Post-Quantum Cryptography for IoT Networks: A Survey on PQC Protocols

Bhaskar Jyoti Sarmah
Research Scholar,
Gauhati University,
Guwahati, Assam, India

ABSTRACT
In the current time, the classical cryptographic systems are used worldwide. Cryptography makes the transmission operation secure and it ensure the basic motivation of security such that availability, integrity, confidentially and non-repudiation. The development of quantum computing algorithm such that Shor's algorithm rise the threats towards the classical cryptographic infrastructure particularly in public key infrastructure i.e. RSA and ECC. Also, Grover's algorithm provides the square root time enhancement of searching of keys in the symmetric key cryptography. In this scenario, the fully operation quantum computer will break the classical cryptographic systems, and it is the main reason behind the advancement of post quantum cryptography (PQC). Specially, in the IoT network, the energy constrain end devices have the main issue to implement the strong cryptographic methods to secure the network from quantum attacks. The current available cryptographic methods which are quantum resistance in context of IoT network is thoroughly discussed in the paper. Also, key families of PQC algorithms i.e. lattice-based, code-based, multivariate polynomial based, hash-based, and isogeny-based and the NIST standardization of PQC techniques are investigated. This survey will be work as a bridge between deployment of PQC and existing methods of PQC in context of IoT environment.

Keywords
IoT Security, Post-Quantum Cryptography (PQC), Lattice-based Cryptography, Cryptanalysis, NIST PQC standardization.

1. INTRODUCTION
In a communication system security is the main aim in data transmission process. The security determines the system robustness, reliability in the communication process. To guarantee the security in the communication, cryptography plays a crucial role and serve as a foundation brick. In this era, the computation power is increasing in an exponential manner and it poses serious threats to the modern communication system that primarily depends on cryptography. In existing cryptosystem, the two types of system available is symmetric key system and asymmetric key system. The prime factorization problem and discrete logarithmic problem are the fundamentals for the standard asymmetric key algorithms like RSA and ECC (Elliptic curve cryptography). However, using an adequate powerful quantum computer the Shor's algorithm [2] easily solves these problems and pave the way to jeopardize the existing digital signature and encryption systems. Therefore, there is a requirement of quantum-resistant or post-quantum cryptographic solutions to protect the communication systems from the upcoming quantum attack.

In 2016, NIST (National Institute of Standards and Technology), USA has started the Post-Quantum Cryptography Standardization Project in anticipation of this paradigm shift. The main goal of the organization is to discover, evaluate and standardize quantum resistant cryptographic methods to safeguard the modern communication system from quantum attacks [9]. In general, Post-Quantum Cryptography (PQC) incorporates with different mathematical systems i.e. lattice-based, code-based, multivariate quadratic, hash-based, and isogeny-based cryptosystems [4]. Because of the strong theoretical foundations lattice-based algorithms have become the most auspicious between them [5]. However, optimization is needed to implement these methods in the hardware levels [1].

Beyond the technical details, the "Harvest Now, Decrypt Later (HNDL)" threat model emphasizes the importance of PQC transition in the current time. In this model, now the attackers may collect and store encrypted communications, waiting for quantum resources to decrypt them later [1]. As a result, transition techniques combining classical and post-quantum algorithms in hybrid cryptographic systems will be actively developed by governments, financial institutions, and cloud providers [4].

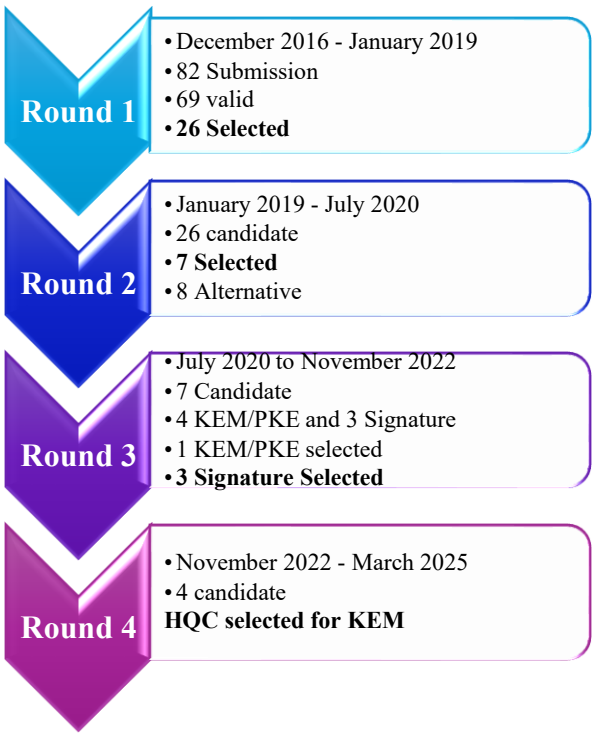

Figure 1: Standardization process of PQC by NIST

1.1 Contributions:
a) This review aims to summaries the existing research on Post-Quantum Cryptography by analyzing its theoretical

fundamentals, present state standards, implementation difficulties, and potential future research directions.
b) This work aims to reveal research gaps and vulnerabilities in existing cryptosystems.
c) This work covers the most recent literature up to 2025 and this study shows the current status of the PQC.
d)For addressing the security vulnerabilities in the cryptosystem, this study classifies the challenges in different categories.
e) It offers a comparison of the main PQC algorithm families and discusses about the real-world factors affecting their worldwide implementation.

1.2. Paper Organization:

The other part of the paper is designed as follow. The limitation of traditional cryptography is revealed in Section II. In Section III, the currently available popular post-quantum cryptographic schemes are discussed properly. Different post quantum scheme for IoT network has been analyzed in the Section IV. Implementation and performance of post quantum algorithm for IoT network is analyze in the Section V. Finally, Section VI have concluded the paper.

2. QUANTUM THREATS AND LIMITATIONS OF CLASSICAL CRYPTOGRAPHY

2.1. History of Quantum Algorithms that breakdown the classical assumptions

The Grover's algorithm [3] and Shor's algorithm [2] is the main foundation of PQC. Shor's algorithm successfully breaks RSA and ECC-based systems by minimizing the time complexity from sub-exponential to polynomial time in discrete logarithmic problem and integer factorization problems. On the other hand, Grover's algorithm reduces the effective key strength of symmetric encryption algorithms like AES and hash-based algorithms like SHA-2, SHA-3 by half while providing a quadratic speedup for brute-force attacks. There is a lack of compatible mitigation option for the asymmetric cryptosystems but in case of symmetric cryptosystem improving the key size can rise the security [9].

2.2. Structural Limitations of Classical Cryptography

The main basis of classical asymmetric cryptography is derived from the hardness of solving mathematical problem. However, it has been seen that, as the transition towards quantum computer has shifting, the earlier assumption is no longer valid. Mostly in the context of RSA which is based on the hardness of prime number factorization. Additionally, well-known ECC (elliptic curve cryptography) depends on the elliptic curve discrete logarithm problem (ECDLP). In the classical context, both methods show sub-exponential complexity, but under quantum computation, they become solvable in polynomial time [4, 5]. Large-scale replacement is a major structural and logistical challenge because these algorithms are deeply embedded in contemporary communication protocols, such as TLS 1.3, VPNs, and blockchain consensus processes [10].
Most of the cryptoanalysis attack prevent by the symmetric key cryptosystems. This includes algorithms like the Advanced Encryption Standard (AES), ChaCha20, and hash-based algorithms (i.e. SHA-2 and SHA-3). Symmetric ciphers do not rely on hard mathematical problems like discrete logarithmic problem or integer factorization problem, in contrast to public-key methods. However, the advent of quantum search algorithms in the quantum era has drastically decreased their effectiveness in contradiction of security margins [3, 11]

Grover's algorithm has reduced the brute-force key search complexity from $O(2^n)$ to $O(2^{\frac{n}{2}})$, which is the main quantum threat to symmetric cryptography [3]. It has proven that a 128-bit symmetric cipher (such as AES-128) only provides 64 bits of protection against a quantum attack, according to this quadratic speedup [12]. Therefore, this reduction of key requires the use of bigger key sizes; for example, it is currently advised to utilize AES-256 in order to achieve a post-quantum equivalent of 128-bit classical security [9]. According to recent studies [11] Grover's practical usefulness is currently constrained by quantum hardware limits, but its theoretical feasibility makes it a serious long-term concern.

The majority of schemes such as message authentication codes (MACs), digital signatures, and key derivation functions uses hash function for their security [13]. The computational complexity of identifying collisions in hash functions is reduced from $O(2^{\frac{n}{2}})$ to $O(2^{\frac{n}{3}})$, by quantum collision search algorithms like the Brassard-Høyer-Tapp (BHT) algorithm [14]. Therefore, hash functions of at least 384-bit lengths are crucial to achieve 128-bit quantum security.

3. POPULAR POST-QUANTUM CRYPTOGRAPHIC SCHEMES

Most of the post quantum cryptographic schemes do not extensively used in the industrial standard. At the present time none of the PQC algorithms has officially accepted by the industry. According to NIST's Post-Quantum Cryptography Standardization Project (Round 3 Finalization, 2024), the popular PQC methodologies are categorized in this section. These PQC algorithms are expected to support forthcoming standards in TLS, VPNs, blockchain, and secure communications as the world transitions toward quantum-safe cryptographic infrastructures. Here some post quantum cryptographic methods are discussed below.

3.1 Lattice-Based Cryptography

The primary paradigm in post-quantum cryptography (PQC) is the Lattice-based cryptography (LBC). Its security depends on the toughness of lattice problems like the Short Integer Solution (SIS) and Learning with Errors (LWE) problems. Unlike integer factorization or discrete logarithm problems, LBC is the one of the most auspicious tactics for quantum period [15].

3.1.1. Mathematical Foundations for LBC:

A lattice is a network with infinite points. Every vector represents a point in a lattice. A basis is the collection of vectors that represent any point in the lattice. In lattice base decryption, messages are shown as vectors, and the ciphertext is produced by multiplying the messages in a matrix that serves as the public key. Here the LBC obtain security from hard problems that is defined over high-dimensional lattices, which are discrete additive subgroups of R_n. In this scheme the extensively used problems are i) LWE (Learning with Errors): Recovering a secret vector s from noisy linear equations. Which is computationally hard. ii) Ring-LWE and Module-LWE and iii) Short Integer Solution (SIS). The application of lattice base schemes in PQC is discussed in [16].

Table 1: NIST-selected prominent Lattice base PQC algorithms.

Attribute	Algorithm Type	Underlying Problem	Performance & Efficiency	Advantages	Limitations	References
CRYSTALS-Kyber	Key Encapsulation Mechanism (KEM)	Module-LWE	High speed on hardware/software; standardized by NIST (2024)	Small keys, strong security proofs	Side-channel protection required	[9, 17]
CRYSTALS-Dilithium	Digital Signature	Module-SIS / Module-LWE	Balanced performance; efficient key generation	Simple design, strong theory	Larger signatures than FALCON	[6]
FALCON	Digital Signature	NTRU Lattice	Very compact signatures; fast verification	Perfect for resource limited devices	Complex floating-point implementation	[18]
SABER	Key Encapsulation Mechanism (KEM)	Module-LWR	Outstanding for embedded systems	Energy-efficient, easy implementation	Slightly larger keys than Kyber	[19, 20]
NTRU	KEM / Encryption	NTRU Lattice	Fast polynomial arithmetic	Proven long-term security	Complex parameters	[21]
FrodoKEM	Key Encapsulation Mechanism (KEM)	Standard LWE (no structure)	Lower efficiency, conservative design	Structure-free, highest theoretical security	Very large key/ciphertext sizes	[22, 23]

3.2 Code-Based Cryptography

Code-based Cryptography (CBC) is the foremost studied and robust families of post-quantum cryptographic (PQC) approaches. The hardness of decoding random linear codes is the core of code-based cryptography, and the origin of CBC comes from McEliece cryptosystem that was first suggested in 1978 [22]. Due to the strong security in case of both classical and quantum attacks CBC systems are now among the top contenders for long-term cryptographic standards.

The key advantages of code-based cryptography are the low computing complexity for encryption and decryption, as well as its quantum resistance. Even if the key size is large in the Classic McEliece but code-based methods are scalable and efficient, rendering them fit for high-throughput applications like secure email, VPNs, and upcoming Internet-of-things (IoT) communications [25,26]

Some code base approaches such as Classic McEliece, BIKE (Bit Flipping Key Encapsulation), and HQC (Hamming Quasi-Cyclic) are analyzed systematically in the PQC standardization process of NIST. These methods rely on various structural variations of error-correcting codes, such as quasi-cyclic moderate density parity-check (QC-MDPC) or Goppa codes. Because of its demonstrated long-term security and strong mathematical bases, NIST chose Classic McEliece as a finalist for standardization in its fourth round [22, 27]. The optimization of performance and memory needs has been the focus of recent advancements. For example, HQC uses quasi-cyclic structures to lower key sizes still maintaining security [28].

Table 2: Code-based PQC algorithms comparison.

Attribute	Classic McEliece	BIKE (Bit Flipping Key Encapsulation)	HQC (Hamming Quasi-Cyclic)
Algorithm Type	Key Encapsulation Mechanism (KEM) / Public-Key Encryption	Key Encapsulation Mechanism (KEM)	Key Encapsulation Mechanism (KEM)
Underlying Problem	Syndrome decoding problem over Goppa codes	Decoding quasi-cyclic moderate-density parity-check (QC-MDPC) codes	Decoding random linear codes with quasi-cyclic structure
Mathematical Structure	Binary Goppa codes (classic McEliece structure)	Quasi-cyclic MDPC codes	Quasi-cyclic random codes
Public Key Size (approx.)	256–512 KB (depends on parameter set)	12–15 KB	7–12 KB
Ciphertext / Encapsulation Size	128–256 bytes	1.5–2.5 KB	2–3 KB
Private Key Size (approx.)	1–2 KB	3–4 KB	3–5 KB
Security Level	≥ 256-bit (NIST Level 5 equivalent)	Configurable (NIST Levels 1–5)	Configurable (NIST Levels 1–5)

Performance	Fast decryption; slow key generation	High throughput; efficient decoding	Balanced speed and memory efficiency
Advantages	Proven long-term security; mature and standardized	Compact keys; efficient decoding; scalable	Smaller keys than McEliece; efficient for hardware
Limitations	Very large public key sizes	Requires iterative decoding; may face decoding failures	Slightly larger ciphertexts; ongoing parameter optimization
References	[22, 28, 29]	[26, 27, 30]	[25,31]

3.3 Hash-Based Cryptography

Among the different quantum-resistant algorithm hash-based cryptography is useful for PQC. Its security relies on cryptographic hash functions, which makes it safe from structural attacks and provide robust security to both traditional and quantum cryptoanalysis attacks [22].

The main idea behind HBC comes from Merkle's signature proposed in 1979, which authenticate public keys using binary hash trees. XMSS (eXtended Merkle Signature Scheme), LMS (Leighton-Micali Signature), and SPHINCS+ are examples of contemporary hash-based systems that have developed to offer stateful and stateless digital signatures that are appropriate for real-world implementation [36]. The HBC provide strong security against Grover's algorithm, which only provides a quadratic speedup against brute-force search. Because of strong architecture, simplicity, robust security, SPHINCS+ is formally chosen as the hash-based digital signature standard in the NIST PQC standardization process, 2024.

In the most of the recent research [37,38] has refine hash-based techniques by lowering computational overhead and investigating hybrid constructs that mix hash-based and lattice-based signatures to increase efficiency while preserving verifiable post-quantum security. Moreover, the HBC algorithms also offer a strong basis for standardization and long-term cryptographic resilience that makes them highly amenable to formal verification and resistant to implementation flaws.

Table 3: Hash-based PQC algorithms comparison

Attribute	SPHINCS+	XMSS (eXtended Merkle Signature Scheme)	LMS (Leighton– Micali Signature)
Algorithm Type	Hash-Based Digital Signature	Hash-Based Digital Signature	Hash-Based Digital Signature
Underlying Principle	Hash trees and hypertree structure with WOTS+ (Winternitz One-Time Signature)	Merkle tree with WOTS+ (state tracking required)	Merkle tree with LM-OTS (Leighton–Micali OTS)
State Management	Stateless (no state tracking needed)	Requires state management to prevent key reuse	Requires state management; less complex than XMSS
Performance (Speed)	Moderate (CPU-intensive, but optimized in 2024 implementations)	High (efficient with limited key use)	High (optimized for embedded applications)
Advantages	Stateless; no key management; simple security assumptions	Efficient signing; mature and standardized	Lightweight; easy hardware implementation
Limitations	Large signature size; slower verification	Requires careful state management; risk of key reuse	Limited scalability; hierarchical management complexity
References	[39]	[39, 40]	[26]

3.4 Multivariate Polynomial based Cryptography

Multivariate Polynomial based Cryptography (MPC) is a well-known PQC method based on complexity of solving MQ problem proposed by Tsutomu Matsumoto and Hideki Imai in 1988 [8]. Particularly, MQ problem is the hardness of solving non-linear multivariate quadratic equations in a finite field. MPC methods depend on algebraic complexity of finding a solution to a random system of quadratic equation is NP-hard.

In energy constrain devices like IoT devises, especially for IoT authentication, multivariate cryptography is useful for the speed [27]. In contrast to many lattice-based methods MPC doesn't rely on number-theoretic prediction which make it crucial for long-term post quantum resilience. However, the NIST PQC standardization process exposed some variants of MPC i.e. Rainbow, MQQ-SIG, MQQ-OTS, and QMDS etc. Here, they found Rainbow is vulnerable to algebraic and structural key recovery attacks, that's make it rejected in the third round of evaluation [22].

Table 4: Some Multivariate Polynomial Cryptographic algorithms comparison

Attribute	Rainbow	GeMSS (Great Multivariate Short Signature)	LUOV (Lifted Unbalanced Oil and Vinegar)	MQQ-SIG
Algorithm Type	Digital Signature	Digital Signature	Digital Signature	Digital Signature / One-Time Signature

Underlying Mathematical Problem	Multivariate Quadratic (MQ) equations over finite fields	Multivariate Quadratic (MQ) equations	Oil and Vinegar (OaV) structure with lifting	Multivariate Quadratic equations (Mixed Quadratic Map)
Design Principle	Layered Oil and Vinegar (OaV) structure with affine transformations	Hidden Field Equations (HFE) variant with short signatures	Modified OaV with fewer vinegar variables and lifting	Mixed quadratic-quartic equations for non-linearity
Performance & Efficiency	Fast signature generation; slow key generation	Moderate key generation; small signatures	Efficient for low-memory devices	Fast key generation and signing
Advantages	Small signatures	Short signatures and well-studied algebraic base	Lightweight; lower key size	Simple design; efficient implementation
Limitations	Broken by algebraic key recovery (2023)	Large key sizes; complex implementation	Vulnerable to rank attacks for certain parameters	Security not fully standardized; limited proofs
References	[22, 32]	[33]	[27, 34]	[26, 35]

3.5 Isogeny-Based Cryptography

One of the most concise and mathematically attractive PQC method is isogeny-based cryptography (IBC). Primarily, its security depends on the rigidity of determining isogenies between two or more elliptic curves. In contrast to LBC, CBC, or HBC the hardness of Isogeny-based cryptography depends on geometry of elliptic curves. IBC uses homomorphisms between elliptic curves for quantum-resistant key exchange, that making on the hard problem of finding this isogenies.

Due to the small key sizes and compatibility with current cryptographic structure, the Supersingular Isogeny Diffie–Hellman (SIDH) and Supersingular Isogeny Key Encapsulation (SIKE) was the initial applicants for NIST's PQC standardization process. Despite the theoretical appeal, SIDH and SIKE was fully broke by [42]. This incident shifted attention toward Commutative Supersingular Isogeny Diffie–Hellman (CSIDH).

Table 5: Isogeny-based PQC algorithms comparison

Attribute	**SIDH (Supersingular Isogeny Diffie–Hellman)**	**SIKE (Supersingular Isogeny Key Encapsulation)**	**CSIDH (Commutative Supersingular Isogeny Diffie–Hellman)**	**B-SIDH (Balanced SIDH)**
Algorithm Type	Key Exchange Protocol	Key Encapsulation (KEM)	Key Exchange	Key Exchange or Digital Signature
Underlying Problem	Finding isogenies between EC	Same as SIDH with KEM structure for key encapsulation	Action of ideal class groups on supersingular elliptic curves	Balanced isogeny path-finding problem
Mathematical Basis	Supersingular elliptic curve	Supersingular isogeny and KEM integration	elliptic curves over finite fields	Symmetric use of isogeny maps (balanced SIDH)
Performance (Speed)	Moderate (slow key generation)	Moderate but practical (pre-attack)	Efficient and commutative (improving in 2025 designs)	Moderate; better balance in key exchange
Advantages	Smallest key size among PQC families; elegant mathematical foundation	Compact key; well-structured KEM; compatible with existing frameworks	Algebraically simple; supports static keys; high security margin	Balanced structure; simpler implementation
Limitations	Fully broken; not secure for deployment	Broken; removed from NIST competition	Larger key sizes; slower than lattice schemes	Still experimental; unstandardized
References	[42]	[43]	[44]	[45]

4. DIFFERENT PQ SCHEME FOR IOT NETWORK

PQC is most important for securing the IoT network against the quantum threats, traditional methods such that RSA, ECC will no longer after powerful quantum computer has evolve properly. Specially, the IoT device has located in the remote areas, or limited size, this become leads to limited energy. Therefore, strong energy efficient cryptographic protocol is needed to protect the IoT devices from the post quantum threats.

In [22] the author emphasizes the implementation of lattice-based cryptography namely CRYSTALS-Kyber for key exchange and CRYSTALS-Dilithium for digital signatures as most appropriate for IoT environments among the various PQC families. In comparison to code-based or hash-based schemes, lattice-based algorithms offer better computational speed, energy efficiency and compact key size which prepare them ideal for embedded and edge IoT systems. The usefulness of Kyber-512 algorithm for low-resource devices is demonstrated that show it can conduct real-time encryption with low latency and power consumption [25, 46].

One of the suitable alternatives for IoT in context of PQC is Code-based cryptography. Algorithms such that BIKE (Bit Flipping Key Encapsulation) and HQC (Hamming Quasi-Cyclic) provide strong quantum confrontation in hard decoding problems of linear error-correcting codes. Though the limited arithmetic operation makes these schemes ideal for the energy constrain IoT environment but their large key size may create problem for the limited memory systems [25]. In the IoT environment the hash-base quantum resistance schemes such that SPHINCS+ is a goodlooking option for PQC. Because, this type of algorithm uses only hash functions and they are straightforward and highly secure, viable option to prevent both classical and quantum attacks [39]. Additionally, multivariate polynomial cryptographic scheme such that LUOV and GeMSS can be a better option for the authentication of IoT network due to its lightweight signature generation and efficient computational cost. On the other hand, the [47] highlight the isogeny-based cryptographic method such as CSIDH offers extremely small keys and future possibilities for hybrid IoT protocols, even if its current computational cost is the limitation for real-time IoT application. Amidst these, one can say that, at the present code-base and hash-based post-quantum schemes are most appropriate for IoT system due to its executability with the existing infrastructure.

5. IMPLEMENTATION AND PERFORMANCE ANALYSIS

5.1 Hardware and software implementations:

In order to move quantum-resistant future cryptographic systems, the PQC implementation on both hardware and software platforms has become crucial. The deployment of PQC algorithms in real-world systems such as embedded IoT devices, high-performance servers, cellular network devices demand strong performance and lower power consumption after proper development of quantum computing.

For developing the software to implement the PQC, some lattice-based algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium are the central point standardize by NIST in 2024. PQClean, liboqs, and OpenQuantumSafe are examples of optimized software frameworks that offer cross-platform, modular implementations that are simple to incorporate with the traditional protocols like TLS and SSH. According to some studies, Kyber-512 can execute effective key exchanges on ARM Cortex-M4 architectures in less than one millisecond, making it viable for constrained IoT environments.

Software is not only the solution for implementing PQC, there is a requirement of hardware acceleration to minimize the computational overhead. The implementations of Kyber, Dilithium, and SPHINCS+ in hardware level have demonstrated significant performance gains like achieving up to 60x faster execution compared to pure software [41]. Additionally, hardware-software co-design techniques are being investigated in [48], in which control and protocol logic are kept in software but important matrix and polynomial operations are assigned to specialized hardware accelerators. This hybridization improves speed and energy efficiency while preserving resistance to side-channel attacks. Even with the advancements, problems still exist, on small embedded platforms, a lots of PQC algorithms still have large memory requirements and slow key generation. For a seamless transition during the NIST PQC transition period, researchers are investigating hardware-level random number generators, energy-conscious PQC cores, and hybrid cryptographic modules that combine classical and PQC primitives.

5.2 Benchmarks: encryption, decryption, and key generation times:

Determining the feasibility of integrating the post quantum algorithms in IoT environment, it is essential to take into account the resource limitation of IoT devices. The primary factors of IoT communication such as latency, throughput, and energy efficiency depends on the computation cost of key generation, encryption and decryption. CRYSTALS-Kyber and CRYSTALS-Dilithium has been taken as a reference's methods by the NIST for the key encapsulation and digital signature [22]. In IoT systems, lattice-based algorithms like Kyber-512 and Dilithium-II exhibit remarkable computational efficiency [49]. These efficiencies display that optimized lattice-based PQC algorithms are feasible in context of resource constrain IoT networks. The large key sizes and complicated decryption process is the main cause for slower performance in code-based algorithms like BIKE and HQC [51]. In firmware authentication, where verification is more important than signing speed, hash-based systems like SPHINCS+ are very secure. For certain IoT use cases that need for long-term security or low-frequency cryptographic operations, including secure updates or sensor node authentication, code- and hash-based methods are more appropriate.

5.3 The real-world factors affecting their worldwide implementation:

Beyond the technical development of quantum-safe algorithms, there are several real-world obstacles to the adoption of PQC algorithms in IoT environments. A number of factors, such as hardware constraints, interoperability, scalability, regulatory frameworks, and economic viability etc. have restricted the widespread deployment of PQC in IoT environment.

In a IoT network, the majority of the IoT devices are severely limited in connection with energy, memory, and processing capability. Lattice-based or code-based PQC algorithms have typically required large key sizes and computation of complex polynomial arithmetic, implementing these PQC schemes into IoT network will show the performance degradation or unnecessary latency. According to [51], PQC key sizes can be up to 20 times bigger than RSA or ECC, which results in communication overheads that restrict their use in low-bandwidth condition. Lack of international standard is also another key issue for PQC deployment worldwide. Successful integration of IoT devices in a IoT network is largely contingent upon cross-manufacturer compatibility. Therefore, the presence of various PQC methods

and implementation frameworks challenges secure integration into established protocols like as TLS, MQTT, and CoAP.
The transition from classical cryptography to post-quantum cryptography poses a hazard for compromising current systems due to incompatibility with outdated protocol. For these issues, the hybrid system i.e. integration of classical and PQC algorithms can be a solution [46]. From a business point of view, a major obstacle to widespread of PQC implementation is the expense of firmware upgrades, re-certification, and infrastructure modifications [41]. Additionally, inconsistent national adoptions are caused by regulatory uncertainties, particularly with regard to export control and data protection legislation. Before an extensive deployment, it is crucial to validate PQC implementations against side-channel attacks, timing leaks, and physical tampering.

5.4 PQC for Cloud Security and Decentralized Environments:

Cloud and decentralized systems rely on public-key algorithms like RSA, ECDSA, and Diffie-Hellman etc. and these algorithms which are fundamental to the authentication, authorization and encryption are susceptible to quantum attacks [22]. Therefore, deployment of PQC can make quantum resistant trust infrastructure to this system, confirming confidentiality and availability in decentralized environments. In IoT-cloud platforms significantly rely on multi-layered, virtualized infrastructures, which require secure authentication and scalable encryption. To create post-quantum secure communication channels, lattice-based techniques such that CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures are being incorporated with TLS is a solution [46]. Blockchain-enabled IoT (BIoT) and federated clouds are the examples of decentralized networks, which mostly depend on authentication techniques and smart contracts to achieve distributed control. By enabling quantum-safe digital signatures and transaction verification, PQC incorporation into these systems increases distributed ledgers' resistance to potential quantum threats. Despite these benefits, large key size, computational cost, and a lack of standardization across international infrastructures pose difficulties to the widespread implementation of PQC in IoT-cloud-decentralized contexts.

6. CONCLUSION

In conclusion, the issues caused by quantum computing are resolved with the development of PQC systems. In most of the classical cryptosystems, quantum computing is a major threat and the total breakdown of these systems is also a new possibility. This study demonstrates the significance of quantum-resistant cryptographic algorithms in safeguarding the digital communication in the IoT network. Through an inclusive investigation of the weaknesses in classical cryptographic systems, this work has highlighted the existing PQC schemes such that it can be useful for the IoT environment. The popular methods for the PQC i.e. lattice-based, code-based, Multivariate Polynomial based, hash-based, and isogeny-based are surveyed such that deployability is possible in the IoT networks. The NIST standardization of PQC has been investigated properly to drawing the attention of security software and hardware developers. Also, this work can be served as a significant foundation for the future researcher in the field of PQC.

7. REFERENCES

[1] Akbar, A., 2025. Analyzing the Harvest Now, Decrypt Later Threat and Post-Quantum Cryptography Solutions: A Systematic Literature Review. *migration*, *2*, p.10.

[2] Shor, P.W., 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), pp.303-332.

[3] Grover, L.K., 1996, July. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219).

[4] Bindel, N., Brendel, J., Fischlin, M., Goncalves, B. and Stebila, D., 2019, May. Hybrid key encapsulation mechanisms and authenticated key exchange. In *International Conference on Post-Quantum Cryptography* (pp. 206-226). Cham: Springer International Publishing.

[5] Peikert, C., 2016. A decade of lattice cryptography. *Foundations and TrendsŴ in Theoretical Computer Science*, *10*(4), pp.283-424.

[6] Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G. and Stehlé, D., 2018. Crystals–dilithium: Digital signatures from module lattices.

[7] Alkim, E., Ducas, L., Pöppelmann, T. and Schwabe, P., 2016. Post-quantum key {Exchange—A} new hope. In *25th USENIX security symposium (USENIX Security 16)* (pp. 327-343).

[8] Bernstein, D.J., 2025. Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1846-1847). Cham: Springer Nature Switzerland.

[9] National Institute of Standards and Technology (2024) NIST Releases First 3 Finalized Post-Quantum Encryption Standards, 13 August. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[10] Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.K., Miller, C. and Moody, D., 2022. Status report on the third round of the NIST post-quantum cryptography standardization process.

[11] Grassl, M., Langenberg, B., Roetteler, M. and Steinwandt, R., 2016, February. Applying Grover's algorithm to AES: quantum resource estimates. In *International Workshop on Post-Quantum Cryptography* (pp. 29-43). Cham: Springer International Publishing.

[12] Erol, V., 2025. Quantum Readiness in Cryptography: A Maturity-Based Framework for Post-Quantum Transition.

[13] Mukhamedovna, A.S., 2024, May. Access Authentication and Key Distribution Using Physically Unclonable Functions, with SHA-256 as an Example. In *International Workshop on Advanced Information Security Management and Applications* (pp. 12-18). Cham: Springer Nature Switzerland.

[14] Brassard, G., Høyer, P. and Tapp, A., 1998, April. Quantum cryptanalysis of hash and claw-free functions. In *Latin American Symposium on Theoretical Informatics* (pp. 163-169). Berlin, Heidelberg: Springer Berlin Heidelberg.

[15] Chen, J., Deng, H., Su, H., Yuan, M. and Ren, Y., 2024. Lattice-based threshold secret sharing scheme and its applications: A survey. *Electronics*, *13*(2), p.287.

[16] Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I. and Cammarota, R., 2019. Post-quantum lattice-based

cryptography implementations: A survey. *ACM Computing Surveys (CSUR)*, *51*(6), pp.1-41.

[17] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G. and Stehlé, D., 2018. Crystals-dilithium: A lattice-based digital signature scheme. *IACR transactions on cryptographic hardware and embedded systems*, pp.238-268.

[18] Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W. and Zhang, Z., 2018. Falcon: Fast-Fourier lattice-based compact signatures over NTRU. *Submission to the NIST's post-quantum cryptography standardization process*, *36*(5), pp.1-75.

[19] Fitzgibbon, G. and Ottaviani, C., 2024. Constrained device performance benchmarking with the implementation of post-quantum cryptography. *Cryptography*, *8*(2), p.21.

[20] Vercauteren, I.F., Roy, S.S., D'Anvers, J.P. and Karmakar, A., 2020. SABER: Mod-LWR based KEM (round 3 submission). *ProQuest Number: INFORMATION TO ALL USERS*, *31657053*.

[21] Hoffstein, J., Pipher, J. and Silverman, J.H., 1998, June. NTRU: A ring-based public key cryptosystem. In *International algorithmic number theory symposium* (pp. 267-288). Berlin, Heidelberg: Springer Berlin Heidelberg.

[22] Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.K., Miller, C. and Moody, D., 2025. *Status report on the fourth round of the nist post-quantum cryptography standardization process* (p. 5). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.

[23] Ahmed, N., Zhang, L. and Gangopadhyay, A., 2025, August. A survey of post-quantum cryptography support in cryptographic libraries. In *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)* (Vol. 1, pp. 906-917). IEEE.

[24] Paul, S., Scheible, P. and Wiemer, F., 2022. Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication. *Journal of Computer Security*, *30*(4), pp.623-653.

[25] Duraibi, S. and Alashjaee, A.M., 2025. Lightweight Post-Quantum Secure Communication Protocol for IoT Devices Using Code-Based Cryptography. *IEEE Transactions on Consumer Electronics*.

[26] Wang, Y. and Ismail, E.S., 2025. A Review on the advances, applications, and future prospects of post-quantum cryptography in blockchain, IoT. *IEEE Access*.

[27] Joshi, A., Bhalgat, P., Chavan, P., Chaudhari, T. and Patil, S., 2024, November. Guarding against quantum threats: A survey of post-quantum cryptography standardization, techniques, and current implementations. In *International Conference on Applications and Techniques in Information Security* (pp. 33-46). Singapore: Springer Nature Singapore.

[28] GonzÁlez de la Torre, M.A., Encinas, L.H. and GarcÍa, J.S., 2025. Structural analysis of code-based algorithms of the NIST post-quantum call. *Logic Journal of the IGPL*, *33*(5), p.jzae071.

[29] Bernstein, D.J., Chou, T., Lange, T., von Maurich, I., Misoczki, R., Niederhagen, R., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N. and Szefer, J., 2017. Classic McEliece: conservative code-based cryptography. *NIST submissions, 1*(1), pp.1-25.

[30] Aragon, N., Barreto, P., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Ghosh, S., Gueron, S., Güneysu, T. and Melchor, C.A., 2022. BIKE: bit flipping key encapsulation.

[31] Melchor, C.A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Persichetti, E., Zémor, G. and Bourges, I., 2018. Hamming quasi-cyclic (HQC). *NIST PQC Round*, *2*(4), p.13.

[32] Ding, J. and Schmidt, D., 2005, June. Rainbow, a new multivariable polynomial signature scheme. In *International conference on applied cryptography and network security* (pp. 164-175). Berlin, Heidelberg: Springer Berlin Heidelberg.

[33] Casanova, A., Faugere, J.C., Macario-Rat, G., Patarin, J., Perret, L. and Ryckeghem, J., 2017. *GeMSS: a great multivariate short signature* (Doctoral dissertation, UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France; LIP6-Laboratoire d'Informatique de Paris 6).

[34] Ding, J., Zhang, Z., Deaton, J., Schmidt, K. and Vishakha, F., 2019. New attacks on lifted unbalanced oil vinegar. In *the 2nd NIST PQC Standardization Conference* (pp. 1-13).

[35] Gligoroski, D., Ødegård, R.S., Jensen, R.E., Perret, L., Faugere, J.C., Knapskog, S.J. and Markovski, S., 2011, November. MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme. In *International Conference on Trusted Systems* (pp. 184-203). Berlin, Heidelberg: Springer Berlin Heidelberg.

[36] Morales Rivero, X., 2023. *Seamless transition to post-quantum resistant: implementing digital signatures for pdf documents Using PQ algorithms* (Bachelor's thesis, Universitat Politècnica de Catalunya).

[37] Azarderakhsh, R., Elkhatib, R., Koziel, B. and Langenberg, B., 2021, September. Hardware deployment of hybrid PQC: SIKE+ ECDH. In *International Conference on Security and Privacy in Communication Systems* (pp. 475-491). Cham: Springer International Publishing.

[38] Giron, A.A., do Nascimento, J.P.A., Custódio, R., Perin, L.P. and Mateu, V., 2023, September. Post-quantum hybrid KEMTLS performance in simulated and real network environments. In *International Conference on Cryptology and Information Security in Latin America* (pp. 293-312). Cham: Springer Nature Switzerland.

[39] Bernstein, D.J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J. and Schwabe, P., 2019, November. The SPHINCS+ signature framework. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 2129-2146).

[40] Hülsing, A., Butin, D., Gazdag, S., Rijneveld, J. and Mohaisen, A., 2018. *XMSS: eXtended Merkle signature scheme* (No. rfc8391).

[41] Bagheri, S., Kaveh, M., Hernando-Gallego, F., Martín, D. and Serrano, N., 2025. A Constant-Time Hardware Architecture for the CSIDH Key-Exchange Protocol. *arXiv preprint arXiv:2508.11082*.

[42] Costello, C., Longa, P. and Naehrig, M., 2016, July. Efficient algorithms for supersingular isogeny Diffie-Hellman. In *Annual international cryptology conference* (pp. 572-601). Berlin, Heidelberg: Springer Berlin Heidelberg.

[43] Azarderakhsh, R., Campagna, M., Costello, C., Feo, L., Hess, B., Jalali, A., Jao, D., Koziel, B., LaMacchia, B. and Longa, P., 2017. SIKE–Supersingular Isogeny Key Encapsulation. *URL: https://sike. org*.

[44] Felderhoff, J., 2019. *Hard homogenous spaces and commutative supersingular isogeny based diffie-hellman* (Doctoral dissertation, LIX, Ecole polytechnique; ENS de Lyon).

[45] Costello, C., 2020, December. B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 440-463). Cham: Springer International Publishing.

[46] Singh, M., Sood, S.K. and Bhatia, M., 2025. Post-quantum cryptography: a review on cryptographic solutions for the era of quantum computing. *Archives of Computational Methods in Engineering*, pp.1-42.

[47] Qi, M. and Chen, C., 2025. Hpqke: Hybrid post-quantum key exchange protocol for ssh transport layer from csidh. *IEEE Transactions on Information Forensics and Security*.

[48] Lee, Y., Youn, J., Nam, K., Jung, H.H., Cho, M., Na, J., Park, J.Y., Jeon, S., Kang, B.G., Oh, H. and Paek, Y., 2024. An efficient hardware/software co-design for FALCON on low-end embedded systems. *IEEE Access*, *12*, pp.57947-57958.

[49] Liu, T., Ramachandran, G. and Jurdak, R., 2024. Post-quantum cryptography for internet of things: a survey on performance and optimization. *arXiv preprint arXiv:2401.17538*.

[50] Kuznetsov, O., Kandiy, S., Frontoni, E. and Smirnov, O., 2023, October. Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece. In *CQPC* (pp. 1-11).

[51] Egbuagha, O. and Ikwunna, E., 2025. Post-quantum cryptography in practice: A literature review of protocol-level transitions and readiness. *Cryptology ePrint Archive*.

[52] Rahmati, M. and Rahmati, N., 2025. Lightweight post-quantum cryptographic frameworks for real-time secure communications in IoT edge networks. *Telecommunication Systems*, *88*(4), p.136.

[53] Almutairi, M. and Sheldon, F.T., 2025. Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review. *Eng*, *6*(12), p.346.

[54] Ramakrishna, D. and Shaik, M.A., 2025. PSESV: A hybrid post-quantum encryption Framework with real-time thermal and EM side-channel attack detection. *Ain Shams Engineering Journal*, *16*(12), p.103776.