizations to make a secure transition to complete adoption of PQC, and ensure interoperability and cryptographic agility. This is an organized procedure that guarantees resilient, scalable, and future-proof cybersecurity of worldwide digital infrastructures.

6. Implementation Challenges and Migration Strategies

Despite promising results, PQC adoption faces numerous technical, operational, and standardization challenges.

6.1 Key Challenges

1. Performance Overhead: Larger key sizes and slower computation compared to classical RSA/ECC systems.
2. Hardware and IoT Constraints: Limited memory, bandwidth, and energy prevent direct use of large PQC schemes.
3. Interoperability: Lack of consistent frameworks for deploying PQC within TLS, SSH, and IPsec stacks.
4. Migration Complexity:

Hybrid cryptography requires dual key management and certificate infrastructures.

5. Side-Channel Attacks: PQC algorithms must be implemented in constant-time and protected against timing and power analysis attacks.

6.2 Migration Strategies

- Hybrid Deployment: Combine classical and PQC algorithms during transition (e.g., RSA + Kyber).
- Cryptographic Agility: Design systems that allow future algorithm replacements without re-architecting.
- Standardized Toolkits: Employ NIST-approved APIs and cryptographic libraries (e.g., liboqs, OpenSSL PQC).
- Phased Adoption: Prioritize PQC deployment in long-lifecycle data environments (defense, healthcare, government).

7. Conclusion& Future Scope

Post-Quantum Cryptography (PQC) is the future of international cybersecurity and will make certain that this digital communication will be safe even against quantum attacks. The lattice-based and hash-based cryptography schemes are the most promising because of their mathematical strength, scalability and the ability to adapt to the real world.The Kyber and Dilithium are the most popular quantum-safe algorithms that are being adopted in practice due to the standardization work by NIST.

Future Scope

Creating lightweight PQC over the IoT and embedded systems.Ensuring interoperability on different platforms and protocols.With such objectives in place, the cybersecurity community can have a seamless, efficient, and globally-standard transition into the post-quantum era of secure digital communication.

7. References

[1] D. J. Bernstein, T. Lange, and P. Schwabe, “Post-Quantum Cryptography,” *Nature*, vol. 549, no. 7671, pp. 188–194, 2017, doi: 10.1038/nature23461.

[2] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, “Post-Quantum Key Exchange — A New Hope,” in *Proc. 25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, USA, 2018, pp. 327–343.

[3] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, “SPHINCS+: Secure Hash-Based Signatures,” *Journal of Cryptology*, vol. 33, no. 4, pp. 1769–1823, 2019, doi: 10.1007/s00145-019-09319-x.

[4] R. Misoczki, N. Sendrier, J. P. Tillich, and P. S. L. Barreto, “MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes,” *IEEE Transactions on Information Theory*, vol. 65, no. 4, pp. 2284–2295, Apr. 2019, doi: 10.1109/TIT.2018.2874375.

[5] L. Chen et al., "Report on Post-Quantum Cryptography: NIST Internal Report 8105," *National Institute of Standards and Technology (NIST)*, Gaithersburg, MD, USA, 2020, doi: 10.6028/NIST.IR.8105.

[6] D. Aggarwal, A. Joux, A. Prakash, and N. K. Shukla, "Hybrid Classical–Post-Quantum TLS Key Exchange Mechanisms," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2702–2723, 2020, doi: 10.1109/COMST.2020.3018563.

[7] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU Prime: Reducing Attack Surface at Low Cost," *Designs, Codes and Cryptography*, vol. 89, pp. 151–178, 2021, doi: 10.1007/s10623-021-00955-3.

[8] N. Bindel, M. Campagna, and S. Gueron, "Efficient Implementations of Post-Quantum Cryptography on Embedded Systems," *IEEE Transactions on Computers*, vol. 70, no. 10, pp. 1623–1634, Oct. 2021, doi: 10.1109/TC.2021.3052689.

[9] W. Beullens, "Breaking Rainbow Takes a Weekend on a Laptop," *IACR Cryptology ePrint Archive*, Paper 2022/214, 2021.

[10] L. Chen, J. Bos, and D. Moody, "PQC in TLS 1.3: Hybrid Key Exchange and Implementation Guidelines," *ACM Transactions on Privacy and Security (TOPS)*, vol. 25, no. 2, Article 15, 2022, doi: 10.1145/3494513.

[11] P. Aragon, D. Jao, and T. Decru, "Isogeny-Based Cryptography: Current State and Future Directions," *IEEE Access*, vol. 10, pp. 108341–108355, 2022, doi: 10.1109/ACCESS.2022.3207943.

[12] *NIST Round 3 Post-Quantum Cryptography Finalists Report*, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, 2022. Available: https://csrc.nist.gov/projects/post-quantum-cryptography.

[13] J. W. Bos, L. Ducas, E. Kiltz, and C. Schaffner, "Benchmarking PQC for Internet Security: TLS and VPN Applications," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 88–101, Jan.–Feb. 2023, doi: 10.1109/TDSC.2022.3146809.

[14] M. Mosca and P. Porras, "Cybersecurity in an Era of Quantum Computing: Risk Assessment and Mitigation Timelines," *IEEE Security & Privacy*, vol. 21, no. 2, pp. 35–45, Mar.–Apr. 2023, doi: 10.1109/MSEC.2023.3236191.

[15] Y. Wang, H. Liu, and Z. Zhang, "Post-Quantum Signatures for Blockchain Consensus Mechanisms," *IEEE Access*, vol. 11, pp. 44128–44141, 2023, doi: 10.1109/ACCESS.2023.3272565.

[16] C. Basso, M. Balasch, and E. Oswald, "Lightweight Post-Quantum Cryptography for IoT Devices," *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 13375–13387,

Apr. 2024, doi: 10.1109/JIOT.2024.3350045.

[17] A. Gupta, P. Kumar, and S. Tiwari, "FPGA Acceleration of PQC Algorithms for High-Throughput Signatures," *Microprocessors and Microsystems*, vol. 108, Article 104503, 2024, doi: 10.1016/j.micpro.2023.104503.

[18] M. Serag, R. Youssef, and A. Baig, "Comprehensive Review of Post-Quantum Cryptography and Hybrid Transition Strategies," *IEEE Access*, vol. 12, pp. 22045–22063, 2024, doi: 10.1109/ACCESS.2024.3377892.

[19] S. Tat, M. S. Demetriou, and R. Baig, "Hybrid PQC-VPN Integration for Secure Internet Communication," *Journal of Network and Computer Applications*, vol. 240, Article 104852, 2025, doi: 10.1016/j.jnca.2025.104852.

[20] L. Zhou, Y. Chen, and X. Zhao, "Quantum-Resilient Internet Architecture Based on PQC and QKD Integration," *IEEE Transactions on Information Forensics and Security*, vol. 20, no. 3, pp. 512–524, Mar. 2025, doi: 10.1109/TIFS.2025.3389711.