iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78550

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Post-Quantum Cryptography for Secure Communication: A Systematic Review of Algorithms, Performance Trade-offs, and Emerging Challenges

Suvhodip Saha[1], Soumendu Banerjee[2]
[1,2]*Department of Computer Science and Engineering, Academy of Technology, Hooghly, West Bengal*

Abstract: ***The rapid growth of quantum computing poses a critical threat to classical cryptographic systems. That is due in large part to the fact that they represent efficient solutions for some of the most challenging mathematical problems such as integer factoring or finding discrete logarithms. Schemes currently in wide use including RSA, Diffie–Hellman, and elliptic curve cryptography are particularly susceptible to being attacked by quantum computers, using algorithms like Shor's Algorithm and Grover's Algorithm. The advent of post-quantum cryptography (PQC) provides a promising potential answer to providing long-term security from adversaries using quantum computing capabilities. This paper presents a comprehensive state-of-the-art review of various PQC techniques currently being researched, including lattice-based methods, code-based methods, multivariate methods, hash-based methods, and isogeny-based methods. key challenges that will need to be addressed include computational overhead, large key sizes and implementation complexity. Furthermore the study reviews the current standardization efforts by the National Institute of Standards and Technology related to PQC and discusses some of the very specific practical considerations that need to be considered before widely deploying these techniques. The paper concludes by a complete list of existing research challenges and proposed future work that will assist in the development of efficient and scalable systems that will resist attacks from quantum computers.***

Keywords- Post-Quantum Cryptography, Performance evaluation, Quantum Computing, NIST Standardization, Lattice-Based Cryptography, Code-Based Cryptography, Hash-Based Signatures, Quantum-Resistant Security.

I. INTRODUCTION

Modern digital communications use cryptographic algorithms for the transmission of information over open networks in a secure manner by providing confidentiality, integrity, and authentication of transmitted information. Most modern secure communication schemes (such as the RSA, Diffie-Hellman and the ECC) are built around the three basic classical cryptographic systems. They are widely used in all areas of secure communication including internet banking, cloud storage and secure messaging as well as digital signatures. The development of quantum computers however creates serious concerns regarding the long-term security of these established cryptographic systems. [1,2]

Quantum computers are able to utilize the principles of superposition and entanglement to perform certain calculations much faster than current classical computers. Shore's landmark quantum algorithm demonstrated how integer factorization and the discrete logarithm can be solved with polynomial time complexity on a sufficiently powerful quantum computer. [3,4] The exponential time reduction to solve a brute force attack against symmetric key cryptosystems from its classic brute force algorithm (such as AES) using Grover's Algorithm will have deleterious effects on the security of symmetric ciphertexts without substantially increasing the size of the symmetric key. [3,5] Together, these two pieces of information and the anticipated development of large scale (error tolerant) Quantum Computers strongly suggest that most public key cryptosystems will be compromised when quantum computers are available. Even though the development of large error tolerant Quantum Computers remains challenging, there are ongoing advancements in the quantum hardware and quantum algorithms, which suggests that they may become a reality in the future.[6,7] As such, it is an urgent research issue, because any sensitive information currently protected by classical cryptography may be collected/stored today by malicious entities, and they may then decrypt that information at some point in the future when Quantum Computers are available.

©IJRASET: All Rights are Reserved

Because of this scenario, organizations have shifted to a model of "harvesting now, decrypting later." As a result, there is growing interest in and need for cryptographic algorithms that do not only protect from classical attacks, but also protect from potential future attacks by quantum computers. [7,8] This has led to the development of Post-Quantum Cryptography (PQC) to address the issues that arise from current, commonly used and accepted methods of cryptography that rely upon classical technologies which will be subject to attacks from future quantum computing capabilities. Several types of post-quantum public key algorithms have been developed, such as Lattice Based Cryptography (LBC), Code Based Cryptography (CBC), Hash Based Signature (HBS), Multivariate Polynomial Cryptography (MPC) and Isogeny Based Cryptography (IBC). [9],[10] These methods rely on mathematical problems that are thought to be resistant to currently known quantum algorithms. While these new methods of establishing security will shape the future of secure communication and email, PQC does bring some problems, including increased size and complexity in hardware, reduced efficiency in computing and memory space requirements, and greater difficulty in implementation.

This paper is focused on the examination of how quantum computers will impact classical cryptography and how post-quantum cryptographic solutions may assist toward achieving secure communication going forward. The aim of this paper is to provide an overview of method approaches, provide insight into their security assumptions and the performance characteristics associated with them, and discuss the trade-offs associated with the practical deployment of methods. In addition, the paper reviews the ongoing post-quantum cryptography standardization efforts led by the National Institute of Standards and Technology (NIST), which play an important role in driving the global transition towards quantum-resistant cryptographic standards.

The rest of this paper is arranged as follows. The second section discussed about the of classical cryptographic algorithms in the context of quantum attack. The third section discussed about the Quantum Computing and application. The fourth section focuses on describing the main families of post-quantum cryptography including some of their key principles. The fifth section provides a review of NIST's standardization process for post-quantum cryptography including an overview of potential candidates for standards. Section sixth provides insight into the preprocessing of the research data, section eighth provides a summary of the findings and future prospect, while recommending that organizations implement quantum safety strategies to secure communications during the possibility of developing quantum computers and after the potential development of quantum computers, all while protecting themselves against any potential risk from these quantum computer technologies.

A. Major Contribution

1) An extensive comprehensive comparative review of the various techniques of post-quantum cryptography (PQC) available today, identifying each technique's strengths, weaknesses and deficiencies as evidenced by gaps in research.

2) The key performance metrics (security level, key size, computational efficiency, and implementation cost) are established and analyzed for each PQC algorithm.

3) The PQC standardization process of the National Institute of Standards and Technology (NIST) is detailed, with algorithms being mapped into their respective categories.

4) Research trend analysis via statistical methods is achieved by year-by-year publication analysis and visualization techniques.

5) Publication source dissemination patterns are analyzed in order to understand how research in this area is being disseminated throughout journals and conference proceedings.

6) A critical evaluation of the practical challenges of deploying PQC will be provided, such as those of scalability, equipment constraints, and integration issues.

7) Future research direction will be made with recommendations for developing efficient and secure quantum-resistant cryptography.

II. CRYPTOGRAPHY

The laws and techniques of cryptography are at the heart of all technology that secures the Internet, email and other online service and application operations, and transmits data and digital objects over unsecured or open Internet and mobile networks. Cryptographic techniques and methods also provide key services to data security, authorization and access control to sensitive information stored in many forms, including web browsers, e-mail, and online transactions.[11]

Cryptography is utilized by many kinds of real world applications. Secure communication is one of the major uses of cryptography whereby Encryption Algorithms are used to secure data sent from users to servers when utilizing cryptographic protocols such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Virtual Private Network (VPN). Another application of cryptography is to secure data stored in databases, cloud storage systems, personal portable devices and so on. Disk and database encryption techniques prevent unauthorised access to sensitive data even when storage systems are compromised [12].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Cryptography provides the basis for authentication and authorisation services for users, including the use of digital signatures, password hashing and multi-factor authorisation methods.

In addition, cryptography is extensively used in the banking, payment and cryptocurrency industry to ensure the security and dependability of online and mobile financial transactions, as well as the security of information shared and transmitted over the Internet. New technologies, such as the IoT, the blockchain, cloud computing and secure software updates, also depend heavily on a cryptographic foundation for secure operations and protection against cyber threats [13], [14]. As digital systems continue to expand, the importance of strong cryptographic solutions is becoming increasingly important.

Cryptography techniques consist of symmetric-key, asymmetric-key and hash functions.

A. Symmetric-key cryptography

With symmetric-key cryptography, two users share a private key which is used to encrypt and decrypt their respective messages. Symmetric-key algorithms are known for their extremely fast processing speed and large data capacities to encrypt. The most commonly used symmetric-key algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Triple Des (3DES). While symmetric systems are fast and efficient, the challenge with symmetric systems lies with securely distributing and managing the associated secret keys between communicating parties.[15]

B. Asymmetric-key cryptography

Key pairs in asymmetric (also known as public key) cryptography are mathematically associated. Asymmetric-key cryptography employs an asymmetric public key to encrypt messages and a private key for decrypting messages. Since the public key can be distributed more easily than the private key, there are additional security features provided by public keys including providing digital signatures and securely transmitting keystrokes between different users. The most common asymmetric-key cryptographic algorithms are RSA, Diffie-Hellman and ECC (Elliptic Curve Cryptography). The strength of all asymmetric keys lies in that current computational methods do not provide an effective way to solve the mathematical equations related to these algorithms, namely integer factoring and the discrete logarithm problem. It is possible that in the future, quantum computers can solve these problems. [16]

C. Cryptographic hash function

All outputs from a cryptographic hashing function will always be produced with the same specific length, called the "hash value". A cryptographic hashing function is intended to be impossible to reverse engineer (one-way), and has no probability of producing identical output values from two distinct inputs (collision-resistant). Therefore, hashes can be used for verifying the integrity of information; to store passwords (without being disclosed) and to use for creating a digital signature, Keys uses by SHA-256 and SHA-3, These are hash functions that were standardized by NIST, the U.S. Government Agency that specializes in creating security standards and is used widely in various security protocols and in blockchains. [17] Figure 1 shown below

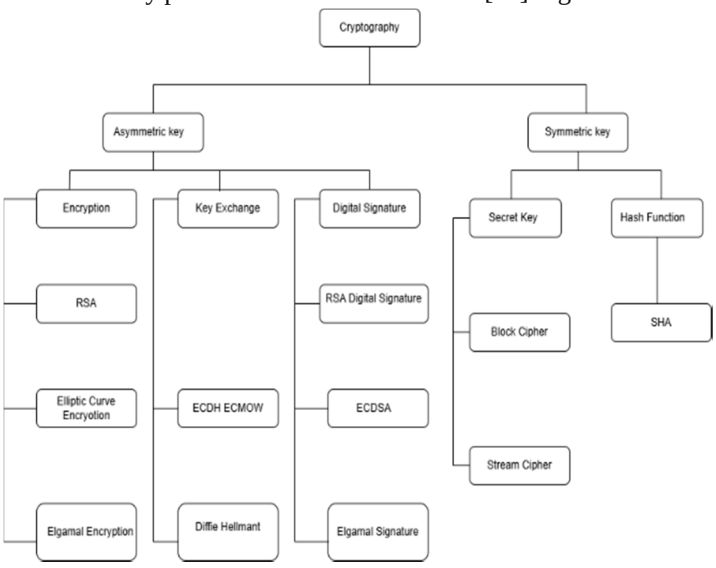


Figure 1: Classification of the Cryptography System

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

III. QUANTUM COMPUTING AND APPLICATION

Quantum computers represent a new way of computing based on quantum mechanical principles of superposition, entanglement, and interference to solve problems that cannot be solved effectively using classical computer systems (e.g., traditional computers). Instead of expressing information as binary digits (0s and 1s), information can be represented in many different states simultaneously through the use of qubits rather than just in two (superposition). [18]

A. Applications of Quantum Computing

Quantum computers have far-reaching implications as a result of being a disruptive technology for a variety of sectors and industries that benefit from advancements in cryptography, optimization, artificial intelligence, and scientific research. Of these, the area of Cryptanalysis attracts the most attention as it threatens the security of many existing public key Cryptosystems by allowing for the rapid solution of numerous mathematical problems previously believed to be infeasible to manipulate. [19]

As a result of this potential risk, considerable research has been directed toward methods of creating Quantum-resistant Cryptosystems. Quantum computing has the potential to be utilized to improve logistics, scheduling, and supply chain management through optimization. Quantum algorithms can theoretically perform searches on extensive solution spaces exponentially faster than any classical algorithm can achieve today. In addition, Quantum Computing can be applied in the Quantum Simulation of Complex Quantum Systems in the fields of Chemistry and Material Science, where it has the potential to enhance our understanding of complex molecular interactions and drug discovery through modeling at a level that would be impossible to replicate on classical computers.[20].

Further, quantum computing has great potential for its application to machine learning and artificial intelligence, by accelerating linear algebraic operations as well as pattern recognition tasks. Other applications include financial modeling, climate simulation, as well as secure communications via quantum key distribution (QKD). Although current quantum computers are classified as "Noisy Intermediate Scale Quantum" devices (NISQ), advancements being made suggest there will be practical applications using large-scale operating QCs in the near future. Quantum Algorithms leverage specific properties of Quantum Mechanics allowing them to run many times quicker than Traditional (Classical) Algorithms. The following are a few quantum algorithms that are particularly important for cryptography and security.

1) Shor's Algorithm

Shor's algorithm is one of the most widely used algorithms in the world. Shor's algorithm enables integer factorization and discrete logarithmic equations to be solved using efficient methods (polynomial-time) rather than using the slower techniques of traditional or classical computers. These issues form the security foundation of widely deployed public-key cryptographic systems such as RSA, Diffie-Hellman, and elliptic curve cryptography. Unlike classical algorithms, which require exponential time for these problems, Schorr's algorithm poses a direct and existential threat to current asymmetric cryptographic infrastructures once large-scale quantum computers become available. [21]

2) Grover's algorithm

Grover's algorithm provides a quadratic speedup for structured search problems, which reduces complexity during brute-force search from O (N) to O ($\sqrt{N}$). In a cryptographic context, this effectively affects symmetric-key encryption and hash functions by halving their security strength. For example, a 128-bit symmetric key provides only 64 bits of security against a quantum adversary using Grover's algorithm. As a result, the key size needs to be increased in order to maintain an adequate security level in the quantum era. [22] For example, in Cryptography where Symmetric Key Encryption utilizes a 128-bit Key there is a compromise of approximately 1/2 the strength of a 128-bit Key as far as security is concerned (64 Bits) for any adversary who has access to a QC using Grover's Algorithm. As a result, in order to maintain a sufficient level of security within the Quantum World it is vital to increase the size of keys being utilized in Cryptography.

3) Quantum Fourier Transform (QFT)

The Quantum Fourier Transform (QFT) is another tool that is found in many quantum algorithms (i.e., Shor's algorithm). It is used to quickly calculate the periodicity of quantum states used to solve algorithms related to the factorization of numbers and discrete logarithms [23].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

4) Quantum Approximate Optimization Algorithm (QAOA)

The QAOA has an exponential speed advantage compared with classical methods for carrying out Fourier Transforms, which showcases the strength of quantum parallelism and interference as compared with classical approaches to the same problems. The quantum approximate optimization algorithm is a hybrid quantum-classical algorithm designed to solve combinatorial optimization problems in near-term quantum devices. In scheduling, network optimization and resource allocation. Although not directly used for cryptanalysis, its development demonstrates the wide-ranging capabilities of quantum algorithms beyond cryptography. [24]

5) Variational quantum algorithm (VQA)

Variational quantum algorithms NISQ combines quantum circuits with classical optimization techniques to solve problems suitable for devices. Variational Quantum Eigen solver (VQE) as one of many examples, is a quantum algorithm that has proven successful for applications in quantum chemistry and materials science and serves to demonstrate that quantum computing can deliver real-world benefits before the advent of fully fault-tolerant quantum computers. [25]

Quantum algorithms that have been developed to achieve advantages over classical algorithms, introduce an entirely new set of constraints on how we evaluate our anticipated security assumptions regarding the security of our contemporary cryptographic infrastructures. As we have witnessed the rise of quantum computing, we are now beginning to realize just how vulnerable our classical cryptographic algorithms have been. The realisation of this vulnerability has given rise to a worldwide movement towards developing Post Quantum Cryptography (PQC), which focuses on providing cryptographic systems that will continue to be secure against both classical and quantum attack vectors. In order to adequately assess the security of crypto-systems in the post-quantum computing landscape, an understanding of quantum computing principles, as well as the principles behind quantum algorithms, is required.

IV. POST QUANTUM CRYPTOGRAPHY

Post-quantum (PQC) refers to the design of new cryptographic algorithms that provide resistance to attacks by both quantum and classical computers. PQC does not require quantum communication channels to operate, as does quantum cryptography, but rather can be implemented on existing (i.e., traditional) devices that are capable of cryptographic functions that resist an attack from a classical computer, while also providing some level of protection against threats posed by an attacking quantum computer. The inspiration for PQC came from widely used public-key cryptographic schemes, such as RSA at, the Diffie-Hellman and elliptic curves arise from weaknesses in quantum algorithms ranging from cryptography to Shor's algorithm. With the advancement of quantum computing technology, p. to ensure long-term data privacy and secure digital communication PQC is indispensable. [26]

A. Applications of Post-Quantum Cryptography

Cryptography, in a post-quantum world, must serve as the basis for protecting existing and future electronic information systems. One important application of PQC is secure communications, where PQC provides a way to ensure that all digital communications (e.g., email) are both kept private and authentic; messages sent over the Internet or another network have the potential to be intercepted and be compromised through quantum computing. For the purpose of using PQC instead of traditional public key encryption (PKE), TLS implementations are a possible mechanism to support VPNs as well as secure email systems to ensure that sensitive passenger data remains protected. The use of PQC is critical when securing the transmission of sensitive data over an untrusted, open, public infrastructure. Another major application of PQC is long-term information security, especially in areas such as healthcare, defense, finance, and government systems, where information must remain confidential for extended periods of time. The threat of "harvest now, decrypt later" attacks to protect encrypted data against future quantum attacks. PQC makes the adoption indispensable. [27]

As post-quantum cryptographic technology continues to evolve, its application across all types of networks, including Cloud Computing/IoT, will gain more attention. Due to huge amounts of connected devices and data being transferred within these systems, they represent a target-rich environment. PQC-based authentication and key-exchange mechanisms increase the resilience of such systems against quantum-enabled attacks. Additionally, Blockchain and Distributed Ledger Technology (DLT) may be utilized in order to ensure that digital signatures and the consensus mechanism used in the decentralization are secure for the long-term. The types of Post-quantum Cryptographic Algorithms are categorized according to the mathematical challenge(s) on which they are built to offer their security.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Post-Quantum Cryptographic Algorithms

Chief algorithm of PQC families are discussed below. Figure 2 shown below

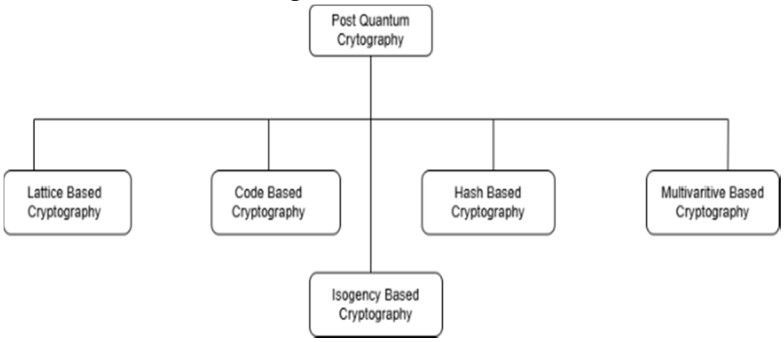


Figure 2: Post quantum cryptography algorithm

1) Lattice-based cryptography

Lattice-based cryptography PQC is one of the most widely studied and promising approaches in C. It is based on the rigor of lattice problems such as Learning with Errors (LWE) and Ring-LWE, which are believed to be resistant to both classical and quantum attacks. Counterfeit-based schemes support encryption, key exchange, and digital signatures with relatively efficient performance. Because of their strong security foundation and versatility, mesh-based algorithms such as Crystals-Kyber and Crystals-Dilithium have been selected for standardization by NIST. [28]

2) Code-based cryptography

Code-based cryptography relies on the difficulty of decoding simple linear error-correcting codes. The McAleese cryptosystem has been in existence for many years and has proven itself as one of the best examples of post-quantum cryptography that still offers a significant level of security from quantum cyber-attacks. Although the Code-based algorithms are the basis of this technology, their large keys create several challenges in terms of storage space and bandwidth constraints due to the volume of communications necessary to support this technology. [29]

3) Hash-based cryptography

Hash-based cryptography focuses primarily on the digital signature scheme and derives its security from the power of the cryptographic hash function. Many of these projects provide good long-term security assurance with few (if any) assumptions and meet the security needs of long-term applications. Examples of such projects include XMSS and SPHINCS +, which are regarded as being "standard" or "de facto standard" by virtue of their resistance to quantum attack. [30]

4) Multivariate polynomial cryptography

Multivariate cryptography is based on the difficulty of solving systems of multivariate quadratic equations over finite fields. Digital signatures are a principal application for these types of schemes. They provide fast, efficient signatures and verification; however, some multivariate schemes have been found to have vulnerabilities in earlier implementations, making careful selection of parameters and design critical for use. [31]

5) Isogeny-based cryptography

Isogeny-based cryptography is based on the proven calculations of isogeny within elliptic curves. Isogeny-based cryptography also provides significantly smaller key sizes than the current PQC schemes, thus being well suited for applications that are sensitive to bandwidth use. Despite its many advantages, the computational intensity of isogeny-based algorithms continues to be studied aggressively due to newly developed techniques for cryptanalysis. [32]

Overall, PQC offers significant resources to implement quantum-proof cryptographic protections. The challenges of performance2, complexity3 of implementation and lack of a defined standard continue to be obstacles for post-quantum security as we prepare for the future of digital communications.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

V. NIIST PQC STANDARDIZATION PROCESS

The rapid growth of Quantum Computing means that there will be a major threat to traditional Public Key Cryptography (RSA, Diffie-Hellman, and Elliptical Curve Cryptography). All these methods of creating public-key infrastructure are based upon the difficulty of solving certain mathematical problems (integer factorization and discrete logarithm). Quantum Computing algorithms (such as Schorr's Algorithm) can provide an efficient solution for these mathematical problems in polynomial time, thus rendering current public-key infrastructures insecure. The National Institute of Standards and Technology (NIST) has created the Post-Quantum Cryptography (PQC) Global Standard to define how the Global Cryptographic Community can determine the appropriate algorithms to secure its global communications against both classical and quantum attacks.

Table 1: Comparison of Post-Quantum Cryptographic Algorithms

Category	PQC Algorithms	Functional Unit	Advantages	Disadvantages
Lattice-based Cryptography	CRYSTALS-Kyber, CRYSTALS-Dilithium, NTRU, SABER, FALCON	Key Encapsulation Mechanism (KEM), Digital Signature	Reliable Security Proofs, Efficient Computing, Suitable Performance on All Platforms, Endorsed by NIST	Large Key and Cipher Text Sizes, Complex Implementations, Possible Side Channel Vulnerabilities
Code-based Cryptography	Classic McEliece	Public-Key Encryption / KEM	Lengthy history of cryptanalysis, large Security Margins, Resistant to Quantum Attacks	Extremely Large Public Keys, High RAM Requirements, Not Suitable for Small Device Usage
Hash-based Cryptography	SPHINCS+	Digital Signature	Minimal Security Assumptions, Well-Defined Hash Functions, Resistant to Quantum Attacks	Large Signature Size, Slow Signing and Verification
Multivariate Cryptography	Rainbow (deprecated), UOV	Digital Signature	Fast Signature Generation and Verification, Low Computing Cost	Most Schemes Have Been Broken, Weak Security Confidence, Large Public Key Sizes
Isogeny-based Cryptography	SIKE (broken), CSIDH	Key Exchange / KEM	Very Small Key Sizes, Strong Theoretical Foundations	High Computational Cost, Slow Speed, Recent Successful Cryptanalytic Attack

The NIST of PQC standardization process evaluates candidate algorithms based on security, performance, feasibility of implementation, and resistance to side-channel attacks Candidates for the PQC Global Standard are organised into groups based on the underlying difficult mathematical problems, and include: Lattice-Based, Code-Based, Hash Based, Multivariate Polynomial, Isogeny Based Among them, fake-based and code-based projects have demonstrated strong security assurance and practical efficiency, making them prominent competitors in the standardization process.

©IJRASET: All Rights are Reserved

Table 2: Round-Wise Post-Quantum Cryptography Algorithms in the NIST Standardization Process

NIST Round	Time Period	Evaluation Focus	Key Algorithms Involved	Outcome
Round 1	2017–2019	Initial entry, Correctness, Basic Security and Feasibility	CRYSTALS-Kyber, SABER, NTRU, FrodoKEM, Classic McEliece, BIKE, HQC, SPHINCS, Dilithium, FALCON, Rainbow, SIKE	Broad based evaluation; those schemes found to be either insecure or inefficient were eliminated.
Round 2	2019–2020	Cryptanalysis Performance, Benchmarks Parameter and algorithm optimization	CRYSTALS-Kyber, SABER, NTRU, FrodoKEM, Classic McEliece, BIKE, HQC, Dilithium, FALCON, SPHINCS+	Reduced the total number of 26 schemes to be used as strong candidates for standardization.
Round 3	2020-2022	Selection of finalists and alternates Maturity assessment of candidates	Finalists: CRYSTALS-Kyber (KEM), CRYSTALS-Dilithium, FALCON, SPHINCS+ (Signatures); Alternates: Classic McEliece, BIKE, HQC; Eliminated: SIKE	Primary algorithms chosen for individual review process were selected.
Round 4	2022–Present	Additional signatures for evaluation, finalizing the standard	CRYSTALS-Dilithium, FALCON, SPHINCS+ (final specs); Additional signature candidates under review	Finalized standards and deployment guidance was developed.

A. Lattice-based cryptography candidate

Lattice-based cryptography forms the backbone of several NIST finalists and standardized algorithms due to its strong worst-case hardness assumption and resistance to known quantum attacks.

1) Crystals-Kyber (Finalist / Standardized KEM)

Crystal-Kiber is a mesh-based key encapsulation mechanism (KEM) selected for standardization by NIST. It is based on the rigor of Module Learning with Errors (MLWE) problem and provides IND-CCA2 security. Kyber supports multiple security layers associated with AES-128, AES-192, and AES-256. Because of its capabilities, Kiber has been adopted in hybrid cryptographic deployments by companies such as Google, Cloudflare, and Amazon Web Services to secure TLS and cloud communications. [33]

2) SABER (Finalist)

SABER is another mesh-based KEM finisher based on the Module Learning with Rounding (MLWR) problem. The Kiber Scheme is a very efficient and straightforward Design for less resource-constrained environments.The Saber Scheme differs from the Kiber Scheme in that it has adopted circular instead of Gaussian noise, resulting in a more straightforward implementation that also enhances side-channel attack resistance. Offering three variants of the service - Lightsaber, Saber, and Firesaber - NIST is compatible with increased security levels.The Kiber Scheme is a very efficient and straightforward Design for less resource-constrained environments. [34]

3) NTRU (Finalist)

NTRU is a mesh-based cryptographic protocol that derives its security from the NTRU mesh problem and is related to the Ring Learning with Errors problem. NTRU is one of the oldest and most established forms of fake-based cryptography and has been extensively investigated through cryptanalysis. In terms of computational speed and minimum key size, it is exceptional for use in real-time applications and with devices that have limited amounts of processing power. [35]

4) Crystals-dilithium (standard digital signature)

Crystals-Dilithium is a mesh-based digital signature project based on MLWE and Module Short Integer Solution (MSIS) problems.Dilithium was nominated as the single post-quantum digital signature standard by NIST due to its balance of strong performance and reasonable robustness. [36]

5) Falcon (the ultimate digital signature)

Falcon is a digital signature scheme based on a mesh-based system of NTRU/mesh (fast Fourier sampling) techniques. The signature size is tiny and provides high security, but great care must be used during implementation to prevent side-channel attacks. Because of its complex nature, Falcon should only be used in highly controlled environments. [37]

B. Code-based cryptography candidate

Classic McAleese (alternate candidate)

The classic McAleese is a code-based cryptographic system, and is based upon the error-correcting codes known as GOPPA codes. It is notable for its long-lasting resistance to cryptanalysis, with no successful quantum attack known to date. Although it suffers from a very large public key size, the classic McAleese offers extremely high security and is considered a powerful fallback option for long-term security. [38]

C. Hash-based cryptography candidate

SPHINCS + (standard digital signature)

SPHINCS+ is a stateless, hash-based digital signature scheme that depends on the security of cryptographic hashes exclusively. Its strong security guarantee along with its few mathematical assumptions enable it to be very resilient against the potential advancements of cryptanalysis in the future. However, the large amount of data generated by SPHINCS+'s signatures and the dependence on slow performance restricts the use of SPHINCS+ in high-security environments. [39]

D. Multivariate-based cryptography candidate

A. Rainbow (Finalist)

Rainbow is a digital signature algorithm derived from a variant of the Unbalanced Oil and Vinegar (UOV) multi-variable cryptographic algorithm. Rainbow has not changed significantly since first introduced in 2005 and exhibits small signatures and very fast signing and verifying speeds. The layered UOV structure of this algorithm makes it resistant to classical algebraic type attacks such as the Kipnis–Shamir attack while still providing computationally efficient performance. The greater complexity of the UOV structure introduces greater vulnerability to potential attacks using more advanced cryptanalytical techniques [40]. Rainbow has been selected as a finalist in the standardisation process carried out by the National Institute of Standards and Technology (NIST) and exists at several different security levels: Level 1, Level 3 and Level 5. The security of this scheme is believed to rely on the extreme difficulty of solving Multivariate Quadratic (MQ) equations in a computationally feasible manner; therefore, it is classified as an NP-hard problem. As a result, the site on which the scheme is based (theoretical) has impacted its security as a matter of fact due to recent event developments. In the aftermath of the Round 3 submission, there were two significant cryptanalytic attacks that were advanced against Rainbow by Beullens. The first was an enhancement of the classical Kipnis-Shamir attack and reduced the effective security of Rainbow levels 1, 3, and 5 by multiple bits. The second attack is more powerful than the first and demonstrates practical key recovery against Rainbow levels 1, 3, and 5. Both attacks outline the structural weaknesses of Rainbow's layered design and illustrate that the selection of parameters cannot be relied upon for long-term security [41]. Due to these weaknesses, it is no longer probable that Rainbow will be regarded by NIST for standardization based on its current parameter sets. Furthermore, the large size of Rainbow's public and private key (up to 1.8 MB) limits its ability to perform efficiently in resource-constrained environments. Although Rainbow performed very well initially, its security weaknesses render it unsuitable for deployment within real world post quantum cryptographic schemes.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

E. Isogency-based cryptography candidate

SIKE (Alternative)

SIKE (Supersingular Isogeny Key Encapsulation) is an isogeny-based post-quantum cryptographic algorithm derived from elliptic curve cryptography. Although traditional elliptic curve schemes are vulnerable to Shor's Algorithm, SIKE mitigates this weakness by utilizing supersingular isogenies, which establish hard-to-invert mappings between elliptic curves rather than relying on point multiplication. This structural similarity to classical protocols such as Diffie–Hellman makes SIKE a promising candidate for easier integration into existing cryptographic infrastructures [42]. SIKE was considered as an alternative candidate in the standardization process led by the National Institute of Standards and Technology (NIST). One of its major advantages is its exceptionally small key size, approximately 750 bytes even at higher security levels, making it highly efficient in terms of communication overhead compared to other post-quantum schemes. Additionally, due to extensive prior research on elliptic curves, parameter selection and resistance to side-channel attacks are relatively well understood [43]. However, SIKE has several critical limitations. The underlying isogeny problems have not been studied as extensively as lattice- or code-based assumptions, resulting in lower confidence in long-term security. Furthermore, SIKE is computationally expensive and significantly slower—often by an order of magnitude—compared to competing PQC algorithms. More importantly, recent cryptanalytic breakthroughs have demonstrated practical attacks capable of completely breaking SIKE's security assumptions, raising serious concerns about its viability.

Due to these vulnerabilities, SIKE was ultimately removed from consideration in the NIST standardization process. While it initially attracted attention due to its compact key sizes and structural compatibility with classical cryptosystems, the discovery of efficient attacks highlights the evolving and uncertain nature of isogeny-based cryptography. Despite this setback, ongoing research continues to explore more secure isogeny-based constructions for future post-quantum applications.

Through its standardization process, NIST creates a transparent, thorough, and community-involved process to evaluate the feasibility of post-quantum algorithms. The selection of several standardised and alternative algorithms by NIST ensures long-term protection against the potential variations in the field of cryptography, as well as any potential unexpected weaknesses that will arise. These algorithms are expected to provide an alternative to traditional Public Key Cryptotherapy for use in secure communications, digital signatures, cloud-based secure storage solutions, the Internet of Things (IoT) and Security for National Security systems.

Table 3 compares the major post-quantum cryptographic algorithms based on their mathematical basis and NIST security level. The classic McAleese provides strong level-5 security but is plagued by large public keys. In the NIST standardization process, mesh-based schemes such as Crystals-Kyber, Crystals-Dilithium, Saber, and NTRU predominate due to efficiency, flexibility, and selectivity. Psyche is included for comparison, despite being removed after Cryptanalytic. For digital signature projects, Crystals-Dilithium provides balanced signature and verification time, which makes it suitable for general-purpose systems. The Falcon achieves a very small signature size but requires careful floating-point implementation. SPHINCS + provides robust security with minimal assumptions at the cost of larger signature sizes and higher computational overhead attacks, illustrating the evolving PQC landscape. SPHINCS + provides strong hash-based security with high performance overhead. Overall, the comparison highlights the trade-off protection for signature validity. All hash-signature projects guarantee a high level of security to their users. In addition, they are built on a limited number of mathematical assumptions which means they will likely continue to provide strong security guarantees from a future perspective. NIST's algorithmic actual review process guarantees that safety, performance, and implementation costs are within reach, providing the most practical balance for deploying lattice-based algorithms.

Table 3: Family and Security Levels of PQC Algorithm[44]

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

VI. PREPROCESSING OF THE RESEARCH DATA

The selection of research articles considered for analysis includes a total of 49 articles published between 2013 and 2025. After the analysing of the chosen articles has been completed, this section will present key results from the reviewed publications. These tables show that all scholarly and high cited articles are focused on the deployment of post quantum cryptography.

Table 3. General surveys and reviews on the Post Quantum Cryptography.

Authors	Technique used	Proposed Work	Gaps/Limitations
Bernstein et al. (2025)	Post-Quantum Cryptography	An extensive examination of quantum resistant cryptographic methods. These are based on lattice, code, and hash techniques and discuss future security risks posed by quantum attacks on future communication systems.	The lack of real-world viability
Alagic et al. (2022)	NIST PQC Standardization	An in-depth examination of the NIST Third Round Candidate Examination Process focusing on the cryptographic security, computational efficiency, and practicality.	Standardization is still not completed
Pirandola et al. (2020)	Quantum Cryptography	Theoretical foundations of quantum cryptography, challenges of developing quantum cryptography protocols (QKD), and issues of quantum key distribution (QKD) implementation for quantum communication systems, are discussed in a detailed review of QKD.	Highly complex and not able to scale
Castryck et al. (2018)	Isogeny-based Cryptography	Newly Introduced Protocol CSIDH for Key Exchange Between Two Commutative Groups That Is Resistant to Quantum Computer Attacks.	Requires high computation capacity
Bos et al. (2018)	Lattice-based Cryptography	Proposes CRYSTALS-Kyber as a New, Secure, and Efficient Means of Key Encapsulation Based on Module Problems in The Lattice.	Key size is very large
Mosca (2018)	Quantum Risk Analysis	Presents An Overview of the Future Cyber Security Threats of Quantum Computers, and Urges the Immediate Need to Adopt Post-Quantum Cryptographic Methods.	There is no plan to implement
Ben-Sasson et al. (2018)	Hash-based Cryptography	Develops Scalable Systems for Maintaining the Integrity of Computational Integrity by Using Post-Quantum Secure Hash-Based Constructions.	High calculation costs
Yin et al. (2020)	Quantum Key Distribution	Through the long-distance experimental demonstration of QKD using quantum keys sent over a 1120 km distance with evidence that a new technique for developing a quantum-secure communications system exists.	Need very specialized facilities
Kim et al. (2023)	Quantum Computing	Provides Early Evidence of Quantum Computing's Advantages Over Classical Computers Before Achieving Full Fault Tolerance.	Very limited scalability
Harrow et al. (2017)	Quantum Supremacy	Studies the Advantages of Quantum Systems Over Classical Systems in Computational Difficulty.	There are experimental boundaries
Xu et al. (2020)	Quantum Key Distribution	Exploring the feasibility of utilizing QKD using actual devices.	Devices are dependent
Fernandez-Carames et al. (2020)	Blockchain + PQC	Proposal to implement PQC safeguards in blockchain applications to enhance their security.	Have scaling problems
Alkim et al. (2016)	Lattice-based Cryptography	Provides The NewHope Key Exchange Protocol, Which Is Based On the Ring-LWE Problem.	Needing more bandwidth
Chen et al. (2016)	PQC Standardization	Gives a Foundational Report on PQC Algorithms and Recommendations for Future Research.	Still in the analysis state

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Alagic et al. (2020)	PQC Standardization	Evaluate NIST's second-round PQC candidates.	Final conclusions are limited
Nejatollahi et al. (2019)	Lattice-based Cryptography	Survey implementations of lattice-based PQC algorithms with an emphasis on performance improvements.	The hardware is complex to use
Sikeridis et al. (2020)	PQC in TLS	Evaluate performance penalties associated with integrating PQC into the TLS and SSH standards.	They're looking for ways to reduce latency
Kumar et al. (2022)	Post-Quantum Cryptography	An analysis of PQC algorithms to determine their performance and standardisation attributes.	No experimental validation
Buchmann et al. (2016)	PQC Survey	A comprehensive overview of PQC methodologies that exist today.	Outdated due to advancements
Crockett et al. (2019)	Hybrid Cryptography	Propose hybrid classical and PQC-based systems for safe migration to PQC.	The system's complexity has increased
Gao et al. (2018)	PQC Blockchain	Develop a new secure cryptocurrency utilizing secure PQC methods.	Inefficiencies are present
Althobaiti et al. (2020)	IoT Security	Address unique challenges of PQC when applied in IoT contexts.	The resources are limited
Basu et al. (2019)	PQC Hardware	Evaluate hardware implementations of PQC algorithms.	Very expensive
Alagic et al. (2025)	PQC Standardization	Provide third round NIST PQC Selection Process Progress Update.	Still have a process to complete
Moody et al. (2020)	PQC Standardization	Conduct a review of NIST's second-round PQC Development Project.	Are only partial results
Bisheh-Niasar et al. (2021)	Lattice-based Cryptography	Recommending high-speed multiplication of polynomials in order to support PQC systems.	The hardware is complex to use
Beullens et al. (2021)	Multivariate Cryptography	Introduce a new digital signature scheme called MAYO, based on the oil and vinegar model.	Key size is very large
Hülsing et al. (2021)	Hash-based Cryptography	Propose a PQ-secure version of WireGuard.	Performance problems
Bürstinghaus-Steinbach et al. (2020)	PQC TLS	Implement a PQC-enabled version of the TLS protocol for embedded computing platforms.	Memory is used
Schwabe et al. (2020)	PQC TLS	Remove the use of signatures as part of the handshake in order to establish a principal's identity using the PQ-enabled TLS.	Incompatible
Li et al. (2018)	Lattice-based Cryptography	Develop lattice-based signature algorithms for use with blockchain technology.	Key size is very large
Bos et al. (2015)	Lattice-based Cryptography	Provide a new key exchange method using RLWE for use with TLS protocols.	Performance problems
Koziel et al. (2016)	Isogeny-based Cryptography	Use FPGA for implementation of PQC algorithms.	Are slow to execute
Malina et al. (2021)	PQC Privacy	Focus on PPVT and PQ security in smarter technology.	Complex
Banerjee et al. (2019)	Hardware Cryptography	Design a PQ cryptographic processor that can be configured.	The lack of power consumed
Mavroeidis et al. (2018)	PQC Impact Analysis	Conduct research on the impact of quantum computing on general-purpose cryptography.	No solution offered
Guo et al. (2020)	PQC Security	Demonstrate timing attack on BTZ signature algorithms.	Security holes
Chase et al. (2017)	PQC Signatures	Develop zero-knowledge proof signatures utilizing PQC.	Computation problems
Katz et al. (2018)	PQC Protocols	Improve non-interactive, zero-knowledge proof algorithms in order to support PQC.	Inefficiencies present
Fritzmann et al. (2020)	PQC Hardware	Propose RISC-V based accelerators for use with	Design too complex

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

		PQC.	
Pessl et al. (2017)	PQC Attack	Demonstrate attacks on BLISS-based digital signature algorithms (i.e., timing and fault attacks).	Security holes
Fritzmann et al. (2022)	PQC Hardware	Develop hardware-based masks for security for PQC.	Expensive to build
De Feo et al. (2020)	Isogeny-based Cryptography	Introduce SQISign, a digital signature scheme for use with PQC.	Very slow to perform
Unruh et al. (2017)	PQC Security	Evaluate Security of the Fiat-Shamir Transformation.	Complex
Liu et al. (2018)	IoT Security	Evaluate Security of Edge Devices with Post-Quantum Cryptography.	Limitations of resource
Liu & Zhandry et al. (2019)	PQC Protocols	Review of Fiat-Shamir Transformations.	More theoretical than practical
Bernstein et al. (2013)	Quantum Algorithms	Investigate Quantum Subset-Sum Algorithms.	Applications are very limited
Mohammed et al. (2018)	Post-quantum Cryptography	Construct a Quantum-Resistant Encryption Model.	Baselines are very low
Irshad et al. (2023)	PQC + Blockchain	Recommend a Hybrid Cloud System Using Block Chain and Post-Quantum Cryptography.	Have a lot of overhead

First the records have been collected, there is a process of processing to obtain the 2013 through to 2025 data. Researchers noted low levels of output in early years (2013-2016), meaning research was still in its infancy during this period. Starting in 2017, however, researchers began publishing many more papers in these fields, indicating an increase in awareness and concern for issues associated with quantum computers threatening classical cryptography systems. The largest number of papers was published between 2018 and 2022 which corresponds exactly with the height of activity during the National Institute of Standards and Technology's (NIST) ongoing PQC standardization process whereby researchers globally accelerated their PQC research efforts. Two years (2014, 2024) show no output, but are included in this plot for the sake of chronological integrity and unbiasedness. Finally, from 2023 to 2025, researchers continue to produce papers on PQC topics. Therefore, this remains a significant area of focus and research for the foreseeable future towards the development and implementation of quantum-resistant cryptographic solutions.

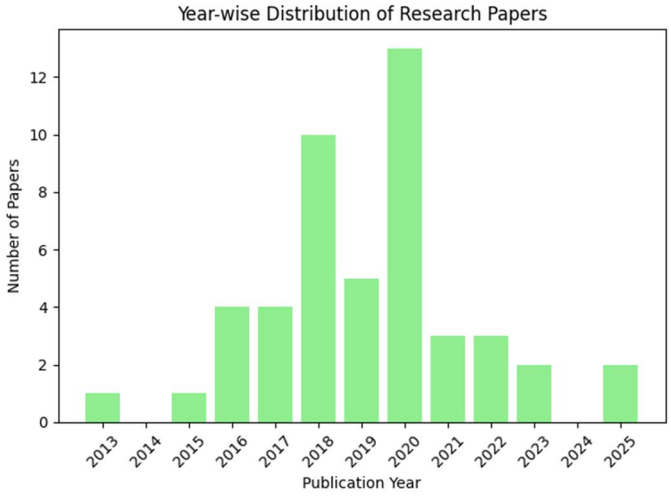


Figure: 3 Year-Wise Distribution of the Research Papers

There was publication source distribution is seen in the selected research works with a high percentage of the total amount of published work coming from journal article (35%) and conference paper (33%), indicating a large amount of participation in both research output and participation at the conference. The remaining sources of publication, preprint (12%), book chapter (10%), and technical report (10%), have a moderate and to small amounts of published research, with technical report being published for the purposes of standardization and institutional use.

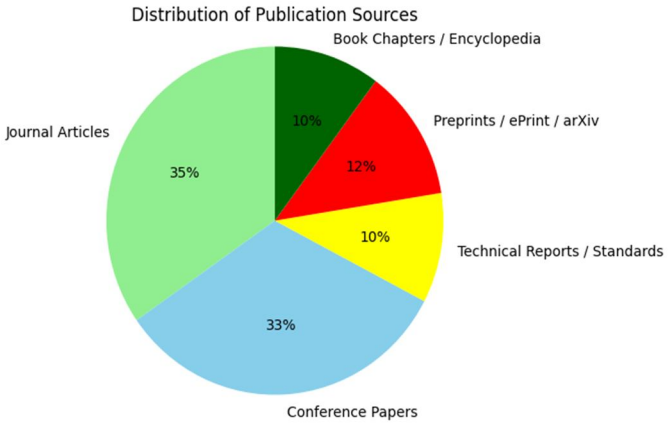


Figure: 4 Distribution of Publication Sources

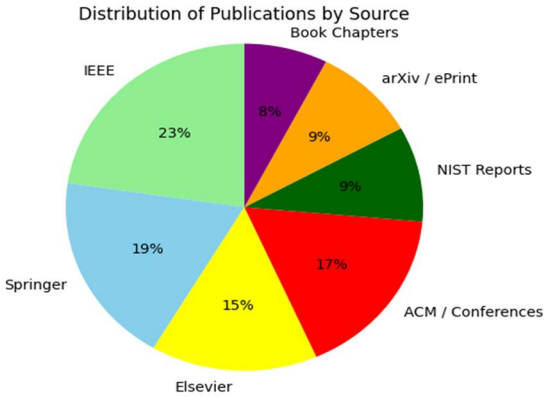


Figure: 5 Distribution of Publication Source

A. Research Questions

RQ1: What are the leading methodologies used to create Post-Quantum Cryptography?

This research question investigates the primary PQC methodologies that include lattice- and code- and hash- and multivariable- and isogeny-based cryptographic methods while looking at the mathematical underpinnings and security assumptions for each.

RQ2: How do Post-Quantum Cryptography and Classic Cryptography and Quantum Cryptography Differ?

This research question examines how Classical Cryptography, Quantum Cryptography, and Post-Quantum Cryptography differ with respect to the security model used or set up for each and what the computational assumptions used there are for each, and how easily an adversary can use quantum computer technology against the three.

RQ3: What Data Sets, Hardware Platforms and Software Tools Are Commonly Used in the Research and Application of PQC?

This research question investigates the use of hardware tools, software tools such as quantum simulators and cryptography libraries in the evaluation of PQC algorithms, as well as a lack of any data set being used here.

RQ4: How Are Digital Signature Schemes Implemented in PQC ?

This research question looks at how digital signature schemes can be designed and implemented using PQC and what existing tools/algorithms are available to use for secure authentication.

RQ5: What Are the Performance Trade-Offs between Different PQC Algorithms?

This research question compares different approaches to PQC with respect to computational efficiency of the algorithms, key size of the algorithms, level of security afforded by the algorithms, and the complexity of the algorithms in terms of implementation.

RQ6. What is the NIST progressed in the area of standardizing post-quantum cryptography?

An assessment of where NIST is at in standardizing post-quantum cryptography (PQC) along with a small selection of PQC algorithms that may be ready for implementation into existing production systems is discussed in this question.

RQ7. What are some of the barriers that organizations face in adopting PQC and what do you feel organizations need to do additionally to help transition to PQC?

This question will involve finding the currently open issues (e.g. scalability, maximum length of time possible to implement on existing technology and how this technology will be integrated) that have to be resolved before organizations transition away from their current systems to quantum-safe solutions.

VII. LIMITATIONS

1) Variability in Evaluations and Performance Metrics: There is a great deal of variability in the evaluation methods, benchmark environments, and performance metrics reported in the literature surveyed. Many of the studies focused on performance parameters such as key size and computational efficiency, for example, neglecting other important parameters like memory overhead, energy use, latency, and cost for real-world deployment. As a result, direct comparisons of PQC schemes are not possible, and this could result in an incomplete performance assessment.
2) Limited Validation of PQC Algorithms in Practice: Although many of the PQC algorithms provide evidence of being highly efficient with strong security claims, most evaluations have been done in a simulated or controlled environment. Real-world deployment scenarios such as constrained IOT devices, cloud systems, and embedded systems are rarely tested for PQC. Consequently, many claims of performance may not accurately reflect their actual performance in practice.
3) Inconsistencies in Methodology and Problems With Reproducibility: There is frequently insufficient information provided in several studies to allow for adequate replication of the resulting outcomes of each experiment; the inclusion of implementation parameters, optimization techniques, and experimental conditions, for example. The lack of reported hardware specifications and software libraries, for example, creates those same challenges in being able to replicate the results of an experiment. A lack of reported information (and sufficient transparency) leads to difficulties in assessing the reliability and validity of comparative analyses of the published PQC research.
4) Minimal Real-World Implementation Considerations: Although theorists believe that all PQC algorithms will be secure against attacks from quantum computers, thus far few efforts have gone into incorporating these forms of algorithms into existing communication technologies. Neither backward compatibility with existing classical systems nor changes to protocol standards (e.g., changes to TLS, SSH, etc.) have been addressed so as to ensure that migrating to truly quantum-resistant systems will be a straightforward process.
5) No Large-Scale Implementation or Standardization: As of this moment in time, there are only a very small number of PQC algorithms that have actually been created and utilized; this is despite the continuing assistance from NIST. Because there has not been enough large-scale deployment or testing of performance in real-world applications, there is simply no clear evidence available that supports or confirms that any of the available PQC algorithms are, in fact, sufficient and/or capable of providing future capabilities for interoperability.
6) Cryptographic Assumptions of Security Being Reviewed and Evolving Cryptanalysis: The security of PQC algorithms is based on certain mathematics that is currently assumed quantum-resistant; however, this is under continual review and there may be new forms of cryptanalysis found that will compromise the security of existing PQC algorithms. For example, isogeny-based cryptography is a PQC algorithm that has been proven to be susceptible to attack, demonstrating the fact that the security of PQC algorithms is continually evolving.

VIII. FUTURE PROSPECT AND CHALLENGES

The rapid advances in quantum computing post-quantum cryptographic. Strengthened global efforts towards the development and deployment of the system. Although significant progress has been made through the NIST standardization process, a number of research challenges and open problems remain. To maintain PQC's viability, the continual improvement of technology is essential in order to ensure its long-term safety and efficacy and real world application.

A major opportunity presented by Post-Quantum Cryptography is the ability to take advantage of existing Infrastructure for Security. Hybrid cryptographic schemes such as PQC. Combining classical algorithms with primitives has already led to the development of Transport Layer Security (TLS) being deployed in protocols such as virtual private networks (VPNs) and cloud security frameworks. These hybrid methods enable a gradual transition while maintaining backward compatibility. Another important aspect is the Internet of Things (IoT) for resource-constrained environments including devices, smart sensors, and embedded systems. optimization of the PQC algorithm. A major opportunity presented by Post-Quantum Cryptography is the ability to take advantage of existing Infrastructure for Security. Field-programmable gate array (FPGA).

Application-specific integrated circuit (ASIC) and the advancement of hardware acceleration using specialized cryptographic co-processors. It is expected to significantly improve the performance of PQC.

Post-quantum digital signatures also present strong opportunities for securing software updates, blockchain systems, and long-term data authentication. Algorithms such as Crystals-Dilithium and SPHINCS + are suitable for applications requiring strong security guarantees for extended periods of time, such as storing government records and archives.

From a theoretical point of view, further research on new difficult mathematical problems beyond lattices and codes can increase cryptographic diversity. Widely accepted this diversity is crucial for mitigating systemic risks when vulnerabilities are discovered in PQC projects.

Despite its promise, post-quantum cryptography faces a number of significant challenges. One of the primary concerns is that many post-quantum cryptography . Increased computational and memory overhead associated with the PQC algorithm. Large public keys, ciphertext, and signatures - especially in code-based and hash-based projects - pose challenges for bandwidth-limited and low-power environments.

Security is another important aspect. Although the post-quantum cryptography . Contrary to the mathematical structures of PQC Algorithms, Real-World implementations are still vulnerable to side-channel attacks, fault injection attacks, and timing attacks. Research in the area of Continuos. Time Implementations and Resistance to physical attack constitutes a growing field of research, particularly concerning Lattice-Based Schemes designed around complex mathematical functions.

Additionally, the development of standards and interoperability poses a myriad of other challenges. The creation of standard algorithms selected for standardization by NIST requires cooperation and collaboration between International Standardizing Bodies, Software Libraries, and Hardware Manufacturers. Transitioning to a Post-Quantum Cryptography-enabled infrastructure involves a lengthy and costly process, which can only be done through extensive planning and risk evaluations. Companies must guard against the risk of premature deployment of algorithms. PQC intake needs to balance out emergencies that may later appear to be debilitating.

Future research efforts in post-quantum cryptography in the focus should be on improving the efficiency and scalability of PQC algorithms, developing robust countermeasures against implementation attacks, and designing flexible cryptographic structures that support algorithm agility. Lastly, due to the current uncertainty regarding the availability, timeframe, and capabilities of Large Scale Quantum Computers, decision-making surrounding the adoption of PQC is hindered. It is vital for Public Cryptanalysis and Benchmarking to continue, thereby ensuring continued public confidence in the standard algorithms.

To summarize, the adoption of post-quantum cryptography is an essential means of protecting digital systems from the impacts of quantum technology. The future development efforts being made by academia, industry and standardization agencies towards advancing the post-quantum cryptographic solutions will greatly determine whether this form of digital security will be realised successfully or not.

IX. CONCLUSION

Quantum computing will likely raise many viable threats to the Public Key Cryptographic systems being utilized today (digital communications, data storage, and authentication), and more importantly to utilize those technologies in an unauthorized fashion with quantum computing assisting in their capability. The Public Key Cryptosystems currently threatened by quantum attacks are RSA, Diffie–Hellman, and ECC. Shor's and Grover's algorithms pose a risk to these systems. Therefore, The need for a new post-quantum cryptographic solution is essential for long-term security in the Post-Quantum Era.

In this paper a detailed examination of the interrelationships among cryptography, quantum computing and post-quantum cryptographic techniques is presented with a focus on their respective areas of application, their mathematical foundations and their impact on security. The work discussed the major families of post-quantum cryptographic methods such as lattice, code, hash, multivariate and isogeny-based methods. It also provided an in-depth analysis of NIST's post-quantum cryptography standards process. The analysis included the reasons, strengths, and performance of the leading candidate algorithms for post-quantum cryptography such as Crystals-Kyber, Crystals-Dilithium, Falcon and SPHINCS+.

A direct comparison of the performance of the solutions illustrates that the networks are able to provide an ideal trade off between security and efficiency. This characteristic makes lattice-based systems attractive candidates for the potential mass-use in numerous applications, particularly in areas like secure communications protocols, cloud computing, and embedded devices. The biggest hindrances to the widespread adoption of mesh-based technologies are still incomplete solutions for ensuring implementation security, an ever-growing computational burden and a limited level of compatibility between multiple implementations of the same solution.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

To summarise, post-quantum cryptography has been a game changer in designing cryptographic systems and gives us an additional layer of defence against the very real threat of quantum technology-based attacks. As we turn our attention towards continuing to do well-researched post-quantum cryptographic research and evaluation of the efficacy of post-quantum cryptography, we will develop strong post-quantum cryptographic systems that secure computers and digital data against the changing technology landscape for years to come. Furthermore, by establishing and applying post-quantum cryptographic solutions today, we will continue to provide our digital infrastructure with defence against possible attacks over the next several decades.

REFERENCES

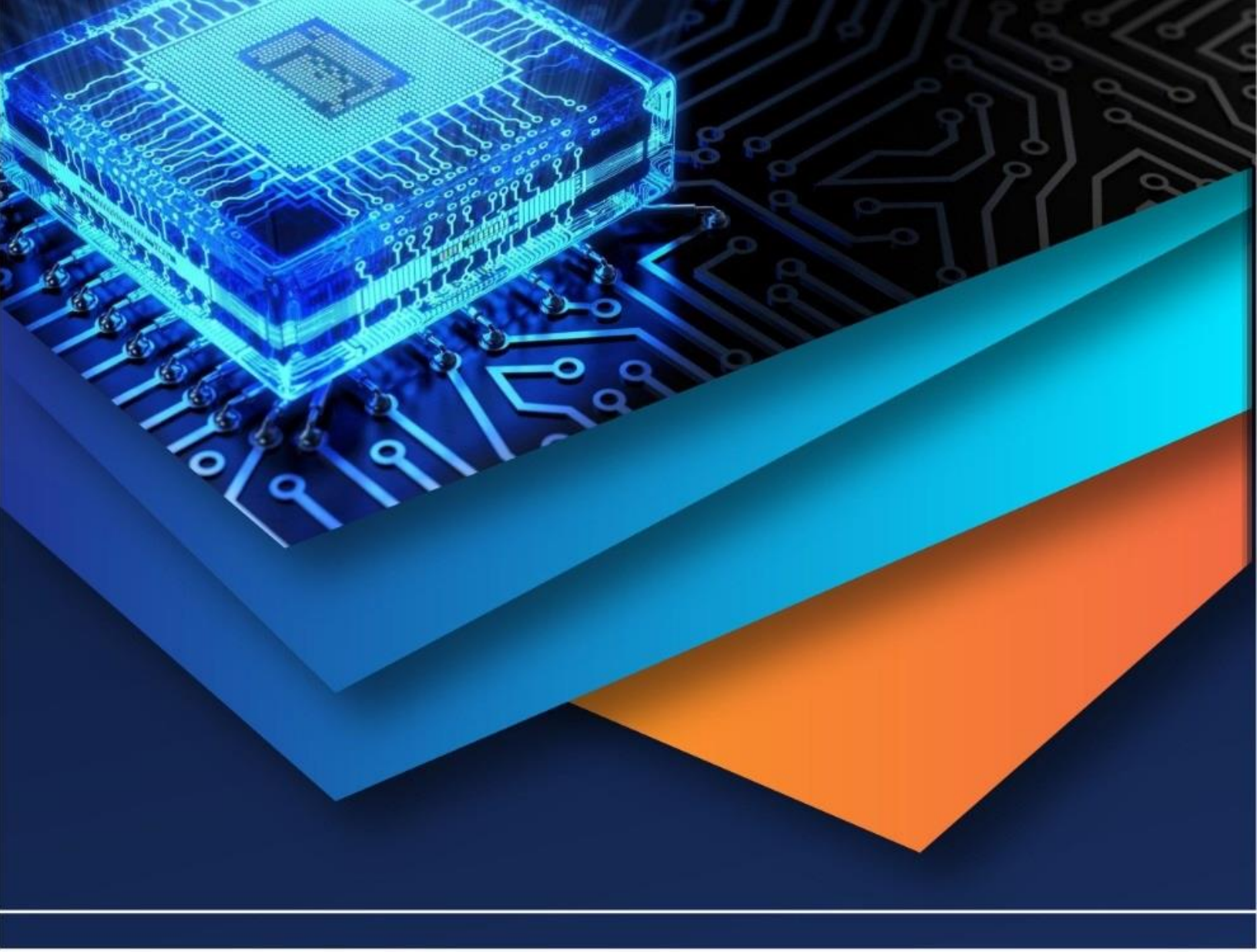
[1] Bernstein, D. J., Buchmann, J., & Dahmen, E., Post-Quantum Cryptography, Springer-Verlag, Berlin, Heidelberg, 2009, ISBN: 978-3-540-88701-0
[2] NIST, FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), Federal Information Processing Standards Publication, 2024.
[3] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997
[4] L. K. Grover, "A fast quantum mechanical algorithm for database search," Physical Review Letters, vol. 79, no. 2, pp. 325–328, 1997.
[5] Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y. K., Miller, C., Moody, D., Peralta, R., & Smith-Tone, D., Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency Report (NISTIR) 8309, 2020.
[6] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, S. Das, "Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey," arXiv, 2025.
[7] Omar Alnaseri, Yassine Himeur, Shadi Atalla, Wathiq Mansoor, "Complexity of Post-Quantum Cryptography in Embedded Systems and Its Optimization Strategies," arXiv, 2025
[8] Elif D. Demir, Buse Bilgin, Mehmet C. Onbasli, "Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms," arXiv, 2025.
[9] Zixian Gong., "A survey on lattice-based digital signature," Cybersecurity, vol. 7, no. 7, 2024
[10] Duc-Thuan dum."A Survey of Post-Quantum Cryptography: Start of a New Race," Cryptography, vol. 7, no. 3, 2023,
[11] Saurabh Sharma. "New Innovations in Cryptography and Its Applications". pp 527–538.
[12] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, 2012.
[13] Laurie Hughes, "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda," volume49.
[14] Abdel Rahman "Internet of Things (IOT): Research Challenges and Future Applications" Vol. 10, No. 6, 2019.
[15] Sourabh Chandra"A study and analysis on symmetric cryptography".
[16] Pubali Maiti "Comparative Study of Asymmetric Key Cryptographic Algorithms in Image Encryption"
[17] Darshana Upadhyay "Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications"
[18] HILAL AHMAD BHAT "Quantum Computing: Fundamentals, Implementations and Applications"
[19] Amirul Asyraf Zhahir "Quantum Computing and Its Application"
[20] R. P. Feynman, "Simulating physics with computers," International Journal of Theoretical Physics, vol. 21, 1982.
[21] Rafael Pereira da Silva "Quantum Factorization: Shor's Algorithm"
[22] Shivani Mehta "Implementation of Grover's Algorithm based on Quantum Reservoir Computing"
[23] Loïc Dewitte. "Application of the quantum Fourier transform in a harmonic balance solver for Burgers' equation"
[24] Kostas Blekos. "A review on Quantum Approximate Optimization Algorithm and its variants".
[25] Supreeth Mysore Venkatesh "Qubit-Efficient Variational Quantum Algorithms for Image Segmentation"
[26] Manish Kumar."Post-quantum cryptography Algorithm's standardization and performance analysis".
[27] Francis Kagai. "Harvest-Now, Decrypt-Later: A Temporal Cybersecurity Risk in the Quantum Transition".
[28] Pawan Kumar Pradhan."Lattice Based Cryptography : Its Applications, Areas of Interest & Future Scope"
[29] N. Sendrier,"Code-Based Cryptography: State of the Art and Perspectives".
[30] Takagi, T., Wakayama."Improving Hash-Based Signature Schemes: From Theory to Practice"
[31] Dheerendra Mishra. "The rise and resilience of multivariate cryptography: Advances, pitfalls, and promising pathways"
[32] Dheerendra Mishra."Isogeny-based cryptography: A comprehensive review on advancements, analysis of attacks, and future directions".
[33] J. Bos. "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," IEEE European Symposium on Security and Privacy, 2018.
[34] D'Anvers, Jan-Pieter. "Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM." International Conference on Cryptology in Africa. Cham: Springer International Publishing, 2018.
[35] Hoffstein, J., Pipher, J., & 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. DOI https://doi.org/10.1007/BFb0054868
[36] Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals–dilithium: Digital signatures from module lattices.
[37] Fouque, Pierre-Alain, et al. "Falcon: Fast-Fourier lattice-based compact signatures over NTRU." Submission to the NIST's post-quantum cryptography standardization process 36.5 (2018): 1-75.
[38] Bernstein, D. J., Lange, T., & Peters, C. (2008, October). Attacking and defending the McEliece cryptosystem. In International Workshop on Post-Quantum Cryptography (pp. 31-46). Berlin, Heidelberg: Springer Berlin Heidelberg.
[39] P. Schwabe, "SPHINCS+," December 2020
[40] Ding, J., & 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.
[41] Beullens, Ward. "Breaking rainbow takes a weekend on a laptop." Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2022.
[42] Jao, David, and Luca De Feo. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies." International workshop on post-quantum cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.
[43] Castryck, Wouter, and Thomas Decru. "An efficient key recovery attack on SIDH." Annual international conference on the theory and applications of cryptographic techniques. Cham: Springer Nature Switzerland, 2023.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[44] Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., & Daniel, S. J. (2022). Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. arXiv preprint arXiv:2202.02826.
[45] Bernstein, D. J. (2025). Post-quantum cryptography. In Encyclopedia of Cryptography, Security and Privacy (pp. 1846-1847). Cham: Springer Nature Switzerland.
[46] Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., ... & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process.
[47] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. Advances in optics and photonics, 12(4), 1012-1236.
[48] Castryck, W., Lange, T., Martindale, C., Panny, L., & Renes, J. (2018, October). CSIDH: an efficient post-quantum commutative group action. In International conference on the theory and application of cryptology and information security (pp. 395-427). Cham: Springer International Publishing.
[49] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European symposium on security and privacy (EuroS&P) (pp. 353-367). IEEE.
[50] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. IEEE Security & Privacy, 16(5), 38-41.
[51] Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive.
[52] Yin, J., Li, Y. H., Liao, S. K., Yang, M., Cao, Y., Zhang, L., ... & Pan, J. W. (2020). Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature, 582(7813), 501-505.
[53] Kim, Y., Eddins, A., Anand, S., Wei, K. X., Van Den Berg, E., Rosenblatt, S., ... & Kandala, A. (2023). Evidence for the utility of quantum computing before fault tolerance. Nature, 618(7965), 500-505.
[54] Harrow, A. W., & Montanaro, A. (2017). Quantum computational supremacy. Nature, 549(7671), 203-209.
[55] Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. Reviews of modern physics, 92(2), 025002.
[56] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access, 8, 21091-21116.
[57] Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key {Exchange—A} new hope. In 25th USENIX security symposium (USENIX Security 16) (pp. 327-343).
[58] Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). Report on post-quantum cryptography (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
[59] Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., ... & Smith-Tone, D. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process. US Department of Commerce, NIST, 2, 69.
[60] Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. ACM Computing Surveys (CSUR), 51(6), 1-41.
[61] Sikeridis, D., Kampanakis, P., & Devetsikiotis, M. (2020, November). Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH. In Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies (pp. 149-156).
[62] Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. Array, 15, 100242.
[63] Buchmann, J. A., Butin, D., Göpfert, F., & Petzoldt, A. (2016). Post-quantum cryptography: state of the art. The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday, 88-108.
[64] Crockett, E., Paquin, C., & Stebila, D. (2019). Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. Cryptology ePrint Archive.
[65] Gao, Y. L., Chen, X. B., Chen, Y. L., Sun, Y., Niu, X. X., & Yang, Y. X. (2018). A secure cryptocurrency scheme based on post-quantum blockchain. Ieee Access, 6, 27205-27213.
[66] Althobaiti, O. S., & Dohler, M. (2020). Cybersecurity challenges associated with the internet of things in a post-quantum world. Ieee Access, 8, 157356-157381.
[67] Basu, K., Soni, D., Nabeel, M., & Karri, R. (2019). Nist post-quantum cryptography-a hardware evaluation study. Cryptology ePrint Archive.
[68] Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., ... & Waller, N. (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.
[69] Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., ... & Alperin-Sheriff, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process.
[70] Bisheh-Niasar, M., Azarderakhsh, R., & Mozaffari-Kermani, M. (2021, June). High-speed NTT-based polynomial multiplication accelerator for post-quantum cryptography. In 2021 IEEE 28th symposium on computer arithmetic (ARITH) (pp. 94-101). IEEE.
[71] Beullens, W. (2021, September). MAYO: practical post-quantum signatures from oil-and-vinegar maps. In International Conference on Selected Areas in Cryptography (pp. 355-376). Cham: Springer International Publishing.
[72] Hülsing, A., Ning, K. C., Schwabe, P., Weber, F. J., & Zimmermann, P. R. (2021, May). Post-quantum wireguard. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 304-321). IEEE.
[73] Bürstinghaus-Steinbach, K., Krauß, C., Niederhagen, R., & Schneider, M. (2020, October). Post-quantum tls on embedded systems: Integrating and evaluating kyber and sphincs+ with mbed tls. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (pp. 841-852).
[74] Schwabe, P., Stebila, D., & Wiggers, T. (2020, October). Post-quantum TLS without handshake signatures. In Proceedings of the 2020 ACM SIGSAC conference on computer and communications security (pp. 1461-1480).
[75] Li, C. Y., Chen, X. B., Chen, Y. L., Hou, Y. Y., & Li, J. (2018). A new lattice-based signature scheme in post-quantum blockchain network. Ieee Access, 7, 2026-2033.
[76] Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015, May). Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In 2015 IEEE symposium on security and privacy (pp. 553-570). IEEE.

[77] Koziel, B., Azarderakhsh, R., Kermani, M. M., & Jao, D. (2016). Post-quantum cryptography on FPGA based on isogenies on elliptic curves. IEEE Transactions on Circuits and Systems I: Regular Papers, 64(1), 86-99.
[78] Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevičius, R., ... & Tang, Q. (2021). Post-quantum era privacy protection for intelligent infrastructures. IEEE Access, 9, 36038-36077.
[79] Banerjee, U., Ukyab, T. S., & Chandrakasan, A. P. (2019). Sapphire: A configurable crypto-processor for post-quantum lattice-based protocols. arXiv preprint arXiv:1910.07557.
[80] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.
[81] Guo, Q., Johansson, T., & Nilsson, A. (2020, August). A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM. In Annual International Cryptology Conference (pp. 359-386). Cham: Springer International Publishing.
[82] Chase, M., Derler, D., Goldfeder, S., Orlandi, C., Ramacher, S., Rechberger, C., ... & Zaverucha, G. (2017, October). Post-quantum zero-knowledge and signatures from symmetric-key primitives. In Proceedings of the 2017 acm sigsac conference on computer and communications security (pp. 1825-1842).
[83] Katz, J., Kolesnikov, V., & Wang, X. (2018, October). Improved non-interactive zero knowledge with applications to post-quantum signatures. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 525-537).
[84] Fritzmann, T., Sigl, G., & Sepúlveda, J. (2020). RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 239-280.
[85] Pessl, P., Bruinderink, L. G., & Yarom, Y. (2017, October). To BLISS-B or not to be: Attacking strongSwan's Implementation of Post-Quantum Signatures. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1843-1855).
[86] Fritzmann, T., Van Beirendonck, M., Roy, D. B., Karl, P., Schamberger, T., Verbauwhede, I., & Sigl, G. (2022). Masked accelerators and instruction set extensions for post-quantum cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 414-460.
[87] De Feo, L., Kohel, D., Leroux, A., Petit, C., & Wesolowski, B. (2020, December). SQISign: compact post-quantum signatures from quaternions and isogenies. In International conference on the theory and application of cryptology and information security (pp. 64-93). Cham: Springer International Publishing.
[88] Unruh, D. (2017, November). Post-quantum security of Fiat-Shamir. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 65-95). Cham: Springer International Publishing.
[89] Liu, Z., Choo, K. K. R., & Grossschadl, J. (2018). Securing edge devices in the post-quantum internet of things using lattice-based cryptography. IEEE Communications Magazine, 56(2), 158-162.
[90] Liu, Q., & Zhandry, M. (2019, August). Revisiting post-quantum fiat-shamir. In Annual International Cryptology Conference (pp. 326-355). Cham: Springer International Publishing.
[91] Bernstein, D. J., Jeffery, S., Lange, T., & Meurer, A. (2013, June). Quantum algorithms for the subset-sum problem. In International Workshop on Post-Quantum Cryptography (pp. 16-33). Berlin, Heidelberg: Springer Berlin Heidelberg.
[92] Mohammed, A. (2018). Quantum-Resistant Cryptography: Developing Encryption Against Quantum Attacks. Journal of Innovative Technologies, 1(1), 1-14.
[93] Irshad, R. R., Hussain, S., Hussain, I., Nasir, J. A., Zeb, A., Alalayah, K. M., ... & Alwayle, I. M. (2023). IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing. IEEE Access, 11, 105479-105498.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)