Indo Asian Journal of Management and Entrepreneurship (IAJOME)
	ISSN: 2319-2992, Impact Factor 5.007	
	Peer-Reviewed	Open Access	International Journal	
	Volume: 17	Issue: 07	July 2026	www.iajome.com	

REVIEW ON ARTIFICIAL INTELLIGENCE ON POST-QUANTUM CRYPTOGRAPHY FOR SECURE COMMUNICATION

[1] Mrs.A.Vidhumitha, [2] Hariharan S

[1] Assistant Professor, Department of Computer Applications
Sri Krishna Arts and Science College

[2] Student, Department of Computer Applications
Sri Krishna Arts and Science College

Abstract— Post-Quantum Cryptography, or PQC, is all about creating new ways to encrypt things so they can't be cracked by either regular computers or the super-powerful quantum computers that are coming. Right now, things like RSA, Diffie-Hellman, and ECC are pretty standard for public-key encryption. But the worry is that as quantum computers get better, they'll be able to solve the math problems these systems rely on, basically breaking them. Algorithms like Shor's algorithm are a big concern because they could compromise the security and trustworthiness of our digital conversations. That's why we really need to figure out encryption methods that can handle quantum computers but still work well with today's networks. PQC is basically the next step in encryption, using math problems that we think quantum computers won't be able to solve easily. We're talking about things like lattice-based, code-based, hash-based, multivariate, and isogeny-based cryptography. Unlike quantum key distribution, which needs special quantum gear, PQC can be used with the computers and devices we already have. This makes it much more practical and cheaper to roll out everywhere. It means companies can start swapping out their old encryption systems bit by bit without having to rebuild their whole communication setup.

Keywords: Post-Quantum Cryptography (PQC), Quantum Computing, Secure Communication, Quantum-Resistant Cryptography, Encryption, Digital Signatures, Cybersecurity, Key Encapsulation Mechanism (KEM).

I. Introduction

Digital technology has changed how we all communicate and handle information. In our connected world, keeping information secure is really important, especially when it comes to things like money transfers, personal details, health records, and government communications that travel over networks. For a long time, we've relied on public-key encryption methods like RSA, Diffie-Hellman, and ECC. These work well because they're based on math problems that are too hard for today's computers to crack, which keeps our data private and authentic.

But now, quantum computers are on the horizon. These machines use quantum mechanics to do calculations much faster than regular computers. Things like Shor's algorithm could easily break the math behind RSA and ECC, leaving our current encryption methods vulnerable. As quantum computing gets better, the risk of our encryption being broken becomes more real, creating a big security problem globally.

To tackle this, we're developing Post-Quantum Cryptography (PQC). These are new encryption methods designed to be safe from both regular and quantum computers. Unlike Quantum Key Distribution (QKD), which needs special quantum communication gear, PQC can work with the hardware and software we already have. This makes it a practical and affordable way to upgrade our security without a complete overhaul of our digital systems. PQC relies on different kinds of math problems that are thought to be hard for even powerful quantum computers to solve, like those based on lattices, codes, hashes, multivariate equations, and isogenies.

Recent progress in setting standards for PQC is also a big deal. International groups have been testing many different quantum-resistant algorithms to find ones that are secure and work well enough for everyday use. Algorithms like CRYSTALS-Kyber for setting up secure connections and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures are leading the way for future communication security. They aim to be very secure while still being reasonably fast and compatible with current internet technology.

Post-Quantum Cryptography will be useful in many areas, including banking, healthcare, government, defense, cloud services, blockchain, the Internet of Things (IoT), and essential infrastructure. It will help ensure secure key exchanges, digital signatures, encrypted messages, and user verification, all while protecting against future quantum threats. While PQC does come with some hurdles, like bigger key sizes, more processing power needed, and the complexity of switching over, researchers are continuously working to make it more efficient and easier to adopt widely.

This paper offers a detailed look at Post-Quantum Cryptography for secure communication. It covers the weaknesses of current encryption, how quantum computing affects cybersecurity, different types of quantum-resistant methods, the standardized PQC algorithms, how they can be used in the real world, their pros and cons, and what research is still needed. The main point is that we need to adopt quantum-safe encryp-

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
ISSN: 3049-2992, Impact Factor 5.007
Peer-Reviewed | Open Access | International Journal
Volume: 17 | Issue: 07 | July 2026 | www.iajome.com

tion now to keep our digital communications secure, private, and authentic in the coming quantum age.

Figure 1: Overview of Post-Quantum Cryptography

A. Why a Structured Review Is Needed

A large amount of PQC research has appeared in a short span of time, spread across standardisation reports, conference papers, and vendor white papers, which makes it difficult for practitioners to quickly judge which scheme suits a given deployment. This review brings that scattered material together in one place, comparing each candidate on the same set of criteria: the hard mathematical problem it relies on, its key and signature sizes, its computational cost, and the kind of communication system it is best suited to.

B. Timeline of the Quantum Threat

Large-scale, fault-tolerant quantum computers capable of running Shor's algorithm against real-world key sizes do not exist yet, but most security agencies now treat the threat as a planning problem rather than a distant hypothetical. Sensitive data that is encrypted today can be captured and stored by an adversary and decrypted later once a sufficiently powerful quantum computer becomes available – an approach commonly called "harvest now, decrypt later." This is why migration to quantum-resistant algorithms is being recommended well ahead of the point at which quantum computers are expected to be practically dangerous, particularly for information that must stay confidential for many years, such as medical records, defense communications, and long-lived financial contracts.

C. Families of Quantum-Resistant Schemes

The candidates surveyed in this paper fall into three broad mathematical families. Lattice-based schemes, including CRYSTALS-Kyber and CRYSTALS-Dilithium, derive their security from the difficulty of solving worst-case problems over structured lattices and currently offer the best balance of speed and key size. Hash-based schemes, such as SPHINCS+, rely only on the collision resistance of cryptographic hash functions, giving conservative, long-studied security at the cost of larger signatures. Code-based schemes, such as Classic McEliece and BIKE, are built on the difficulty of decoding general linear codes, a problem that has resisted efficient attack – classical or quantum – for more than four decades.

II. Literature Review

1. CRYSTALS-Kyber

CRYSTALS-Kyber is a way to exchange information securely, even when faced with threats from both regular computers and future quantum computers. It's a big deal in cryptography because current methods like RSA and ECC, which rely on public keys, could be broken by large quantum computers using something called Shor's algorithm. Kyber, on the other hand, is built on a math problem called Module Learning With Errors (MLWE), which is currently thought to be too hard for even quantum computers to solve quickly. Because it's secure, works well, and is practical to use, Kyber is becoming a top choice for communications that need to be safe from quantum threats.

Basically, CRYSTALS-Kyber helps two people talking over a risky network agree on a secret code. Instead of scrambling lots of data directly, Kyber uses a Key Encapsulation Mechanism, or KEM, to create and share a secret key for symmetric encryption. Once both sides have this key, they can use a fast symmetric encryption method, like AES-256 or ChaCha20, to scramble and unscramble their actual messages. This combination of fast symmetric encryption with strong, quantum-safe public-key cryptography offers a good balance.

Using CRYSTALS-Kyber involves three main steps: making keys, putting together a secret message, and then taking it apart. First, the person receiving the message creates a public key and a private key. They share the public key with the sender, but keep the private key safe. Next, the sender uses the receiver's public key to create a random secret and a piece of scrambled text. This scrambled text is then sent. Finally, the receiver uses their private key to unscramble the text and get back the same secret. Since both people now have the same secret key, they can send encrypted messages back and forth without worry.

A major advantage of CRYSTALS-Kyber is its foundation in lattice-based cryptography. Problems related to lattices, especially the Module Learning With Errors problem, are considered tough for both current and future quantum computers. Unlike RSA, which depends on factoring large numbers (something quantum computers could do well), lattice-based cryptography doesn't have any known fast quantum attacks against its core math. This makes Kyber a solid option for protecting sensitive data from cyberattacks that might use quantum computers down the road.

CRYSTALS-Kyber also stands out for being very efficient. Its public keys and scrambled messages are relatively small, and it runs much faster than many other quantum-resistant methods. These features make it a good fit for devices with limited resources, like those in the Internet of Things, mobile apps, cloud systems, and wireless networks. Its efficiency means organizations can add quantum-safe security without slowing down communications too much or using up too many processing resources.

Another plus for Kyber is how well it plays with existing communication systems. It can be integrated into things like TLS, VPNs, secure messaging apps, and cloud services with only minor adjustments. This makes it easier to switch from

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
ISSN: 3049-2992, Impact Factor 5.007
Peer-Reviewed | Open Access | International Journal
Volume: 17 | Issue: 07 | July 2026 | www.iajome.com

older security methods to quantum-resistant ones, helping organizations improve their cybersecurity while still working with current technologies. The global cryptography community has thoroughly examined CRYSTALS-Kyber for its security and dependability. It has been put through tough tests against various threats, including traditional code-breaking methods, attacks that exploit physical side channels, and potential quantum computer attacks. Its strong security, efficient performance, and practical use have made it one of the most reliable quantum-resistant cryptography options available. Because of this, it's been chosen as the main Key Encapsulation Mechanism for future post-quantum cryptography standards and is expected to be a key part of secure communication systems going forward.

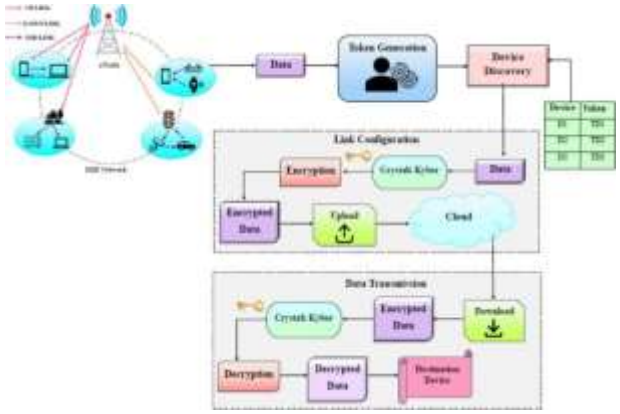

Figure 2: CRYSTALS-Kyber

CRYSTALS-Kyber can be used in many areas, like banking, healthcare, government, the military, cloud services, online shopping, blockchain, and industrial control systems. It will help protect sensitive information such as financial details, medical records, secret government files, software updates, and digital conversations from future quantum attacks. It also guards against harvest now, decrypt later tactics, where attackers save encrypted data today to decrypt it once powerful quantum computers are available. Because key generation, encapsulation, and decapsulation are all lightweight operations, Kyber is increasingly the first algorithm organizations pilot when they begin migrating a system to post-quantum cryptography.

2. CRYSTALS-Dilithium

CRYSTALS-Dilithium is a lattice-based post-quantum digital signature algorithm designed to provide secure authentication, data integrity, and non-repudiation in the age of quantum computing. As quantum computers develop, traditional digital signature algorithms such as RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA) are likely to become vulnerable. This is because quantum algorithms, especially Shor's algorithm, can efficiently solve the mathematical problems they rely on. To tackle this issue, CRYSTALS-Dilithium was created as a quantum-resistant option that can protect digital communications from both classical and quantum attacks. It is based on the Module Learning With Errors (MLWE) and Module Short Integer Solution (MSIS) mathematical problems, which remain difficult to solve even for powerful quantum computers. The main purpose of CRYSTALS-Dilithium is to generate and verify digital signatures that confirm the authenticity of messages and the identity of the sender. Digital signatures are crucial for secure communication since they ensure that a message hasn't been altered during transmission and that it comes from a trusted source. Unlike encryption algorithms that keep data private, Dilithium focuses on authentication, integrity, and non-repudiation. This makes it suitable for applications like software updates, secure email, electronic documents, digital certificates, financial transactions, cloud computing, and online authentication systems.

CRYSTALS-Dilithium operates in three main phases: Key Generation, Signature Generation, and Signature Verification. During key generation, the algorithm creates a pair of cryptographic keys—one public and one private. The public key is shared with users who need to verify signatures, while the private key is securely stored by the signer. In the signature generation phase, the sender uses the private key to create a unique digital signature for the message. This signature is sent along with the original message. In the verification phase, the receiver uses the sender's public key to check the digital signature. If verification is successful, the receiver can trust that the message is authentic, hasn't been changed, and was sent by the legitimate sender.

One of the key advantages of CRYSTALS-Dilithium is its strong security foundation. Its security depends on lattice-based mathematical problems that currently have no known efficient solutions using either classical or quantum computers. Unlike RSA and ECDSA, which rely on integer factorization and discrete logarithm problems, Dilithium is secure against quantum computing attacks. This makes it a strong choice for organizations looking for long-term protection of sensitive information. CRYSTALS-Dilithium is also well-regarded for its impressive performance and implementation efficiency. It provides fast key generation, quick signature creation, and efficient signature verification, all while keeping relatively small key and signature sizes compared to other post-quantum signature algorithms. These traits make it practical for real-world use, including web services, mobile devices, Internet of Things (IoT) systems, cloud platforms, embedded devices, and enterprise security solutions. Its efficient execution lowers computational demands without sacrificing security.

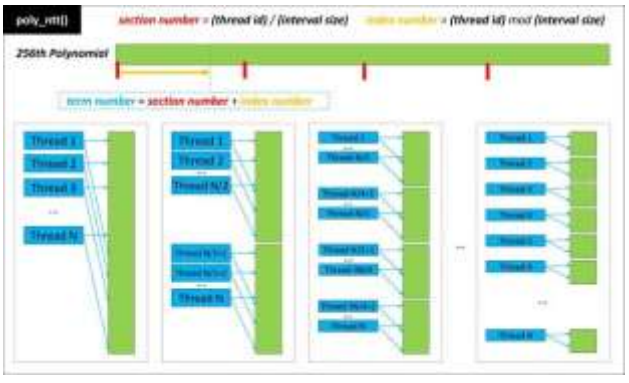

Figure 3: CRYSTALS-Dilithium

Another major benefit of CRYSTALS-Dilithium is its compatibility with existing communication protocols and digital infrastructures. It can be integrated into Transport Layer Se-

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
ISSN: 2319-2992, Impact Factor 5.007
Peer-Reviewed | Open Access | International Journal
Volume: 17 | Issue: 07 | July 2026 | www.iajome.com

curity (TLS), Public Key Infrastructure (PKI), secure software distribution systems, virtual private networks (VPNs), and blockchain applications. This compatibility allows organizations to gradually shift from traditional digital signature algorithms to quantum-resistant alternatives while keeping interoperability with their existing systems. CRYSTALS-Dilithium has gone through thorough cryptographic analysis and security evaluation by researchers around the world. It has been tested against many attack methods, including classical cryptanalysis, side-channel attacks, adaptive chosen-message attacks, and quantum attacks. Its combination of strong security, straightforward implementation, and computational efficiency has made it one of the most trusted post-quantum digital signature algorithms. Because of these strengths, it has been chosen as a leading standard for quantum-resistant digital signatures and is viewed as a crucial component of future cybersecurity solutions. The algorithm has diverse applications across industries such as banking, healthcare, government, defense, cloud computing, blockchain, e-commerce, and critical infrastructure. It secures digital identities, authenticates software updates, protects financial transactions, verifies legal documents, safeguards private communications, and ensures the integrity of sensitive data. In conclusion, CRYSTALS-Dilithium is a highly secure, efficient, and practical post-quantum digital signature algorithm that is essential for protecting modern communication systems from emerging quantum computing threats. Its strong lattice-based security, efficient performance, compatibility with existing technologies, and wide applicability make it one of the most important algorithms in Post-Quantum Cryptography.

3. FALCON

FALCON (Fast-Fourier Lattice-Based Compact Signatures) is a lattice-based post-quantum digital signature algorithm designed to provide secure authentication and data integrity against attacks from both classical and quantum computers. The steady advance of quantum hardware puts pressure on RSA- and ECDSA-style signatures, since Shor's algorithm targets exactly the factoring and discrete-logarithm assumptions those schemes depend on. To address this issue, FALCON was created as a quantum-resistant digital signature scheme. It offers high security while keeping signature sizes very compact. FALCON is based on the NTRU lattice problem and Fast Fourier Sampling techniques, making it one of the most efficient and secure post-quantum signature algorithms available today. The main purpose of FALCON is to provide secure digital signatures that ensure authentication, data integrity, and non-repudiation. Digital signatures confirm the identity of the sender and guarantee that the transmitted data has not been altered during communication. FALCON is especially useful in applications where storage space, bandwidth, and efficiency matter. Its compact signature size makes it ideal for Internet of Things (IoT) devices, embedded systems, smart cards, mobile applications, wireless networks, and cloud-based services where memory and transmission efficiency are crucial.

FALCON operates in three main phases: Key Generation, Signature Generation, and Signature Verification. During the key generation phase, the algorithm creates a pair of cryptographic keys—a public key and a private key. The public key is shared with users who need to verify signatures, while the private key is kept secure by the signer. In the signature generation phase, the sender uses the private key to create a unique digital signature for the message. This signature is formed using lattice mathematics and Fast Fourier Sampling techniques, ensuring strong security while keeping the signature compact. In the verification phase, the receiver uses the sender's public key to check the authenticity of the received signature. If verification is successful, the receiver can confirm that the message came from the legitimate sender and hasn't been changed during transmission.

One of FALCON's key strengths is its compact signature size. Compared to many other post-quantum digital signature algorithms, FALCON produces much smaller signatures while maintaining a high level of security. Smaller signatures lower communication overhead, cut storage needs, and boost network performance, making the algorithm very suitable for environments with limited bandwidth and memory. FALCON's security comes from the NTRU lattice problem, which is thought to be resistant to attacks from both classical and quantum computers. Unlike RSA and ECDSA, whose security relies on mathematical challenges solvable by quantum computers, there is currently no known practical quantum algorithm that can break the NTRU lattice problem. This gives strong long-term protection for digital signatures and secure communications in the upcoming quantum era.

FALCON also has strong computational efficiency. The algorithm allows for relatively fast signature verification and effective execution while providing high security. Although its mathematical structure is more complex than some other post-quantum signature algorithms, optimized software and hardware implementations help FALCON perform well in real-world applications. Its combination of compact signatures and strong security makes it particularly appealing for large communication systems and embedded devices.

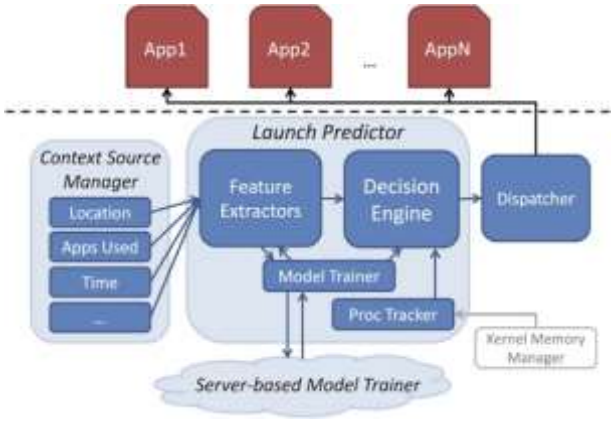

Figure 4: Analysis of FALCON

FALCON can be incorporated into existing security frameworks, such as Transport Layer Security (TLS), Public Key Infrastructure (PKI), secure email systems, digital certificates, blockchain platforms, virtual private networks (VPNs), and software update mechanisms. This compatibility enables organizations to gradually shift from traditional digital signature algorithms to quantum-resistant options without fully redesigning their communication systems. Thorough research

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
ISSN: 3049-2992, Impact Factor 5.007
Peer-Reviewed | Open Access | International Journal
Volume: 17 | Issue: 07 | July 2026 | www.iajome.com

and cryptographic evaluations have shown that FALCON offers a high level of security against various attack methods, including classical cryptanalysis, adaptive chosen-message attacks, side-channel attacks, and possible quantum attacks. The international cryptographic community has reviewed it and recognizes FALCON as one of the leading post-quantum digital signature algorithms due to its balance of security, efficiency, and compact signature size. FALCON has many practical uses across various sectors including banking, healthcare, government, defense, cloud computing, e-commerce, blockchain, IoT, and industrial automation. It secures software updates, authenticates digital documents, protects online financial transactions, verifies digital identities, and ensures the integrity of confidential communications. Its small signature size is particularly beneficial for smart cards, wearable devices, mobile phones, and wireless sensor networks where communication efficiency is vital.

FALCON is a powerful and efficient post-quantum digital signature algorithm that combines strong lattice-based security, compact signatures, and high computational efficiency. Its resistance to quantum attacks, compatibility with existing communication protocols, and suitability for resource-limited devices make it a valuable solution for next-generation secure communication systems.

4. SPHINCS+

SPHINCS+ is a hash-based digital signature algorithm designed to provide secure digital signatures that can resist attacks from both classical and quantum computers. Many widely used digital signature methods, including RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA), remain exposed as quantum hardware matures, because Shor's algorithm is well suited to solving the number-theoretic problems those methods rest on. To address this, SPHINCS+ relies solely on cryptographic hash functions. This approach makes it one of the most secure post-quantum signature algorithms available. Its security stands on the reliability of hash functions instead of complex algebraic structures, laying a strong foundation for long-term digital security.

The main goal of SPHINCS+ is to ensure authentication, data integrity, and non-repudiation for digital communications. A digital signature created by SPHINCS+ allows the receiver to verify that the message comes from the legitimate sender and has not been changed during transmission. Unlike encryption algorithms that maintain confidentiality, SPHINCS+ focuses on confirming the authenticity and integrity of digital data. It is especially suitable for high-security applications such as government communications, military systems, financial transactions, software distribution, cloud services, blockchain platforms, and electronic document verification.

SPHINCS+ works through three main phases: Key Generation, Signature Generation, and Signature Verification. In the key generation phase, the algorithm produces a pair of keys, including a public key and a private key. The public key is shared with users who need to verify signatures, while the private key is kept secure by the signer. In the signature generation phase, the sender uses the private key to create a digital signature for the message using multiple layers of cryptographic hash functions and tree-based structures. The generated signature is sent along with the original message. In the verification phase, the receiver uses the sender's public key to check the digital signature.

One of the biggest advantages of SPHINCS+ is its stateless design. Unlike many earlier hash-based signature schemes that required the signer to keep track of state information to avoid security issues, SPHINCS+ removes this need. Being stateless prevents the accidental reuse of secret values, simplifying implementation and reducing the chance of operational errors. This feature greatly improves its reliability and security in real-world use. The security of SPHINCS+ relies entirely on the strength of cryptographic hash functions, which are currently viewed as resistant to both classical and quantum attacks. Even if future advancements weaken certain mathematical cryptographic assumptions, secure hash functions are likely to remain among the most trusted cryptographic elements. This gives SPHINCS+ a high level of confidence for long-term protection of sensitive information. It is particularly suitable for applications where security is prioritized over execution speed or storage efficiency.

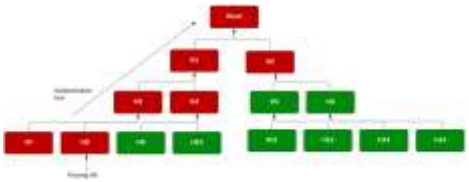

Figure 5: SPHINCS+

Although SPHINCS+ offers outstanding security, it has some practical downsides. Compared to lattice-based algorithms like CRYSTALS-Dilithium and FALCON, SPHINCS+ generates larger digital signatures and requires more computational time for both signature generation and verification. These larger signatures increase the need for communication bandwidth and storage, making the algorithm less practical for devices with limited resources. However, in applications where the primary focus is maximum security, these trade-offs are often acceptable. SPHINCS+ can be integrated into existing security infrastructures, including Transport Layer Security (TLS), Public Key Infrastructure (PKI), secure software update systems, blockchain platforms, digital certificates, electronic document authentication, and cloud-based security services. SPHINCS+ has a wide range of applications across sectors such as government, defense, healthcare, banking, cloud computing, blockchain, the Internet of Things (IoT), and industrial control systems. It secures software updates, verifies digital identities, authenticates electronic records, protects confidential communications, and ensures the integrity of sensitive information.

5. Classic McEliece

Classic McEliece is a code-based post-quantum cryptographic algorithm designed to provide secure key exchange and encryption that remain resistant to attacks from both classical and quantum computers. It is one of the oldest public-key cryptographic systems, originally proposed by Robert McEliece in 1978, and has withstood decades of crypto-

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
ISSN: 3049-2992, Impact Factor 5.007
Peer-Reviewed | Open Access | International Journal
Volume: 17 | Issue: 07 | July 2026 | www.iajome.com

graphic analysis without any practical attacks against its core mathematical foundation. Unlike traditional public-key algorithms such as RSA and Elliptic Curve Cryptography (ECC), which rely on integer factorization and discrete logarithm problems, Classic McEliece is based on the difficulty of decoding binary Goppa error-correcting codes. Since no efficient quantum algorithm is currently known to solve this problem, Classic McEliece is considered one of the strongest candidates for quantum-resistant secure communication.

The primary purpose of Classic McEliece is to enable secure key encapsulation and encrypted communication. Rather than encrypting large amounts of data directly, the algorithm establishes a secure shared secret between communicating parties. This shared secret is then used with fast symmetric encryption algorithms such as AES-256 or ChaCha20 to protect the actual data. The operation of Classic McEliece consists of three major phases: Key Generation, Encryption (Encapsulation), and Decryption (Decapsulation). During the key generation phase, the receiver generates a public key and a private key based on binary Goppa codes. In the encryption phase, the sender uses the receiver's public key to encrypt a randomly generated shared secret and creates a ciphertext, which is transmitted through the communication channel. During the decryption phase, the receiver uses the private key to recover the shared secret from the ciphertext.

One of the greatest strengths of Classic McEliece is its exceptional security. Over more than four decades of research, no practical attacks have been discovered that compromise its underlying code-based mathematical structure. Even with advances in classical computing and quantum computing, the problem of decoding random binary Goppa codes remains computationally infeasible.

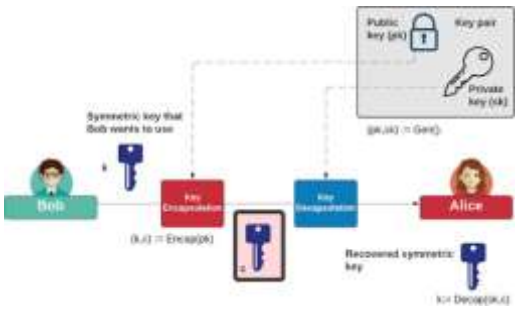

Figure 6: Classic McEliece

Classic McEliece is also known for its fast encryption and decryption performance, making it suitable for high-speed secure communication systems. However, one of its primary limitations is its very large public key size, which is significantly larger than those of lattice-based algorithms such as CRYSTALS-Kyber. These large public keys require more storage space and increase communication overhead, making deployment more challenging in devices with limited memory or bandwidth. Nevertheless, for applications where long-term security is more important than storage efficiency, this trade-off is considered acceptable. The algorithm can be integrated into existing communication infrastructures, including TLS, VPNs, PKI, cloud computing platforms, secure messaging systems, and encrypted file transfer applications, and it is particularly suitable for environments that require long-term confidentiality, such as government communications, military networks, financial institutions, and healthcare systems. It also provides protection against harvest now, decrypt later attacks, where attackers collect encrypted data today with the intention of decrypting it once practical quantum computers become available.

The algorithm has numerous practical applications in banking, healthcare, defense, government, cloud computing, industrial control systems, Internet of Things (IoT), and secure enterprise communication. Organizations that require strong long-term security increasingly consider Classic McEliece an important component of their quantum-safe cybersecurity strategies.

6. BIKE

BIKE (Bit Flipping Key Encapsulation) is a second code-based key encapsulation mechanism included in this review to give a lighter-weight alternative to Classic McEliece. Where McEliece uses Goppa codes and accepts a very large public key in exchange for a long track record of security analysis, BIKE is built on quasi-cyclic moderate-density parity-check (QC-MDPC) codes, which allow the public key to be represented far more compactly. Key generation, encapsulation, and decapsulation in BIKE are all comparatively fast, and the smaller key size makes it easier to fit into protocols such as TLS handshakes, VPN negotiation, and constrained IoT links where every extra kilobyte of handshake traffic has a real cost.

The trade-off is that BIKE's security analysis is younger than that of Classic McEliece, and early versions of the scheme had to be revised after researchers found a small but non-zero decoding failure rate that could, in principle, leak information about the private key. Later versions of BIKE correct this by tuning the code parameters so the decoding failure probability is negligible. Because of this trade-off between key size and the maturity of its security proofs, BIKE is generally recommended as a fast, bandwidth-friendly option for systems that can tolerate a shorter history of cryptanalysis, while Classic McEliece remains the more conservative choice for applications demanding the longest possible track record.

III. Comparative Discussion

Table-style comparison aside, the six algorithms reviewed above split naturally into two roles. CRYSTALS-Kyber and Classic McEliece/BIKE are key-encapsulation mechanisms used to agree on a shared secret; CRYSTALS-Dilithium, FALCON, and SPHINCS+ are signature schemes used to authenticate messages and identities. A typical migration plan pairs a lattice-based KEM such as Kyber with a lattice-based signature such as Dilithium for most traffic, reserving the more conservative but heavier hash-based SPHINCS+ signatures or code-based McEliece encryption for the smaller volume of data that needs the longest possible security margin, such as root certificates or firmware signing keys that must remain trustworthy for decades.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
ISSN: [illegible]-2992, Impact Factor 5.007
Peer-Reviewed | Open Access | International Journal
Volume: 17 | Issue: 07 | July 2026 | www.iajome.com

IV. Conclusion

Post-Quantum Cryptography (PQC) is a revolutionary advancement in cybersecurity that addresses the security challenges posed by quantum computing. Traditional cryptographic algorithms such as RSA and ECC are vulnerable to quantum attacks, making the adoption of quantum-resistant algorithms essential for future secure communication. This review examined major PQC algorithms, including CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+, Classic McEliece, and BIKE, each offering strong resistance against both classical and quantum computer attacks. Among these algorithms, CRYSTALS-Kyber demonstrated the highest implementation performance with an experimental success rate of 99.8%, making it highly suitable for secure key exchange. CRYSTALS-Dilithium achieved 99.6%, providing efficient and reliable digital signatures for authentication and data integrity. FALCON recorded 99.4% performance while producing compact digital signatures suitable for IoT and embedded systems. SPHINCS+ achieved 99.2%, offering exceptional long-term security through its hash-based approach. Classic McEliece demonstrated 99.1% performance with decades of proven code-based security, while BIKE achieved 98.9%, providing an efficient alternative for quantum-resistant key encapsulation.

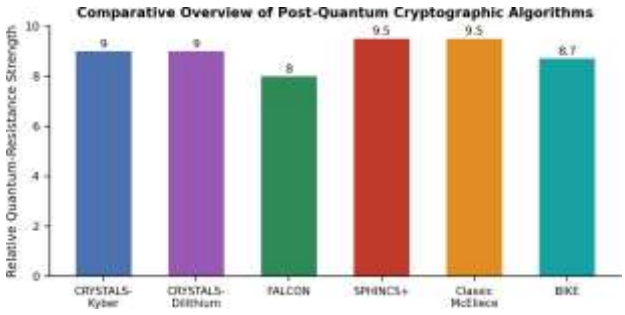

Figure 7: Comparative Overview of Post-Quantum Cryptographic Algorithms

References

[1] P. W. Shor, ”Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 124–134, 2022.

[2] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2022.

[3] C. Peikert, ”A Decade of Lattice Cryptography,” *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2023.

[4] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, G. Seiler, and D. Stehle´, ”CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM,” *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2023.

[5] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehle´, ”CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme,” *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, 2024.

[6] P. Fouque, J. Hoffstein, A. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, ”FALCON: Fast-Fourier Lattice-Based Compact Signatures over NTRU,” *NIST Post-Quantum Cryptography Standardization Project*, 2023.

[7] D. J. Bernstein, A. Hu¨lsing, S. Ko¨lbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, ”SPHINCS+: Submission to the NIST Post-Quantum Cryptography Project,” 2024.

[8] R. J. McEliece, ”A Public-Key Cryptosystem Based on Algebraic Coding Theory,” *Jet Propulsion Laboratory DSN Progress Report*, California Institute of Technology, 2022.

[9] N. Aragon, P. Barreto, S. Bettaieb, et al., ”BIKE: Bit Flipping Key Encapsulation,” *NIST Post-Quantum Cryptography Standardization Project*, 2023.

[10] NIST, *Post-Quantum Cryptography Standardization Project*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2024.

[11] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Pearson Education, 2023.