Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 5, 2025

POST-QUANTUM CRYPTOGRAPHY: FROM THEORY TO PRACTICE

Javairia Armakoon[*1], Umair Paracha[2], Jawaid Iqbal[3], Muhammad Ajmal Khan[4]

[*1]*Master in Software Engineering, Riphah International University, Islamabad.*
[2]*Directorate of ICT, Allama Iqbal Open University, Islamabad*
[3]*Assistant Professor, Faculty of Computing Riphah International University Islamabad*
[4]*Computing & Technology Dept, Iqra University Islamabad*

[*1]jarmakoon@gmail.com, [2] umair.paracha@aiou.edu.pk, [3] Jawaid.iqbal@riphah.edu.pk,
[4]ajmalkhan.niazi666@gmail.com

DOI: https://doi.org/10.5281/zenodo.15552804

Keywords
Post-Quantum Cryptography, Lattice-Based Cryptography, Quantum Attacks, NIST Standardization, Cryptographic Algorithm Migration, IoT Security, Quantum Key Distribution.

Article History
Received on 21 April 2025
Accepted on 21 May 2025
Published on 30 May 2025

Corresponding Author: * Javairia Armakoon

Abstract
Quantum computers have developed into a leading thrust for new Post-Quantum encryption algorithms in the last ten years. However, there are systems generating quantum resistant systems. The security and safety of a system is based upon trusting the software. Cryptographic content, such as digital signatures in program images, can be trusted through a process whereby you issue images only to entities you know and trust. However, big (and bigger) quantum computer systems have decreased the safety of cryptographic primitives like Rivest-Shamir-Adleman (RSA) and Elliptic-Curve Cryptography (ECC), so with the motion to transport to Post-Quantum Cryptography (PQC) we want to transport, and it's far essential that we move. The paper discusses modern-day cryptographic schemes (symmetric and asymmetric), the consequences and dangers of quantum computing, quantum algorithms (Shor`s, Grover's), public key cryptography, symmetric schemes of concern, side-channel attacks, fault analysis, every approach of countermeasures to [provide a] quantum-resilient environment, a taxonomy of protection protocols, hybrid types of cryptography, stable communications models, the significance of hash functions, and post-quantum cryptography. The Post Quantum Cryptography respective phase discusses the numerous quantum key distribution strategies in addition to the mathematical schemes, along with lattice-primarily based totally cryptography, multivariate-primarily based totally cryptography, hash-primarily based totally signatures, and code-primarily based totally algorithms for encryption schemes. It specializes in present standardized algorithms (i.e., Kyber, Dilithium, and SPHINCS+). The implementation of PQC being included into present protection protocol frameworks (i.e., TLS, SSH, and DNSSEC) and as carried out to the Internet of Things (IoT).where limitations in resources and architectural constraints are vital points, has also been addressed in the survey. Both categories have advantages and disadvantages. All in all, lattice-based schemes are simple to implement and realize the optimal compromise among performance, key size, and memory requirements.

INTRODUCTION

With the advances of technology and science, computer systems become the basis of infrastructure. Modern quantum computers with fast speed can apply confidence vulnerabilities in existing systems, thus presenting major difficulties [1]. Cryptographic technological know-how is one of the maximum essential regions in records technology, simply because the confidentiality, integrity, authentication, and non-repudiation of information transmission and garage may be critical. Cryptography is a nation of software to shield records being transmitted or stored, from third-celebration attackers. The phrase cryptography comes from the Greek phrase for veiled and writing.

Current secure systems must also be secure in a post-quantum world with its integrity, authenticity, and non-repudiation intact, to leverage quantum systems to their full potential. Given all of this new threat space, it is abundantly clear that conventional cryptographic protocol based on mathematics, which has underpinned digital security for decades, must be revisited, particularly with the quantum computer revolution. As a paradigm shift in compute power, quantum computers will be able to solve challenging problems at scales well beyond anything conceivable with conventional computers [2].Richard Feynman proposed the notion of quantum computing in 1982. The two forms of this are symmetric cryptosystems and asymmetric cryptosystems. It has been researched ever since and is seen as the basis of 'modern symmetric cryptography'. We also know that some quantum algorithms impact symmetric cryptography as well, while it is possible to show that larger key spaces will provide security. Further, techniques were proven to interrupt uneven crypto schemes that depend upon the discrete logarithm trouble and the issue of factoring huge top numbers. Even elliptic curve cryptography, that is idea to be the high-quality and maximum steady manner to get a post-quantum pc, appears to be susceptible to quantum computers. Thus, there has been a want for encryption algorithms strong to quantum computations. These cryptographic techniques, which can be idea to be proof against quantum pc attacks, are known as post-quantum cryptography. PQC is a practical and scalable method of future-proofing digital security because, unlike quantum cryptography, it does not need quantum hardware and can be achieved with traditional systems. A range of quantum-resistant algorithms from mathematical problems such as lattices, multivariate polynomials, hash-based structures, and error-correcting codes has been introduced by researchers over the past decade. Most of these are in the process of being standardized by organizations such as NIST, and are the foundation upon which modern PQC primitives such as Kyber, Dilithium, and SPHINCS+ will be built. New algorithms, previously impossible under classical computing paradigms, will be brought into existence using this new way of thinking. The Shor's algorithm is such an algorithm; it is capable of solving the integer factorization problem in polynomial time and to compromise most of the current public-key cryptography schemes. In essence, all the security protocols have to be reconfigured to remove RSA, DSA, ECC [3], and other protocols once a quantum computer of manageable size is demonstrated. New public-key cryptography systems with quantum resistance were designed by the cryptography community in response. While the precise date of the development of massive quantum computers is not known, a number of predictions position it between 10 and 20 years from now [4]. This paper presents a thorough overview of Post-Quantum Cryptography with the aim to be a foundation for learning about its basic principles, algorithm families, implementation techniques, and security implications. The survey is initiated by revisiting classical and quantum cryptography fundamentals such as symmetric and asymmetric cryptography, hash functions. This article specializes in strategies that paintings at the hardness of factoring big top numbers and the discrete logarithm trouble. Then we have a take a observe quantum mechanics and the trouble of creating a real quantum computer. We have a take a observe quantum algorithms, Shor`s set of

rules and Grover's set of rules, on the way to have the primary impact on uneven cryptography, and much less impact on symmetric. Finally we have a take a observe post-quantum cryptography. The studies explores quantum key distribution and arithmetic primarily based totally options, like: lattice-primarily based totally, multivariate-primarily based totally, hash-primarily based totally, and code-primarily based totally cryptography [5]. PQC can prove particularly valuable in resource-constrained environments, as we experience with IoT technology, where secure communications requires trade-offs between efficiency, memory and computational complexity. The paper discusses the deployment of PQC in various commonly-implemented security protocols including TLS, DNSSEC and SSH. The paper considers side-channel and fault attacks, along with countermeasures, and presents a taxonomy of security schemes. The focus is on both theoretical vulnerabilities around PQC, and the issues of practical deployment. Given the period of rapid progress in the fields of cryptography research and standardization work, alongside operational strategies for deployment, the book is intended to provide readers with a comprehensive description of Post-Quantum Cryptography as we embrace the quantum technology era. There is a lot of work to be done before we can achieve an acceptable level of security [6].

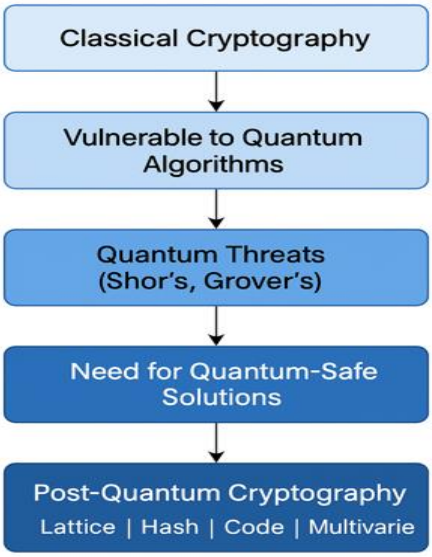

Figure 1. An Overview of the Quantum Era's Cryptographic Transition

LITERATURE REVIEW

Over the last decade, the growing threat of quantum computing has inspired substantial study into quantum-resistant cryptography systems. This study was prepared by reviewing 50 peer-reviewed research articles and standards publications, with an emphasis on the theoretical foundations and practical implementations of Post-Quantum Cryptography (PQC).

The literature encompasses academic research, NIST competition reports, cryptography library documentation, and experimental study of quantum-safe algorithms. After that, they contrasted how well these techniques worked in both confined and unconstrained settings for various key sizes and input data [7].

Table 1. Summary of Literature Review on Post-Quantum Cryptography

No.	Methods	Algorithms/Protocols	Tools/Frameworks	Limitations	Contributions
1	Theory analysis	NTRU, McEliece	N/A	No practical benchmarks	Defined PQC types
2	Design + testing	SPHINCS	Custom code	Large signature	Stateless, secure hash-signature
3	TLS integration	NewHope, TLS 1.2	OpenSSL fork	No IoT focus	First PQC in TLS
4	Side-channel test	Kyber, Dilithium	Hardware setup	Single attack type	Revealed vulnerabilities
5	Benchmark eval	Kyber, Dilithium, Falcon	PQCrypto, NIST tools	Standardization ongoing	Compared NIST candidates
6	IoT simulation	Kyber, NTRU	TinyPQC, Contiki	Only mid-tier IoT	Optimized PQC for embedded
7	Fault injection	CRYSTALS-Kyber	Custom fault rig	Limited scope	Suggested fault countermeasures
8	Hybrid design	Kyber + AES	OpenSSL	High overhead	Showed hybrid crypto viability
9	Library analysis	SPHINCS+, Falcon	Liboqs	Performance not stable	Tool-level integration insights
10	Quantum impact	RSA, ECC	N/A	Focuses only on classical	Stresses urgency of PQC switch

The studied literature confirms that Post-Quantum Cryptography is an important and dynamic research subject that addresses the pressing need for secure communication in a future shaped by quantum computing. The corpus of work not only demonstrates the possibility of quantum-resistant cryptographic algorithms, but it also highlights the practical constraints of deployment, particularly in IoT, critical infrastructure, and standardization compliance.

Core Concepts in Post-Quantum Cryptography

PQC is based on the change from classical to quantum computing paradigms. Quantum computers use qubits that can utilize the principles of superposition and entanglement to reside in multiple states at once, rather than classical deterministic binary bits that can be either 0 or 1. Classical encryption methods usually rely on either it being hard to compute discrete logarithms, or it being hard to factor large primes, and this quantum behavior could change the expectation of this difficulty. Indeed, any public-key cryptography algorithm that is used today would not be auditable in the post-quantum world [8]. PQC is predicated on nearly tough troubles which can be computationally tough for quantum computer systems to solve, in some other try to increase cryptographic algorithms which can be sturdy towards quantum attacks.

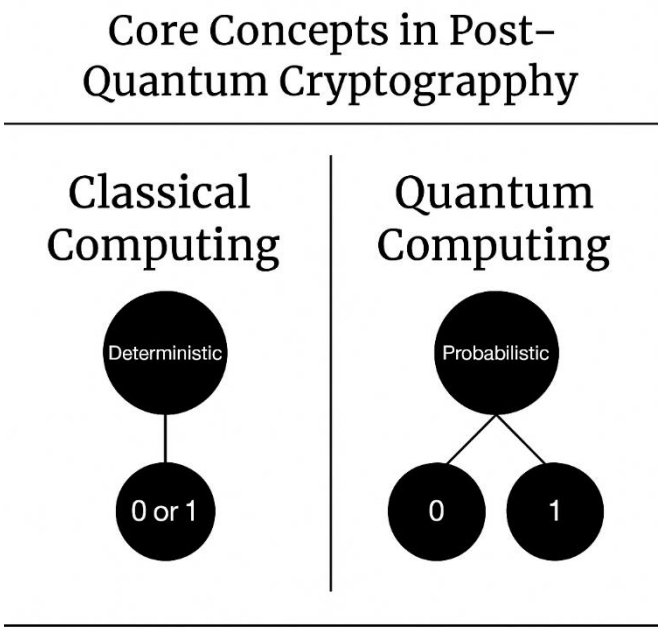

Figure 2. Comparison of Classical and Quantum Computing

Quantum Computing vs Classical Computing

The quantum computer, based on quantum mechanics, was conceptualized by physicist Richard Feynman in 1982. Quantum mechanics, can be viewed as the study of strange behaviors of physical phenomena that occur at the microscopic level. Bits, which are the basis of a computer, have only two states: 0 and 1. Quantum bits or "qubits" are used for quantum computers. Superposition is the ability of a qubit to be in the 0 and 1 states at the same time. When you observe a particle it collapses to one of the two states. Quantum computers use this ability to calculate complex problems. PQC is based on almost difficult issues which may be computationally difficult for quantum laptop structures to solve, in a few different try and growth cryptographic algorithms which may be robust toward quantum attacks. If the two qubits change states, the other, regardless of distance, will also change state. This provides true parallel processing capabilities. The number of values being computed in a single operation increases exponentially as the number of entangled qubits increases. So, an n-qubit quantum computer can compute and process 2n operations simultaneously. Bone and Castro argue that quantum computers are not significantly different than classical computers using transistors and diodes. Experimenter researchers have explored several designs, such as calculation fluid and quantum dots. They, too, argued that quantum computers would not demonstrate their advantage over classical machines until their applications with the algorithms take advantage of quantum parallelism. The quantum computer would perform multiplication just as poorly as a classical machine. These frequently leverage cryptographic primitives consisting of Elliptic-Curve Cryptography (ECC), and Rivest-Shamir-Adleman (RSA), whose protection is in jeopardy as quickly as a sufficiently large quantum pc exists. Therefore, it's far suitable to shift to Post-Quantum Cryptography (PQC) [9].

Table 2. Comparative Analysis: Classical vs Quantum Computing

Classical Computing	Quantum Computing
Bit (0 or 1)	Qubit (0 and 1 at the same time – superposition)
Deterministic state	Probabilistic & superposed state
Independent bits	Entangled qubits (interdependent)
Linear processing	Exponential parallelism (2^n operations)
Operates via transistors and diodes	Operates via quantum properties (superposition, entanglement)
Standard algorithms	Quantum-optimized algorithms (e.g., Shor's, Grover's)
Limited by classical physics	Uses quantum mechanics for processing

Qubits

In quantum computing, qubits are used instead of classical bits. Any two-state quantum mechanical system, such as the electron spin or the photon polarization, can be employed to implement a qubit. A qubit, like a classical bit, can be in two different base states. The mathematical representation of these states are two orthogonal unit vectors, which are usually denoted with the symbols |0i and |1i. The important difference is that the qubits can be in a superposition of the two states. A common way to describe the superposition state is

$$|\psi i = \alpha\ |0i + \beta\ |1i.$$

Where the complex integers α and β are referred to as the state's amplitudes.

$$|\ \alpha|^{\ 2} + |\beta|^{\ 2} = 1.$$

This may lead to the misconception that a single qubit can store infinite amounts of information, which is false. With probabilities of $|\alpha|^{\ 2}$ for |0 and $|\beta|^{\ 2}$ for|1, the superposition collapses into one of the two base states upon measurement and remains in that state. The superposition state's abilities can be utilized to perform parallel computations in a way that classical computers cannot, while making the qubit behave more like classical bits. This is accomplished through a process called quantum entanglement and clever mathematics. When two quantum particles are entangled such that they can affect one another's state regardless of the distance between them that is called quantum entanglement. To date, there are no quantum computers that are cryptographically relevant that is, they do not have enough qubits to break ECDSA [10].

Quantum gates

Quantum circuits utilize quantum gates, similar to how digital circuits employ logic gates. The NOT gate, controlled NOT gate, and Hadamard gate are the three most important gates. For a single qubit, the behavior of the NOT gate is identical to a regular NOT gate: it changes |0 to |1 and back to |0. It does this by swapping the two probabilities when applied to a quantum bit that is in superposition. The controlled NOT gate does the same thing; it affects the value of the second qubit, but only when the state of the first qubit is |1. The Hadamard gate is specific to a quantum computer and is not applicable on a traditional computer; however, the first two gates are applicable. After the Hadamard gate has been applied, it places a qubit in a superposition between the two states. The qubits in superposition are encoded to a linear combination of the two new bases, qubits in the |0 state are encoded to |0+|1√2, and qubits in the |1 state are encoded to |0−|1√2. If applied iteratively, the Hadamard gate can produce a system of n entangled qubits in the superposition state.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

Where N means 2n. Which implies that as you increase n for qubits, the amount of information it can process also increases. Additionally, it should be noted the program is a specifically crafted PQC standard IEEE 2030.5 program used universally with different types of gateway hardware and operating systems [11].

Challenges in Quantum Computing

Quantum computing presents numerous hurdles for researchers to address. Although it is sometimes heralded as the next big development in general computation, quantum computing only has the ability to speed up the computation of a small number of computer science tasks [12].

- Quantum algorithms are mostly probabilistic. A quantum computer can produce multiple solutions in a single move, but one solution is correct. Quantum computing speed benefit is diluted by trial and error to ensure correct solutions.
- Errors affect qubit performance from heat, thermal noise, or other stray electromagnetic couplings that exist. In classical computers, we with bit-flips, zero becomes a one, and one becomes a zero. Qubits experience bit-flips as well as phase issues. You definitely do not want to directly check for errors because that will collapse the value into a superposition.
- Another hassle is incoherence. Qubits can keep our quantum nation for simplest a fed on quantity of time. Scientists on the University of New South Wales in Australia constructed forms of qubits, Phosphorous and Artificial beforehand, and comprise them in magnetic noise for manage in a medium of silicon (silicon 28) to remove errors. Phosphorous qubits have an accuracy of 99.99% overall performance rate, one mistakes each 10,000 quantum operations. Their qubit may be in superposition for 35 seconds that is file information. For these qubits to maintain a long-term coherence, they need to be separated and of course kept at absolute zero. The issue is once they become isolated we have difficulty controlling them without inclusion of further noise.

Preliminaries of PQC

The subject called post-quantum cryptography - or additionally called quantum-resistant cryptography or quantum-secure cryptography seeks to create algorithms for cryptocurrencies which can be proof against quantum pc attacks [13]. Because of development being made with inside the blockchain area and quantum computing area, the cost of public key PQC to guide stable communications is none too little [14]. The branches of post-quantum cryptography are quantum cryptography and classical quantum-resistant cryptography. Though Wiesner first proposed quantum cryptography in 1970, it turned into now no longer till 1983 that he proposed quantum cash and a quantum channel in his paper "Conjugate Coding." Standard bit cryptography makes use of bits, quantum cryptography makes use of qubits. A qubit, like a chunk may have the values "0" and "1". Unlike a chunk, however, a qubit also can exist in superposition. The superposition states exist from the fact a qubit can exist in pure and mixed state and also gives the capability to encode more states into less [15]**.** After the development of Shor's quantum algorithm, which can crack RSA- and ECC-computational-based cryptographic systems, the cryptography community has proposed additional public-key alternative quantum attack resistant cryptographic techniques called post-quantum cryptography. NIST has been a leader in PQC research and standardization [16].The reason of post-quantum cryptography, or quantum-resistant cryptography, is to create affirmative warranty that steady cryptographic structures should paintings on modern-day community and communique protocols which can be nevertheless in use. These replacements want to be primarily based totally on mathematically tough troubles which can be quantum secure and need to perform similar to conventional PKC. An attacker might also additionally make use of associated statistics to make the most periodicity, in addition to the quantum advantage/enhancement to create

authentication tags such that the enquirer can't retrieve keys anyway, however that authenticity can nevertheless harm integrity [17]. Post-quantum cryptography (PQC) is a shape of cryptography that is based on mathematical issues and is assumed to be proof against quantum-laptop attacks. PQC comes in lots of varieties. The 5 essential kind varieties of PQC are lattice-based, hash-based, isogeny-based, code-based, and multivariate. Each has its strengths and weaknesses. In occasion of R-LWE public key systems to its predecessor of LWE public key systems, R-LWE are better in terms of computation because of lower overhead, greater message space capacity, and smaller size of public keys[18]. Research on post-quantum cryptography is advancing quickly. NIST selected four algorithms as the initial winners in 2022. Key Encapsulation Mechanism (KEM) is represented by CRYSTALS-Kyber, whilst digital signatures are represented by CRYSTALS-Dilithium, Falcon, and SPHINCS+. In terms of applications, post-quantum cryptography approaches perform better than pre-quantum methods with the same degree of security [19]. PQC is essential for ensuring secure communication, particularly in light of the developments in quantum computing technology. Researchers in cryptography are working hard to create reliable and effective PQC protocols and solutions. The CRYSTALS-DILITHIUM (Dilithium) method was chosen by the NIST in 2022 because it has been demonstrated to be a good fit for server-client architectures and provides legible code and comprehensive documentation [20]. PQC is at the leading edge of constructing encryption protocols that are resistant to quantum-computer-attacks.

Table 3. PQC Algorithm Comparison at 128-bit Security Level

Algorithm	Public Key Size	Ciphertext Size	Signature Size
Kyber512	1632 bytes	800 bytes	N/A
Dilithium2	1312 bytes	N/A	2420 bytes
SPHINCS+-128s	32 bytes	N/A	7856 bytes
FALCON-512	897 bytes	N/A	666 bytes
Rainbow-I	104 bytes	N/A	66 KB
McEliece (8192,4608)	N/A	261120 bytes	N/A

Design Principals (Precision, Security, Flexibility)

The layout standards of the framework make sure accuracy, flexibility, and safety. The method is designed to assist the transition from classical cryptographic processes to post-quantum cryptographic options whilst adapting to the evolving quantum laptop chance landscape.

- **Accuracy:** Determining dependencies within cryptographic objects and assets is critical to comprehending their effect on data-related security. Insight into dependencies enhances the ability of organizations to make more educated decisions on the possible implementation of post-quantum cryptography solutions that best fit the organization and its properties.
- **Security:** The framework emphasizes security by identifying, examining, and implementing post-quantum cryptography solutions as a means of preventing quantum attacks. This means systematically investigating, gathering, and assessing existing cryptography inventory, weaknesses, enables crypto-agility and proposes post-quantum solutions that will address specific data security needs.
- **Flexibility**: The framework's flexibility offers compatibility with new and quantum secure cryptographic procedures and standards, other security frameworks and approaches, and with organization of all sizes and

industries. This is an important benefit as most organizations are likely already sedentary with their existing security processes; the flexibility helps to support a seamless experience with current security infrastructure while addressing areas that may be out of scope, such as risk assessment, common threat detection, and business continuity.

Fundamentals of Cryptography

Cryptography is essential for secure digital communication because it ensures data secrecy, integrity, authenticity, and non-repudiation. It is an essential step to further enhance data security and confidentiality [21]. It is divided into two specific types symmetric and asymmetric. The asymmetric form is the most used and known of the two standards [22]. Symmetric cryptography makes use of the identical mystery key for each encryption and decryption. Symmetric cryptography is speedy and clean to use, despite the fact that dispensing the name of the game key demanding situations with inside the actual world. This vicinity of cryptography makes use of many unique algorithms, however the maximum famous is Advanced Encryption Standard (AES). Symmetric cryptography makes use of a non-public and public key pair. Asymmetric algorithms use the general public key for encryption and the non-public key for decryption. This summary fashion of cryptography is extra powerful than symmetric cryptography due to the fact the general public key may be used to offer a quicker way of trade of keys among speaking events in a stable manner, despite the fact that now no longer overall performance wise. Some acknowledged uneven algorithms encompass RSA, Diffie–Hellman, and Elliptic curve cryptography (ECC). Now that we blanketed the essential styles of encryption it's far critical to recognize the milestones reached as human beings get towards growing quantum resistant encryption algorithms. In a few instances, quantum algorithms provide higher overall performance (speed) than classical algorithms [23].

Symmetric Cryptography

Symmetric cryptography is commonly employed for large-scale data transfers due to its speed benefit. Symmetric encryption requires secret agreement between sender and recipient on the same key, which is a drawback. The process of two people transferring keys in front of enemies is known as key exchange. The same key is shared between parties if they utilize symmetric keys; if not, a public key needs to be shared [24]. Let`s say Alice took a plaintext message and encrypted it together along with her shared mystery key, and Bob takes Alice's encrypted plaintext and decrypts it the use of the equal cryptographic algorithm, and shared mystery key. In this manner Alice and Bob need to be the best humans to have get right of entry to to the shared mystery key in the event that they intend to maintain the encryption mystery. The mbed TLS library provides application programming interfaces (APIs) to cryptographic algorithms that are encapsulated in modules with loosely coupled interfaces. The encapsulated modules for the cryptographic algorithms can be further categorized into hash functions, random number generators, symmetric encryption, and modes of operation [25]. An efficient method for the transport of secret keys over open networks must be found. Asymmetric cryptography was developed to resolve the issue of key distribution in symmetric encryption. Symmetric algorithms like AES and 3DES are widely used. Symmetric cryptosystems rely on the challenge of probing about several secret values. In systems like Advanced Encryption Standard (AES) exhaustive key searches are a real threat. Grover's algorithm allows for AES key searching to be completed quicker (with fewer operations) than classical computers.

Grover's algorithm in Symmetric Cryptography

Grover's algorithm is a quantum search algorithm first put forth by Grover, and this search algorithm can discover an element in an unsorted set of data with a very high probability of success after making only O (√n) queries instead of O (n) queries that a classical computer would use. The discovery system utilizes Hadamard gates to put

the qubits into superposition of all possible states before increasing the probability of the correct element. This is accomplished by applying two operators many times. The first operator is called a phase inversion, and performs a computation of the phase of the amplitude of the desired element by altering the sign of the amplitude. Grover's algorithm searches through an unsorted database in √N time. For example, if one considers a list of four elements: {0, 1, 2, 3} and the correct value is 2, a classical algorithm may take a maximum of four queries for it to determine the value of 2. Grover's technique, on the other hand, begins with all states in superposition and then utilizes a quantum oracle to invert the amplitude of the correct answer. Following one round of amplitude amplification (diffusion operator), measuring the system provides the correct number 2 with high probability, exhibiting a quadratic speedup over traditional search. Grover's technique enables faster brute-force searches for cryptographic keys. This affects all cryptographic algorithms; nonetheless, doubling the key-size is a suitable countermeasure. Grover's quantum technique impacts hash function security since it quadruples the pace of brute-force searches [26].

Common Algorithms (AES, DES)

We focus on NIST standards because these standards are still commonly used today and have global impact and reach indicated through the standardization of DES in the1970s and AES in the 1990s [27] AES, or Advanced Encryption Standard, changed the out of date Data Encryption Standard with inside the USA in 2001 after the National Institute of Standards and Technology (NIST) finished the AES specification. AES turned into designed with the aid of using Joan Daemen and Vincent Rijmen and is a symmetric key set of rules with key sizes of 128, 192, and 256 bits, and a 128-bit records block length for encryption. AES`s technique includes a procedure wherein plaintext will become ciphertext via the repeated felony alterations implemented to the plaintext through a mathematical operations procedure, and this makes use of a Substitution Permutation Network (SPN).

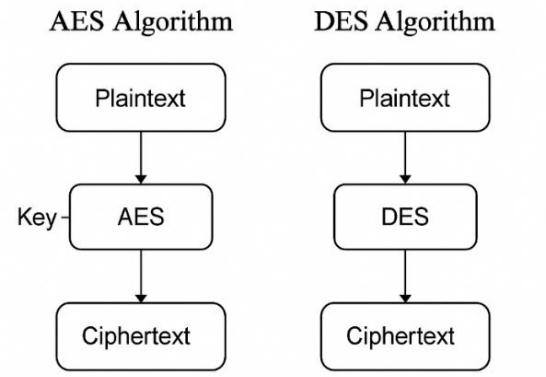

Figure 3. Overview of the AES and DES encryption process

Figure 6 shows how encryption begins with plain text and a secret key. The inputs undergo various changes to hide and jumble data. Each round uses four basic operations.

• S-boxes and lookup tables are used to do non-linear byte substitutions and break patterns.
• Row-wise cyclic shifts rotate bytes within each row to disperse data associations.
• Columnar mixing utilizes finite field arithmetic and mathematical blending of column values to convey changes throughout the block.
• Round-key integration using XOR operations to combine processed data with unique subkeys produced from the main secret.

The number of transformation rounds (10, 12, or 14) varies with key length (128, 192, or 256 bits), allowing for a flexible compromise between cryptographic strength and computing needs.

The layered technique assures that even slight input changes have a significant impact on the cipher text, known as the avalanche effect, while remaining efficient for broad use. Though SPHINCS+ Haraka 192 took 216 MS for key generation, 3,168 MS for signing and 2.9 MS for verification, the Dilithium 2 AES implementation on Android had timings of 275 μs for key generation, 667 μs for signing, and 120 μs for verification [28].

AES became the global encryption standard by addressing vulnerabilities in DES, such as its short 56-bit keys that might be cracked by 1990s hardware. This was accomplished by the use of strong 128-256-bit keys and a substitution-permutation network (SPN) that prevents pattern analysis. AES's mathematical structure and extended key space need infeasible 2128 operations to break, even with quantum-accelerated methods, unlike DES, which may be breached in hours using brute-force attacks. Its efficiency in hardware/software resulted in widespread usage in TLS, Wi-Fi, and disk encryption, but security is dependent on truly random keys: bad key generation degrades AES's strength regardless of algorithmic soundness. The move from DES highlighted cryptography's arms race for processing power. AES's bigger blocks (128 vs. 64 bits) and SPN design protect against the specialized hardware attacks that destroyed its predecessor, preserving its relevance in modern security environments.

Vulnerabilities in symmetric Cryptography

Grover's method presents a quantum threat to symmetric encryption algorithms such as AES and SM4. Although often more resistant because of key-size adjustability that AES provides, Grover's method can efficiently shrink even AES-128—a 128-bit key—to a 64-bit key. Similar weaknesses exist with SM4, which has a constant 128-bit key size. The only defense to reduce quantum issues is to use larger key sizes (e.g., AES-256). DES illustrates how symmetric encrypted-bad actors are influenced by quantum assaults. Bone and Castro (1997) display that Grover`s set of rules can ruin DES the usage of most effective 185 seek attempts (key size = 56-bits). This is once more an instance of the requirement for nonce resistant cyber defenses towards quantum assaults bearing on symmetric encryption.

Asymmetric Cryptography

Asymmetric cryptography, additionally known as public key cryptography (PKC), encodes records with pairs of keys. Each aspect must have their personal public key and personal key. In the PKC sense, to encrypt a verbal exchange, Alice might ship Bob her public key. Bob might do the encryption the usage of Alice`s public key. Bob might ship his encrypted message to Alice, and Alice can use her non-public key to decrypt it. To encrypt a verbal exchange we use a public key and handiest the non-public key proprietor can decrypt the verbal exchange. Asymmetric cryptography is likewise used for virtual signatures. For example, we will have Alice digitally signal a file together along with her non-public key, and then, Bob can confirm the file with Alice's public key. The protection of PKC is primarily based totally upon a few implausible computational challenges, like factoring very massive top numbers. Also, supplying answers for the discrete logarithm trouble being one of the greater extensively universal varieties of one-manner capabilities which can be handiest capabilities which are clean to compute one manner than to invert. There is a few feature that, going one manner, is simple to compute, which means we will discover its inverse feature despite the fact that it is now no longer feasible (i.e., it takes a long term to compute). Asymmetric encryption can generate a shared key in ways. You can use an encryption set of rules (e.g. RSA) or a key change set of rules (e.g. Diffie-Hellman, mentioned below). When enforcing an encryption set of rules, one birthday celebration encrypts a randomly generated key the usage of the opposite birthday celebration's public key and sends it over in ciphertext, then each events can talk while the opposite birthday celebration effectively decrypts the ciphertext. A key change set of rules permits each events to agree on a shared mystery and pick a few subset of that key. The key can both be a shared mystery or hashed

to supply a key. The predominant issues for a unbroken transition from present cryptographic uneven algorithms to post-quantum ones are implementation protection and performance [29].

Shor's Algorithm in Asymmetric Cryptography

Mathematician Peter Shor confirmed in his 1994 paper "Algorithms for Quantum Computation: Discrete Logarithms and Factoring" that quantum computing goes to dramatically alternate the factorization of very huge integers. Because Shor`s approach is primarily based totally at the discrete logarithm trouble or huge high integer fractionalization it might be going to demolish cutting-edge uneven cryptography. If you take into account the subsequent instance it's going to illustrate how Shor's approach elements huge high integers. The instance will discover the high factorization of the integer 15. To do that it's going to take a 4-qubit sign up. A 4-qubit sign up ought to arguably be idea of as a trendy 4-bit sign up on a trendy computer. 15 in binary is 1111, consequently the high factorization of the integer may be accommodated (calculated) in a 4-qubit sign up. Bone and Castro describe that a computation at the sign up is largely a sequence of parallel computations for every value (0–15) that the sign up can accommodate. The computation is the best issue to be executed on a quantum computer. Subsequently, that is what the set of rules does:

- We want to factor n = 15.
- Let x be some random number, such as $1 < x < n - 1$.
- X is taken to the power held in a register (all possible states), then x is divided by n. The first 4-qubit register holds the remainder of the divide operation. The space for results of the superposition state are now stored in the second register. We will assume x = 2, as it is greater than 1 and less than 14.
- Electronic calculations are performed. We clearly see a cycle of four numbers (1, 2, 4, and 8). Given x = 2 and n = 15, we can say that we can encapsulate this series as defined by the value of f = 4. A formula that we can use to find a possible factor based on this value of f: One possible factor comes out to be $P = x^{f/2} - 1$.

Table 4 gives the remainder from the series of divides by 15, with the variable raised to the 4-qubit register, with a maximum of 15.

When the end result isn't a top integer we carry out the calculation the use of unique f values. Discrete logarithm troubles also can be calculated the use of Shor`s set of rules. Vazirani very well analyzed the technique of Shor's set of rules and validated that a brand new superposition will be created such that we might have a excessive chance of integers that fulfill an equation for the reason that we commenced with a random superposition kingdom of integers and executed some of Fourier transformations. This equation lets in us to calculate the fee of r, the unknown exponent of the DLP.

Table 4. Qubit Remainders and Registers

Register 1:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Register 2:	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8

Cryptographic Cyphers

In the following section Key Algorithms in Cryptography are explained

RSA Cryptosystem: RSA is a public-key gadget created through Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. RSA makes use of the mission of factoring biprime numbers. Paar and Pelzl advocate that uneven algorithms like RSA can't be a substitute to symmetric algorithms because of the computational complexities. RSA is typically used to set up stable key trade among stop users. Typically it's far used with symmetric algorithms for records encryption and decryption like as an instance AES. Kirsch suggests that RSA is a serious risk if there are substantial increases in processing speed or factorization methods.

One method of achieving this goal is through quantum-computers that use quantum mechanics and models.

Discrete Logarithm Problem (DLP): Because each Diffie-Hellman (DH) and Elliptic Curve Cryptography (ECC) are uneven schemes which can be primarily based totally at the discrete logarithm problem (DLP), it'd be hard to interrupt both of the algorithms (protocols) utilized in both of the schemes.The probability of discovering the integer r such that gr = x mod p is very low. The discrete logarithm problem of the integer x and non-integer base g is determined by the number r = logg x mod p. It could be difficult to solve the discrete logarithm problem in an efficient manner with large values of a parameter.

Diffie-Hellman (D-H): Typical key settlement could use modular exponentiation withinside the context of the Diffie-Hellman key exchange. Key-time table assaults and key-associated differential timing assaults, are feasible on the primary 3 rounds of the discrete logarithm (D-H) cryptography set of rules additionally with eight rounds [30]. Alice and Bob agree on a public modulus (p) and base (g). Alice agrees to a secret number a, computes

$$A = g^{a} \bmod p,$$

And sends it to Bob. Bob sends

$$B = g^{b} \bmod p$$

To Alice. The key can be computed by both parties using the formula

$$B^{a} = g^{ab} = A^{b} \bmod p.$$

The D-H key exchange's security relies on the difficulty of calculating the discrete logarithm and extracting x from g^{x} mod p).

Elliptic curve Diffie-Hellman (ECDH): Elliptic curve Diffie-Hellman key exchange is conceptually similar to the classic version of the protocol, though it enables smaller key sizes. The protocol requires both parties to agree on certain public parameters, including:

- The field Fp in which they will be working.
- Elliptic curves (for example y2 = x3 + ax + b).
- A cyclic set of points on the curve (one element in the set, G).

Then, Alice picks a secret number, dA, and computes dAG, which she sends to Bob. Bob sends her dBG. They can then compute the key from the coordinates of dAdBG.
Like Diffie-Hellman encryption, the only way to break the system is to compute the discrete logarithm on elliptic curves.

Vulnerabilities in Asymmetric Cryptography
ECC algorithms, like ECDSA, provide superior security as compared to classical algorithms with smaller key sizes. The downside of ECC is that it is based on problems provably solvable using Shor's algorithm. Shor's methodology has real dangers against actual ECC signatures, not to mention the key exchange methodology that one would use. Following Kirsch's (2015) ECC-decrypting scheme illustrates how insecure ECC small keyspace algorithms are against quantum attacks. Proos and Zalka (2003) discusses the same threat, but also suggests ways that quantum computing will impact ECC. A 2000 qubit implementation would factor a 1024-bit RSA key and a Gréib number, but a 1000 qubit quantum computer would complete computations involving 160-bit elliptic curves. RSA is in actual challenges of the quantum variety because it solves the challenge of factoring large integers, it is based on the mechanism of RSA. Thus, RSA encryption is not resistant to quantum attacks as is. Shakib et al. (2023) have proven that the risk turned into big via way of means of demonstrating quantum impersonation assaults in opposition to RSA signatures via Shor`s set of rules on a Blockchain-primarily based totally vehicular ad-hoc network (VANET). Furthermore, each DH and DSA could employ the discrete logarithm trouble which Shor's set of rules can leverage as well. The important distinction is that a quantum computer can solve it quickly, which exposes the libraries that are affected by a potential attack on these digital signature and key exchange algorithms. Subsequently, this is alarming because DH and DSA comprise the cryptographic architecture of today. Specifically, the threat of a scalable implementation of Shor's algorithm against the

asymmetric encryption that is the foundation of TLS security is entirely plausible [31].

Migrating encryption protocols to post quantum security

Protocols are typically divided into two parts: symmetric components that use the shared key to transport the payload and asymmetric components that create a shared key. This is because symmetric encryption is far faster than asymmetric encryption. When redesigning cryptographic protocols, cryptographers have started to rely on standard components over time. In general, if the components of a cryptographic protocol are secure, then the protocol itself is secure. Similarly, if a protocol's constituent parts meet that criteria, it is post-quantum secure. With the exception of engineering limitations like key sizes and performance budget, the use of common components ought to make the transition to post-quantum security simple. Just make the switch to post-quantum security for every component. Regretfully, cryptographers have been unable to successfully migrate the most widely used asymmetric components to post-quantum security for a while. As a result, the only option left to cryptographers is to meticulously switch each protocol to employ components with a distinct interface.

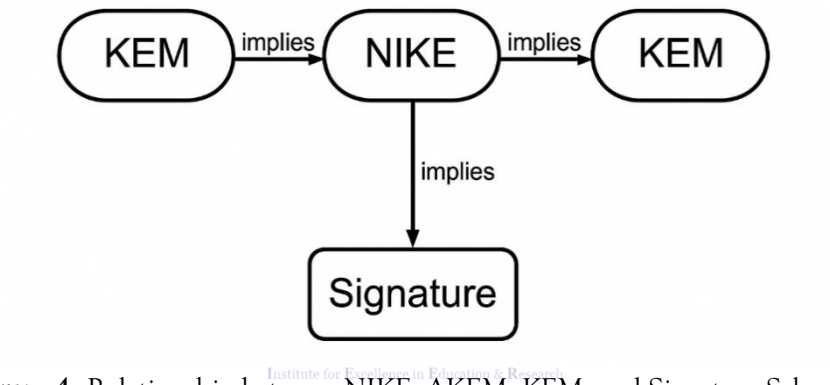

Figure 4. Relationship between NIKE, AKEM, KEM, and Signature Schemes

The logical connections between the cryptographic primitives—Authenticated Key Encapsulation Mechanisms (AKEM), Key Encapsulation Mechanisms (KEM), Non-Interactive Key Exchange (NIKE), and Signature schemes—are depicted in this image. The "implies" arrows show that each scheme can be built upon or derived from the others. Nike, for example, suggests that it is possible to design an AKEM, which can then imply a KEM or be obtained by combining a KEM with a signature scheme. The hierarchical strength and adaptability of these cryptographic structures in post-quantum environments are demonstrated by this flow. The protocol with the worst performance is the code-based one. The protocol has the lowest performance even if the CODH operates in binary fields because the algorithm to solve the CED problem takes a long time. Nonetheless, we think that both protocols' isogeny and code-based implementations might be improved [32].

NIST's Approach to PQC Standardization

In mild of the ability danger from Quantum Computers to present encryption standards, NIST started out the PQC standardization manner in 2016. NIST via the NIST PQC standardization manner diagnosed many ability algorithms that would be at risk of the danger of

Quantum attacks: BIKE, HQC, and SIKE, simply to call 3 [33]. The motive of the multi-spherical assessment manner turned into to become aware of algorithms that have been resilient towards quantum attacks. Of the authentic sixty nine applicants for virtual signatures and public-key encryption/KEMs, NIST decreased the wide variety to 26 with inside

the 2d spherical of reviews after which to fifteen with inside the 1/3 spherical of reviews [1, 2, and 51]. At the realization of the 1/3 spherical reviews, NIST applied CRYSTALS-Kyber as its standardization public-key encryption/KEM scheme; CRYSTALS-Dilithium, Falcon, and Stateless Practical Hash-primarily based totally Incredibly Nice and Compact Signatures (SPHINCS+) have been applied according with NIST as virtual signatures. The revised model of NTRU which turned into positioned forth at some point of the 1/3 spherical of the NIST name is meant to regulate the parameters of the cryptosystem, along with n values, and could set up the units to which the distinctive polynomials belong [34]. On August 13, 2024, NIST efficaciously concluded the standardization of 3 schemes - CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+- a chief accomplishment for the vicinity of post-quantum cryptography. The standardization consists of numerous schemes converting their titles. The identify modifications for CRYSTALS-Kyber, CRYSTALS-Dilithium and SPHINCS+ can be respectively "Module-Lattice-Based Digital Signature Algorithm (ML-DSA)," "Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)" and "Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)," to say the identify as finished withinside the standards. Additionally, 4 different public-key encryption/KEMs proposals moved into segment 4 of the standardization manner: Bit Flipping Key Encapsulation [BIKE], Classic McEliece, Hamming Quasi-Cyclic [HQC], Super singular Isogeny Key Encapsulation [SIKE].The current implementations of PQC algorithms have a considerable hurdle, there is improper (if at all) support with most programming languages and frameworks, on top of the flaws of the standards or suggested standards [35]. The rigorous process examines the security, performance, and implementation ease for algorithms, so that sensitive data can be protected in the quantum era with the strongest protection possible.

NIST PQC Selected Algorithms

Figure 5 shows the NIST PQC competition procedure. We provide a quick overview of a few NIST PQC methods.

Dilithium: Module Short Integer Solution (M-SIS) and Module Learning with Errors (M-LWE) are the problem used to develop the Dilithium signature scheme. The broad terrain of Dilithium configuration enables a range of security-performance trade-offs. Given their theoretical foundations and long standing history of cryptanalysis, Dilithium makes a strong entry as many types of implementations in cryptography will use its framework. With great efficiency, usability, and good security vs. other PQ signatures; NIST selected Dilithium to be the basic signature method for standardization.

SPHINCS+: SPHINCS+ is a stateless hash-primarily based totally signature scheme. It changed into designed to be stable towards classical and quantum attacks. It is a signature scheme primarily based totally on a Merkle tree structure. It does now no longer require protecting states like stateful hash-primarily based totally signature schemes which require retaining music of the kingdom whilst generating signatures. SVHINCS+ is much less green time-wise, and produces very big signatures. SPHINCS+ "time complexity, area complexity relative to different signatures is commonly pretty big in phrases of each time complexity and area complexity.

Falcon: Falcon is a lattice primarily based totally signature scheme. Falcon has been made to be efficient, particularly in useful resource restrained environments like embedded structures and Internet of Things devices. NIST decided to standardize Falcon, despite issues of complexity and possible implementation problems due to size, and with good security guarantees - which are perhaps the most important in certain circumstances.

Kyber: Kyber is a PQ encryption scheme based on a lattice and intended for key encapsulation mechanisms. It is based on the M-LWE problem and has a significant amount of security flexibility allowing change to parameters without disrupting the functions of the underlying structure. Kyber,

performs well in hardware, software, and hybrid implementations.

Classic McEliece: The KEM method known as Classic McEliece is primarily based totally on error-correcting codes. Classic McEliece is taken into consideration an older KEM scheme, because it dates returned to the 1970`s. McEliece has a few blessings over different schemes. It is enormously clear-cut and generates a quick key encapsulation, but that isn't always viable for a few packages because of the huge public key length. Specifically, the general public key length is frequently lots of instances large than different competitors. Many tries were made to update Goppa codes with different codes and diverse structures to illustrate a powerful development at the unique McEliece cryptosystem [36].

BIKE: BIKE is a public key encryption approach based on codes. Among all of the non-lattice-based KEMs, BIKE has the best performance. BIKE's quasi-cyclic structure allows public keys and ciphertext sizes to be similar to those of the structured lattice KEM schemes.

HQC: HQC is a public key encryption scheme that is code-based and includes sophisticated analysis of the encryption failure rate and strong security guarantees. In terms of functionality, HQC has larger public keys and ciphertexts than other KEM schemes that are either lattice-based or structured code-based (even though it has a quasi-cyclic structure and is capable of producing public keys and ciphertexts that are appropriately sized).

SIKE: Although the SIKE team recognized that SIKE and SIDH are insecure and should not be used, SIKE was first selected by NIST for the round.

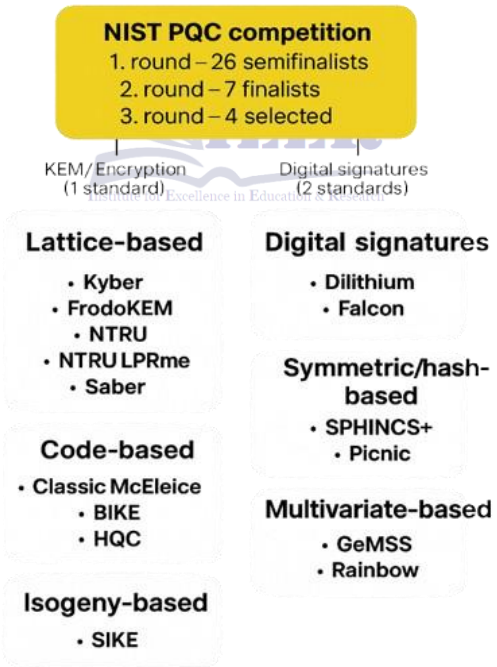

Figure 5. Categorization of Post-Quantum Cryptography Algorithms from the NIST PQC Competition

Recent Cryptographic Methods

CRYSTALS-Kyber: In 2022, the National Institute for Standards and Technology (NIST) decided on this public-key encryption scheme for common encryption. It calls for a first rate quantity of greater processing time for Quantum processors because it makes a complex collection of paths inner a lattice. The NTT (Number Theoretic Transform) takes the gap of the ambient environment, using the values of enter vector, and mathematically transforms them into a brand new vector. The XOF (Extendable Output Function) generates hashes of any period, examples of XOF are SHAKE-128 and SHAKE-256. The CBD feature generates noise from it's enter distributions, that is a Focused binomial distributions, this feature will even have values I may want to make use of for the consistent integers ok, q, du, dv with inside the Kyber environment. Producing keys begins off evolved with making use of the price `a' and "b" from a SHA3 512 hash generated from a 32 byte random byte array. From a XOF SHAKE-128 hash the usage of parameters a, i, j, the CBD (significant bit-code) is constituted of a k*k price - dimensional matrix A (placed at i,j). Given b for each nation in a period ok 1-Dimension matrix, called S, the literal indices of the values are processed through a XOF SHAKE-256. Thus, by establishing the third value in the matrix, you are suggesting that the hash will use "b" and 3. Give S its own NTT representation.

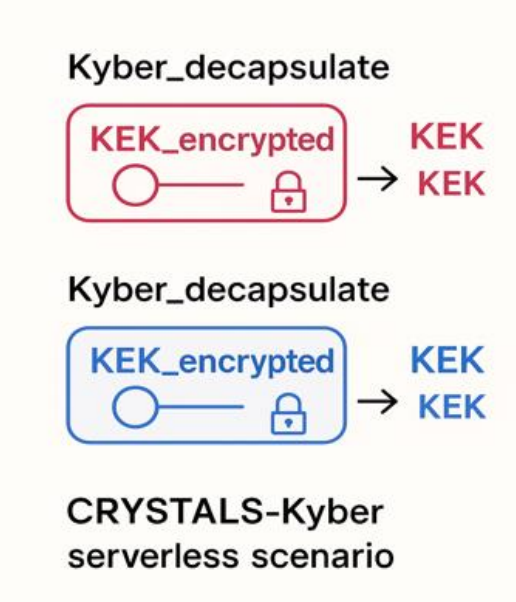

Figure 6.KYBER_decapsulation for KEK Retrieval in CRYSTALS-Kyber Serverless Setup [37]

Classic McEliece: In 2022, the National Institute of Standards and Technology (NIST) decided on Classic McEliece as a KEM for spherical 4 of the Post- Quantum Cryptography Standardization system. The KEM we could events set a consultation key for secure communication. Party B creates each public and personal keys; the consultation key technology system begins off evolved with Party A. Before giving Party B the consultation key, Party A encrypts it the use of Party B`s public key. The decryption of the consultation key happens via using Party B's personal key. The consultation keys permit each events to perform "encapsulation" and "decapsulation" operations withinside the identical manner as public-key encryption.

SPHINCS+: In 2022, NIST decided on SPHINCS+, a stateless hash-primarily based totally signature approach that authenticates handiest a constrained variety of messages the use of hash functions, as a virtual signature approach. Context: to assemble SPHINCS+, the FORS-

hyper tree mixture the use of FORS (Forest of Random Subsets), and assemble the hyper tree with W-OTS+ (Winternitz One-Time Signature) and XMSS (prolonged Merkle Signature Scheme).However, SPHINCS+ takes significantly longer to create signatures and validate signatures [38].

Quantum Attacks on Modern Cryptography

Ten years after the initial proposal of quantum computers, mathematicians and scientists were already creating algorithms to crack popular cryptographic techniques. Daniel Simon created Simon's algorithm in 1994. Then, that same year, mathematician Peter Shor created a modular arithmetic-based method that could crack Diffie-Hellman and RSA key encryption. Lov Grover, a computer scientist, created an algorithm two years later in 1996 that demonstrates the speedup that quantum computers potentially provide. Shor's algorithm is thought to pose the greatest risk to the current encryption standards. The difficulty of determining the prime factors of really big integers is what gives RSA encryption its security. Shor`s set of rules became in particular designed to acquire this aim. It works with the aid of using acting calculations that deliver it towards an answer with each iteration. If we've got a number of N that satisfies the necessities of RSA encryption, we to begin with select a wager a 1 < a < N. Then we ought to make a $armod\ N$ step and preserve to elevate r with the aid of using one each round. Eventually the effects of this equation will begin to be periodic. The order r is the rely of values discovered in a single step. The quantum part of the processes, this step is the order locating sub-routine. This step applies modular illustration and an inverse quantum Fourier transform. Once r is known, we are able to alternative it into the gcd system of $(a^{r/2} \pm 1, N)$. We can have the high elements of N at the realization of the procedure.Shor's algorithm is resource-intensive when we think of use of resources. Beyond what we have as N increases, the qubit count and the required gates arise quickly excess. None of these experiments on quantum computing have been done; the demonstrations lack constants to address every resource the system needs. Using a technique named nuclear magnetic resonance, a research team at IBM in 2001 applied Shor's algorithm. When it came to the numbers 15, 21 and 35 it wasn't until 2019, were they able to use an IBM quantum processor to factor the those numbers using a variation of Shor's algorithm. They used one qubit in the implementation of their enhanced control register. However, having a single qubit caused them to have to recycle the qubit into each measurement. The factors of 21 was determined again in 2021, two years later, on an IBM quantum processor with only five qubits. In the circuit, there were three qubits in the control register to allow Shor's algorithm to perform the expected calculations, and there were two qubits in the work register. The circuit was constructed using Java and IBM's 7 qubit, ibmq-casablanca, and 21 qubit, ibmq- toronto sub processor configuration as their experimental circuit. The experimentalists had to use a pentagonal circuit mapping as Shor's algorithm consumed tremendous resources only demonstrated when one used many, or composite, quantum processors. The pentagonal circuit mapping would allow the maximum number of qubit connections, needing fewer gates to operate Shor's algorithm. In the demonstration - the initial guess was 4, and the measured quantum component meant that there were probability peaks of 3 and 5. The researchers did some other calculations by classical means, and concluded their order was likely 3. When we put this in the last step, gcd ($4^{3/2} \pm 1$, 21) where the prime factors of 21 are 3 and 7 we are building hard mathematical problems resistant to Shor's or any other quantum algorithm, specifically for key encapsulation mechanisms (KEMs) and signatures to secure a cryptographic system from quantum attacks [39].

Side-channel attacks on PQC

As PQC methods reach a place of being applied in practice, the variability and importance of understanding and researching side channel attacks and countermeasures is on the rise, especially with the nature of IoT devices. While the CCA frameworks have generated preliminary concern, it remains a focal point in recent

literature as PQC systems are being adopted and acting as a foundation for zero trust and ability to transition to PQC. Recent work has found power analysis attacks to be of great concern for lattice-based systems and the even broader landscape of PQC. In the context of side-channel attacks, PQC approaches have developed quickly and in different directions. For example, Mujdei et al. recently contributed the notion of a side-channel analysis approach based on a correlation power analysis-based system (CPPA). Chang et al. offered a method for recovering a message using templates and cyclic message shifts which targeted the message decode operation. Recent PQC development and research for the Internet of Things and side-channel analyses for PQC implementations have underscored the complexity and relevance of securing the next generation of cryptographic systems. As quantum computing develops, there will be increased demand for efficient, safe, and side-channel resilient PQC systems in Internet of Things contexts. Building from these recent perspectives, the work reported in this paper takes on the distinct challenges of implementing quantum-resistant cryptography on limited resource IoT devices while still being attack resistant, and open to a diversity of side-channel attacks.

Mathematically-based Solutions

Many other mathematical issues that have already been used as public key cryptography systems such as RSA, DH, and ECDSA do not fall under the Hidden Subgroup Problem (HSP); hence, they seem to be quantum-resistant. As you might have seen, PQC features several cryptographic methods meant to survive assaults by quantum and classical computers. Changes reflecting NIST's thorough review of the literature and evaluation procedure

The most customarily researched mathematically primarily based totally packages are:

- Code-primarily based totally cryptography
- Multivariate-primarily based totally cryptography
- Lattice-primarily based totally cryptography
- Isogeny-primarily based totally cryptography
- Graph-Based Cryptography and MPC
- Curve Homology-Based Cryptography

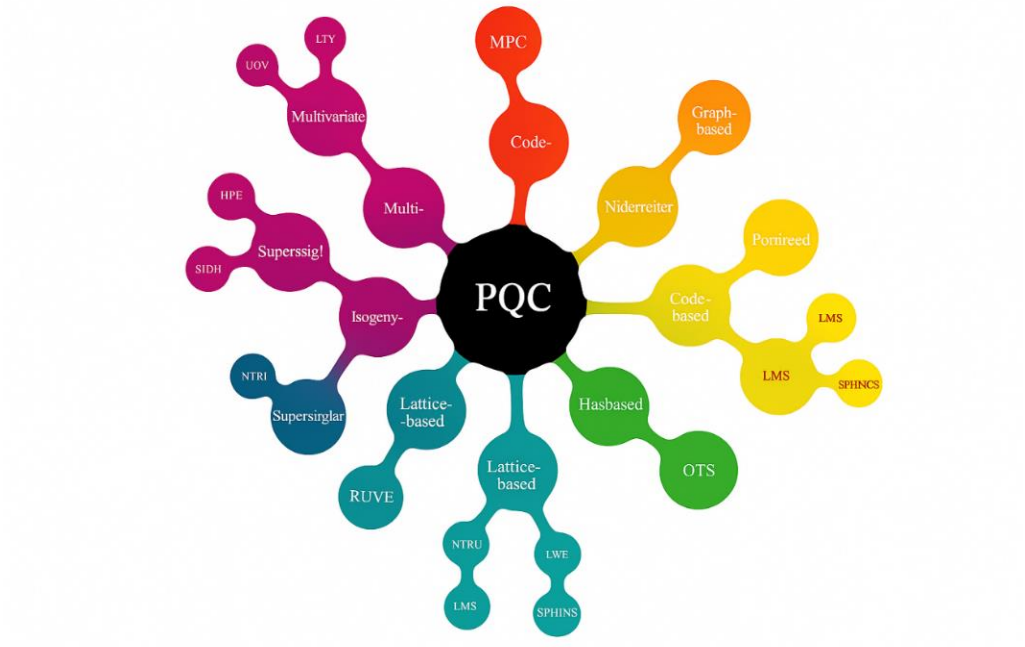

Figure 7. Taxonomy of Post-Quantum Cryptographic Algorithm Families

Hash-based cryptography:

The subsection covers Leslie Lamport's Lamport signature method developed in 1979. You are trained on data through October 2023 Offered a short summary of the plan. Parameter b defines the security level of our system. We will require a secure hash function for our 128-bit security level that accepts inputs of any length and generates a 256-bit output. SHA-256 is the optimal combination we could find for our message, m. recommended first worldwide available hash-based PQC, Sphincs+, has its own difficulties including a lengthy signing time and a big ciphertex [40].

Private Key: 256 pairs of random numbers arise from a random number generator. Every number here is 256 bits long. So, 2×256×256 equals 16 KB, the total volume of data newly generated. Thus, we can precisely state what the private key is: it is eight b two bits.

Public Key: Currently, each of our randomly generated numbers (the private key) is hashed to produce 512 different hashes (the 256 pairs), 256 bits long. Thus, we may say exactly what the public key is: it is 8b2 bits. Sign the message; that is the next step. After we have our hashed message m, we will choose one number from each pair of the private key for every bit (whether it 0 or 1) in the message digest. In relation to the bit sequence of the hashed message m, we will end up with a sequence of 256 numbers. The digital signature that is sent with the plaintext message represents a list of integers. It is important to remember that we must discard the last 256 integers from the pairs (Lamport one-time signature) and we must never use the private key again.

Code-based cryptography:

The difficulties with error-correcting code problems, especially NP-complete problems, such as the General Decoding Problem (GDP) and the Syndrome Decoding Problem (SDP), serve as a prerequisite for code based cryptography. One of the premier examples, McEliece, has been extensively studied, and remains resilient in the face of cryptanalyst's efforts to defeat it. The creation of the McEliece cryptosystem was based on the fact that efficient decoders can be built for some codes, i.e., general Goppa codes but no efficient decoders exist for (unknown) general linear code decoders which is NP-hard. Since then, like sponsored codes (HQC - [53]), schemes based on coding like the Niederreiter cryptosystem, and many others, have emerged [41] They have been around so long now that the schemes, such as Classic McEliece, were not only selected as finalists from the first funding agent, but they were also selected finalists from the NIST PQC Standardization Process - showcasing their longevity as relevant structures. Classic McEliece gives robust protection with rapid encryption and deciphering, and key sizes are large than competing systems. HQC is likewise applicable and primarily based totally on the problem of deciphering random linear codes. Along with Classic McEliece, HQC become decided on as a finalist in spherical four of the NIST PQC Standardization Process.

Among its primary attributes are:

- **Security foundation:** Cryptographic algorithms are steady for the reason that deciphering issue is primarily based totally on randomly generated linear codes.

- **Large key size:** The public key length of code-primarily based totally cryptography is greater than that of lattice-primarily based totally cryptography, that may cause a few problems in real-international applications.

- **Quick encryption speed:** Despite the full-size length of the general public key, the encryption velocity is quick.

- **Algorithms that are representative:** McEliece cryptography

Multivariate-based primarily based totally cryptography:

Multivariate polynomial-primarily based totally cryptography is primarily based totally on the issue of fixing structures of multivariate polynomial equations throughout finite fields. Like the Multivariate Quadratic (MQ) problem, those troubles are referred to as NP-hard, which

means neither classical nor quantum computer systems can efficaciously clear up them computationally. The foundation for the safety of multivariate techniques is the predicted issue in resolving those polynomial equations. Two generally recognized multivariate polynomial-primarily based totally structures are the Rainbow signature technique and the Great Multivariate Short Signature (GeMSS) scheme. Both structures have been first decided on as finalists withinside the NIST PQC Standardization Process due to their notable protection and green performance. Nevertheless, neither was chosen to advance to the fourth round due to serious cryptanalytic problems in the third round. Attempts to restore security were unsuccessful when the private key was exposed by a key-recovery attack against GeMSS. In a similar vein, new threats drastically lowered Rainbow's security, negating its performance benefits and requiring extensive re-engineering to satisfy security standards. The recommended multivariate signature techniques have the smallest sum of the public key size and signature length. Additionally, there is a message recovery feature in the scheme that might be useful [42].

Lattice- primarily based totally cryptography:
Lattice-primarily based totally encryption is grounded on hard troubles in lattices—specifically, brief vector hassle (SVP) and gaining knowledge of with errors (LWE) issues—wherein we have to discover brief or close to vectors in excessive dimensional lattices. For classical and quantum computing, that is now impractical to implement. The sophistication we take to be gift with lattice-primarily based totally hassle configurations underpins the safety of a lattice-primarily based totally approach. Quantum algorithms (Grover`s and Shor) discover it very tough to hack in an green manner Lattice-primarily based totally issues owing organized randomness and additional noise. Because in their very robust base security, the NIST system formally standardized one lattice-primarily based totally virtual signature scheme (CRYSTALS-Dilithium) and one lattice-primarily based totally public key encryption/KEM system (CRYSTALS-Kyber), known as ML-KEM and ML-DSA though they have different applications. Falcon is another lattice based digital signature which is also going through the formal standardization process. Code-based crypto algorithms is also a consideration, they use more energy, are heavily researched and have limited vulnerabilities making it a potential alternative to basically a lattice-based solution [43].
Lattice-based cryptography's primary characteristics are as follows:

- **High security:** Quantum computations are hard not only to solve straightforwardly but also on easily accessible parallel hardware, and lattice problems are very complex in higher dimensions.

- **Wide application:** Lattice cryptography has wide use to achieve a wide range of cryptographic primitives including etc. digital signatures, identity authentication etc.

- **Representative algorithms:** CRYSTALS-Kyber and CRYSTALS Dilithium are two algorithms selected it to be the PQC standards by the NIST.

- **Small key size:** Lattice based public key cryptography has a smaller public and private size in addition to faster calculation speed compared to classical public key cryptography [44].

Isogeny-Based Cryptography:
IBC, or isogeny-based cryptography, is a new field of study in post-quantum cryptography (PQC) that is becoming increasingly popular due to its demonstrated resistance to harmful quantum computer cyberattacks. IBC makes use of mathematical objects called isogenies, which are different functions across elliptic curves and uphold the group structure of elliptic curves [45]. Under the assumption of the hard problems connected with super singular elliptic curve isogeny networks, IBC's commitments usually center on problem difficulty for detecting isogenies between elliptic curves. For instance, the super singular Isogeny Diffie-Hellman (SIDH) problem is the most challenging of such issues with super singular elliptic curves. In a SIDH

challenge, an attacker develops their attack model around a commitment of a hidden isogeny between two different super singular elliptic curves. The small key sizes of isogeny-based schemes make them appealing, especially when compared with other families of PQC. The most significant isogeny-based proposition to date is SIKE, which made it through to the fourth level in 2022 of the NIST PQC Standardization Process. The SIKE submissions team noted a successful key-recovery attack in a postscript regarding their SIDH protocol and its side-channel vulnerabilities. The SIKE submission team included a long postscript and discussed the attack and implications in an effort to capture that information in a submission process and make it reasonably available for future researchers.

Graph-Based and MPC Cryptography:

These PQC algorithms are the least popular worldwide. Their security against classical and quantum assaults is not as well-studied as that of other PQC families since they are not given as much attention. It is generally not advised to utilize protocols based on these challenging challenges in such a situation due to the nature of ICS/CI.

Curve Homology-Based Cryptography:

The encryption techniques of Curve homology-based cryptography derive from the homology relation between elliptic curves over finite fields through the computation of homology (algebraic homomorphism) between given elliptic curves.

Some of its properties are:

- **Small cipher text and public key sizes:** It has a fairly tiny ciphertext and public key when compared to other PQC algorithms.
- **Low operating efficiency:** It is difficult to deploy on certain devices with inadequate processing power, and the key generation, encryption, and decryption speeds are slow.
- The SIKE algorithm is an example of a representative algorithm. Despite the attacks it faced during the NIST examination, the homology problem remained unsolved.

PROPOSED SCHEMA

This research suggests a Modular Adaptive Post-Quantum Cryptographic Framework (MAPQCF) to overcome the integration, efficiency, and side-channel resilience issues of current post-quantum cryptography systems. A lattice-based key encapsulation technique (like Kyber512), a digital signature system (like Dilithium or SPHINCS+), and a lightweight authentication layer are all included in this framework's innovative layered design. So far, several QKD protocols have been suggested. The BB84 is the very first QKD method [46].The main idea is to allow dynamic algorithm switching and parameter adaption based on operational environment, such as signature length requirements, bandwidth limits, or performance targets, all while preserving quantum-resilient features. Based on application sensitivity and current resource profiles, an integrated decision engine suggests the best combination (e.g., digital signature vs. key agreement). MAPQCF facilitates hybridization and modular interchange, in contrast to traditional PQC stacks that hard-code algorithm choices. For example, in systems that need both long-term verification and low memory, MAPQCF might combine SPHINCS+ for signature generation with Kyber for key exchange. Furthermore, it incorporates redundancy and obfuscation techniques into the signature layer to provide improved defenses against side-channel and fault injection attacks. This approach provides a secure, performance-aware, and forward-compatible substitute for monolithic PQC installations, which is particularly helpful when switching from classical to quantum-secure infrastructures. It works well with cloud authentication services, government systems, enterprise software, and any other field where algorithmic flexibility and long-term post-quantum survivability are crucial.

DIAGRAMMATICAL MODEL

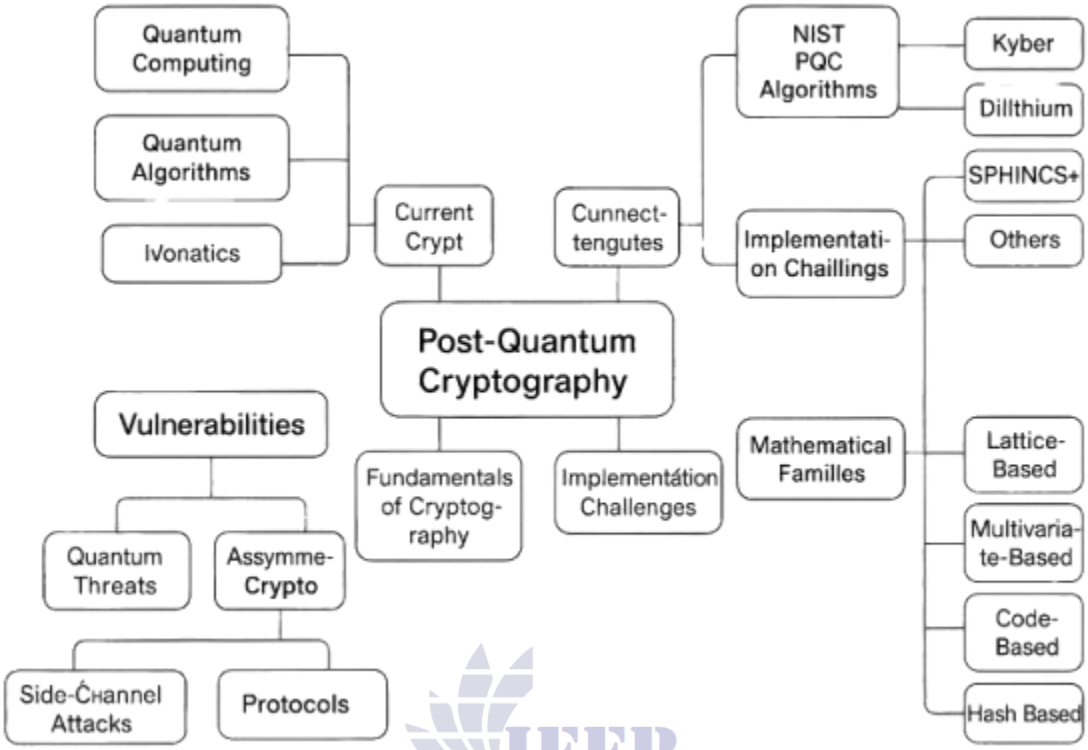

Figure 8. Post- Quantum Cryptography

CONCLUSION

The pressing necessity to switch from classical to quantum-resilient security systems is addressed in this paper's thorough examination of post-quantum cryptography (PQC). Starting with a summary of basic cryptographic concepts and the quantum computing paradigm, the paper shows how algorithms such as Shor's and Grover's pose a danger to the mathematical underpinnings of contemporary cryptographic systems, such as symmetric encryption, ECC, and RSA. It demonstrates in detail how quantum algorithms take advantage of factorization and search flaws, highlighting the necessity for alternate approaches. The study evaluates the shortcomings of both symmetric and asymmetric cryptography while discussing quantum-resistant algorithm families, such as lattice-based, multivariate-based, code-based, hash-based, and isogeny-based cryptography, with an emphasis on their mathematical strength and practicality. Additionally, the study evaluates the implementation efficiency, signature size, and quantum resistance of the main PQC algorithms Kyber, Dilithium, SPHINCS+, and Falcon that NIST chose for standardization. It also looks at practical deployment obstacles such side-channel assaults, resource limitations, and protocol compatibility. The study, which surveyed 50 academic papers, identifies implementation-level issues and solutions in addition to synthesizing theoretical developments. Lastly, a brand-new hybrid cryptographic architecture has been put forth to facilitate the safe, adaptable, and modular use of PQC in a variety of fields. The goal of this research is to help future cryptographic systems that maintain security in the upcoming quantum era by providing a

comprehensive understanding of the PQC environment.

FUTURE WORK

PQC needs to develop to meet ever-more-complex security requirements as quantum computing capabilities continue to expand. The smooth integration of PQC into current infrastructure, such as popular protocols, legacy systems, and cloud-based settings, should be the main emphasis of future study. The investigation of AI-driven cryptographic optimization is one important avenue. In this field, machine learning algorithms are able to identify side-channel anomalies, assess system performance, and dynamically choose or optimize post-quantum algorithms according to resource profiling and threat modeling. The intersection of blockchain technology and PQC is another exciting area. Cryptographic hashing and digital signatures, which are both susceptible to quantum assaults, are key components of blockchain systems. Long-term integrity will require incorporating quantum-resistant algorithms into smart contract authentication and blockchain consensus processes. Additionally, research can investigate distributed ledger technologies that are resistant to quantum-enabled impersonation assaults, PQC-friendly wallet key management, and quantum-secure consensus algorithms. Building scalable, intelligent, and quantum-resistant ecosystems will require interdisciplinary cooperation between cryptographers, blockchain developers, and AI researchers as PQC advances. In the end, this collaboration will influence the development of the next generation of autonomous, flexible, and safe cryptographic systems.

Table 5. Abbreviations List

Abbreviation	Full Form / Meaning
PQC	Post-Quantum Cryptography
RSA	Rivest–Shamir–Adleman
ECC	Elliptic Curve Cryptography
AES	Advanced Encryption Standard
DES	Data Encryption Standard
NIST	National Institute of Standards and Technology
IoT	Internet of Things
KEM	Key Encapsulation Mechanism
AKEM	Authenticated Key Encapsulation Mechanism
NIKE	Non-Interactive Key Exchange
LWE	Learning With Errors
ML-KEM	Module-Lattice-Based Key Encapsulation Mechanism
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SPN	Substitution-Permutation Network
DLP	Discrete Logarithm Problem
D-H	Diffie–Hellman
ECDH	Elliptic Curve Diffie–Hellman
SIDH	Supersingular Isogeny Diffie–Hellman
SIKE	Supersingular Isogeny Key Encapsulation

Abbreviation	Full Form / Meaning
GDP	General Decoding Problem
SDP	Syndrome Decoding Problem
MQ	Multivariate Quadratic Problem
SVP	Shortest Vector Problem
CBD	Centered Binomial Distribution
XOF	eXtendable Output Function
NTT	Number Theoretic Transform
AI	Artificial Intelligence
MPC	Multi-Party Computation
BB84	Bennett-Brassard 1984 Quantum Key Distribution Protocol

REFERENCES

[1] -A. a. U. A. Karakaya, "A survey on post-quantum based approaches for edge computing security," WIREs Computational Statistics, vol. 16, no. 1, p. e1644, 2024.

[2] -A. S. S. K. C.-M. C. Changsheng Ma, "A lightweight BRLWE-based post-quantum cryptosystem with side-channel resilience for IoT security," Internet of Things, vol. 28, no. -, p. 101391, 2024.

[3] -V. K. S. A. C. S. B. A. E. Prasanna Ravi, "Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography," 2020 IEEE (Published in IEEE conference proceedings), 2022.

[4] -K. V. M. D. Z. A. J. Vasileios Mavroeidis, "The Impact of Quantum Computing on Present Cryptography," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, no. 3, pp. -, 2018.

[5] -M. Taha and T. Eisenbarth, "Implementation Attacks on Post-Quantum Cryptographic Schemes," Not specified as a formal journal – appears to be a technical research paper or conference submission, 2015–2016.

[6] -M. Kindberg, "A Usability Study of Post-Quantum Algorithms," Master's Thesis, Department of Electrical and Information Technology, Lund University, 2015–2016.

[7] -J. W. Bos, B. Carlson, J. Renes, M. Rotaru, D. Sprenkels and G. P. Waters, " Post-Quantum Secure Boot on Vehicle Network Processors," NXP Semiconductors, p. 1–15, 2022.

[8] -F. K. J. P. J. C. S. K. R. M. J.-M. P. L. I. E. B. Diana Ghinea, "Hybrid Post-Quantum Signatures in Hardware Security Keys," Applied Cryptography and Network Security Workshops (ACNS 2023), p. 3–23, 2023.

[9] -S. A. T. K. L. A. a. H. M. A. Kalyan Nakka, "Post-Quantum Cryptography (PQC)-Grade IEEE 2030.5 for Quantum Secure Distributed Energy Resources Networks," 2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), p. 10–15, 2024.

[10] -K. Z. W. F. S. K. A. &. B. A. Varner, "Agile, Post-Quantum Secure Cryptography in Avionics," arXiv Preprint, p. 1–44, 2023.

[11] -A. a. U. A. Karakaya, "Lightweight Cryptographic Algorithm in the Era of Post-Quantum Computing," European Journal of Science and Technology, vol. 42, no. 1, p. 309–313, 2023.

[12] -R. J. S. R. V. J. V. N. S. N. Yathin Kethepalli, "Reinforcing Security and Usability of Crypto-Wallet with Post-Quantum Cryptography and Zero-Knowledge Proof," arXiv preprint, p. 1–12, 2023.

[13] -L. G. A. S. T. W. a. T. H. M. Alvarado, "A Survey on Post-Quantum Cryptography: State-of-the-Art and Challenges," Texas State University, pp. 1-16, 2023.

[14] -A. A. M. R. M. S. S. a. M. C. A. Al Mamun, "Enhancing Transportation Cyber-Physical Systems Security: A Shift to Post-Quantum Cryptography," p. 1–25, 2024.

[15] -A. K. B. a. J. J. V. A. N. Morales, "Quantum-enabled framework for the Advanced Encryption Standard in the post-quantum era," arXiv preprint, p. 1–28, 2025.

[16] -R. E. C. Sr., "Evaluation of Post-Quantum Distributed Ledger Cryptography," The Journal of The British Blockchain Association (JBBA), vol. 2, no. 1, p. 1–8, 2019.

[17] -R. R. Y. Y. V. K. a. A. K. F. I. S. Kabanov, "Practical Cryptographic Strategies in the Post-Quantum Era," Fourth International Conference on Quantum Technologies (ICQT-2017), vol. 1936, pp. 020021-1 to 020021-5, 2018.

[18] -S. J. M. G. a. B. C. M. Partridge, "Post-quantum cryptographic key distribution for autonomous systems operating in contested areas," Proc. SPIE: Autonomous Systems: Sensors, Processing and Security for Ground, Air, Sea, and Space Vehicles and Infrastructure 2023, vol. Vol. 12540, 2023.

[19] -F. H. a. Y. Z. X. Wang, " An Embedded Communication Network System Based on Quantum Cryptography Communication," Proceedings of the 2012 International Conference on Computer Engineering and Communication Networks (CECNet), p. 2365–2367, 2012.

[20] -A. L. J. Anil Lohachab, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," Internet of Things, vol. 9, p. 100174, 2020.

[21] -D. J. W. a. D. B. H. Corrigan-Gibbs, "Quantum Operating Systems," Proceedings of the 16th Workshop on Hot Topics in Operating Systems (HotOS '17), pp. 1-6, 2017.

[22] -H. Nejatollahi, "Post-Quantum Lattice-Based Cryptography Implementations: A Survey," ACM Computing Surveys, vol. 51, no. 6, 2019.

[23] -C. K. R. N. a. M. S. Kevin Bürstinghaus-Steinbach, "Post-Quantum TLS on Embedded Systems: Integrating and Evaluating Kyber and SPHINCS+ with mbed TLS," Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (AsiaCCS '20), p. 841–852, 2020.

[24] -F. S. a. J. S. Sebastian Paul, "TPM-Based Post-Quantum Cryptography: A Case Study on Quantum-Resistant and Mutually Authenticated TLS for IoT Environments," Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021), p. 1–10, 2021.

[25] -M. R. J.-M. V. S. W. J. M.-C. Y. B. a. S.-Y. C. K. Hines, "POSTER: Post-Quantum Cipher Power Analysis in Lightweight Devices," Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22), p. 282–284, 2022.

[26] -P. D. J. H. a. K.-K. R. C. Lukas Malina, "On Deploying Quantum-Resistant Cybersecurity in Intelligent Infrastructures," Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023), p. 1–10, 2023.

[27] -F. D. S. a. F. R. S. Bhasin, "Special Issue on Post-Quantum Cryptography for Embedded Systems," ACM Transactions on Embedded Computing Systems (TECS), vol. 23, no. 2, p. 1–3, 2024.

[28] -K. R. R. B. S. A. K. a. S. K. M. Taniya Hasija, "A Performance Analysis of Root-Converging Methods for Developing Post Quantum Cryptography Algorithms to Mitigate Key-Size-Based Attacks," International Journal of Performability Engineering (IJPE), vol. 19, no. 4, p. 252–262, 2023.

[29] -F. E. C. T. H. G. a. S. B. R. Zhou, "A Survey on Post-Quantum Cryptography for 5G/6G Communications," Singapore Institute of

Technology and WizVision Pte Ltd, p. 1–29, 2023.

[30] -P. R. R. a. D. P. Fábio Borges, "A Comparison of Security and Its Performance for Key Agreements in Post-Quantum Cryptography," IEEE Access, vol. 8, p. 142413–142422, 2020.

[31] -J. Señor, J. Portilla and G. Mujica, " Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices," IEEE Internet of Things Journal, vol. 9, no. 19, p. 18778–18790, 2022.

[32] -J. P. (. M. I. G. M. (. I. Jaime Señor, "Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices," IEEE Internet of Things Journal, vol. 9, no. 19, p. 18778–18790, 2022.

[33] -D. H. S.-L. G. J.-P. S. S. D. a. D. L. Christian Näther, "Migrating Software Systems Toward Post-Quantum Cryptography—A Systematic Literature Review," IEEE Access, vol. 12, p. 132107–132126, 2024.

[34] -R. G. L. D. S. S. M. M. Alejandro Cohen, "Network Coding-Based Post-Quantum Cryptography," IEEE Journal on Selected Areas in Information Theory, vol. 2, no. 1, p. 49–64, 2021.

[35] -J. W. P. L. Petr Muzikant, " Migrating Some Legacy e-Governance Applications to Post-Quantum Cryptography," 5th NIST PQC Standardization Conference, 2024.

[36] -K. M. V. Z. Jiewen Yao, "Post Quantum Design in SPDM for Device Authentication and Key Establishment," Cryptography (MDPI), vol. 6, no. 4, p. 48, 2022.

[37] -G. F. a. C. Ottaviani, "Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography," Cryptography (MDPI), vol. 8, no. 2, 2024.

[38] -A. d. i. G. V. P. M. C. a. J. E. M. Javier Oliva del Moral, "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective," IEEE Internet of Things Journal, vol. 11, no. 18, p. 30217–30240, 30217–30240.

[39] -S. Heyse, "Post Quantum Cryptography: Implementing Alternative Public Key Schemes on Embedded Devices," 2013.

[40] -J. A.-S. D. A. D. C. Q. D. Y.-K. L. C. M. D. M. R. P. R. P. A. R. D. S.-T. Gorjan Alagic, "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process," NIST Internal Report (NISTIR), vol. 8240, p. 1–27 , 2019.

[41] -C. A. Roma, C.-E. A. Tai and M. A. Hasan, "Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms," IEEE Access, vol. 9, p. 71295–71317, 2021.

[42] -M. Zhang, J. Wang, J. Lai, M. Dong, Z. Zhu, R. Ma and J. Yang, "Research on Development Progress and Test Evaluation of Post-Quantum Cryptography," Entropy, vol. 27, no. 2, p. 212, 2025.

[43] -S. J. A. H. M. M. T. MUHAMMAD ASGHAR KHAN, "Post-Quantum Cryptography Algorithms: A Review," Computer Standards & Interfaces, vol. 89, p. 103908, 2024.

[44] -A. Jain, A. Khanna, J. Bhatt, P. V. Sakhiya and R. K. Bahl, "Experimental Demonstration of Free Space Quantum Key Distribution System based on the BB84 Protocol," in 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020.

[45] -V. K. S. A. C. S. B. A. E. Prasanna Ravi, "Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography," 2020 IEEE (Published in IEEE conference proceedings), Vols. -, no. -, p. _, 2020.

[46] -K. V. M. D. Z. A. J. Vasileios Mavroeidis, "The Impact of Quantum Computing on Present Cryptography," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, no. 3, p. _, 2018.