Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Post Quantum Cryptography: Securing Data in the Quantum Era

Mohammed Kasara
Dept of Computer Science DR DY Patil ACS, Pimpri
Pune, India

Yash Wankhede
Dept of Computer Science DR DY Patil ACS, Pimpri,
Pune, India

***Abstract*- Quantum Computers are no more a science fiction concept, they are the definitive future of computing, with that in mind Quantum computing is going to introduce very new, profound and unprecedented threats to our current cryptography systems and architecture . Public-key algorithms such as RSA and Elliptic Curve Cryptography (ECC), which secure global communications, financial systems, and critical services currently, are mathematically vulnerable to quantum based cyber attacks enabled by Shor's and Grover's algorithms. This vulnerability changes the question of "if" this data's security will be compromised to "when" it will be compromised.**

This paper investigates quantum computing, its impact on classical cryptographic systems and will asses Post Quantum Cryptography (PQC) as a viable approach towards quantum-resistant security. A comparative analysis of major post-quantum approaches including lattice-based, hash-based, and code-based cryptographic schemes is presented, with reference to ongoing standardization initiatives led by the National Institute of Standards and Technology (NIST).

Going beyond theoretical analysis, this study examines the practical challenges presented with PQC, including computational challenges and the need for cryptographic agility. this study examines the practical challenges presented with PQC, including computational challenges and the need for cryptographic agility. Based on these findings, practical and strategic recommendations are proposed for organizations to establish the adoption for PQC architectures. This research highlights the importance of early preparation to ensure the confidentiality, integrity and availability of all digital systems, data and infrastructure.

Keywords:
Post-Quantum Cryptography, Quantum Computing, Quantum-Resistant Security, Classical Cryptography, Public-Key Encryption, Cryptographic Agility, Cybersecurity, Cryptography.

1 INTRODUCTION-

Before delving into quantum cryptography itself, it is imperative to present a succinct overview of conventional cryptography, as it is pertinent to our discussion. Cryptography constitutes the discipline that facilitates the transformation of information exchanged between two entities into a format that is incomprehensible to any unauthorized individual. Despite being an ancient field of study, its range of applications has largely remained confined to military and diplomatic contexts until the advent of electronic and optical telecommunications. Over the past five decades, cryptography has transitioned from its classification as a "classified" science, and it is now progressively mandated by regulations that govern data protection within commercial and public institutions. While confidentiality has historically been the primary application of cryptography, it is presently employed to achieve a wider array of objectives, including data authentication, digital signatures, and non-repudiation. Prior to the transmission of sensitive information, the sender amalgamates the plaintext with a confidential key, employing a specific encryption algorithm, to generate the ciphertext. This encoded message is subsequently dispatched to the recipient, who undertakes the inverse operation, thereby recovering the plaintext by integrating the ciphertext with the confidential key through the utilization of the decryption algorithm. An unauthorized observer is unable to infer the original message from the encoded version without possessing the key. To exemplify this concept, consider a scenario in which the sender secures his message within a safe and secures it with a key. The recipient, in turn, utilizes a duplicate of the key, which he must possess, to access the safe. The methodology is predicated on the premise that both the sender and recipient are in possession of symmetric keys, which are exclusively known to the authorized individuals (commonly referred to as secret or symmetric key cryptography). For an extended period, it was posited that the singular method to address the key distribution conundrum was to convey a tangible medium – such as a disk – encompassing the key. In the contemporary digital landscape, this stipulation is evidently impracticable. Furthermore, it is infeasible to ascertain whether this medium has been intercepted and its

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

contents replicated. During the latter part of the 1960s and early 1970s, scholars affiliated with the British "Government Communication Headquarters" (GCHQ, now designated as the National Cyber Security Centre, or NCSC) devised an algorithm to address this key distribution dilemma. To elucidate, the process can be likened to substituting the aforementioned safe with a padlock. Prior to the communication, the intended recipient transmits an open padlock to the entity responsible for dispatching sensitive information. The recipient retains the key to the padlock. Before relaying the information, the sender secures the padlock, thereby safeguarding the data being dispatched. [2]

Consequently, the recipient is the sole individual capable of unlocking the data using the key that has been retained. Thus, the concept of “public key cryptography” emerged. A crucial phase in the procedure, the distribution of the open padlock, is frequently neglected. The future information sender must be capable of verifying the open padlock, ensuring that it is from the correct sender and has not been altered. In public-key cryptography, this is accomplished through specific certificates issued by trusted entities known as Certificate Authorities, which are attached to the public keys. A public-key cryptography system needs to be incorporated into a foundational Public Key Infrastructure (PKI). Technically, these padlocks represent mathematical formulations of "one-way functions," as they are straightforward to compute but challenging to reverse. Since public key cryptography algorithms entail intricate computations, they tend to be slow. Due to this, they are not utilized for encrypting large volumes of data, but rather for exchanging short session keys used in secret-key algorithms like AES [2,4]. Although it is highly effective, the process of exchanging keys through public key cryptography is affected by two significant limitations. The first limitation is its susceptibility to advancements in technology. With enough computational power or time, one can reverse a one-way function. The resources needed to break an algorithm are dependent on the key length, which must be chosen with care. The second significant weakness of public key cryptography is its susceptibility to advances in mathematics. Despite extensive efforts, mathematicians have yet to demonstrate that public key cryptography is entirely secure. It has proven impossible to eliminate the possibility of classical algorithms that might reverse one-way functions. The emergence of such an algorithm could render public key cryptography insecure in an instant [2,3].

Additionally, evaluating the pace of theoretical advancements is even more complex than tracking technological improvements. There are historical instances in mathematics where a single individual solved a problem that had occupied other researchers for years or even decades. It's conceivable that someone may have already found an algorithm capable of reversing certain one-way functions, yet chosen to keep it confidential. These potential threats indicate that public key cryptography does not assure key distribution that will remain secure in the future. Quantum cryptography addresses the challenge of key distribution by enabling the secure transfer of a cryptographic key between two remote entities, with security ensured by the essential principles of physics. This key can then be employed safely with traditional cryptographic methods. Consequently, a more accurate term for quantum cryptography is Quantum Key Distribution. The fundamental concept of quantum key distribution (QKD) is relatively simple [2,3]. It takes advantage of the principle that, as stated in quantum physics, the act of observing a quantum entity alters it in an irreversible manner. For instance, when you read this document, the page must be illuminated, and the interaction of the light particles will slightly increase its temperature, thereby causing a change. This effect is minimal on macroscopic objects like a sheet of paper. However, the scenario is completely different when it involves microscopic objects. When the value of a digital bit is encoded on a single quantum entity, its interception will inevitably lead to a disturbance because the eavesdropper must observe it. This disturbance results in errors in the bit sequence transmitted between the sender and the recipient. By checking for these errors, the two parties can determine if an eavesdropper has intercepted their key. It is crucial to emphasize that this verification occurs after the bits are exchanged, meaning that one only discovers afterwards whether the communication was compromised [2,3].

This is the reason technology is employed for key exchange rather than for transmitting valuable information. After the key exchange is verified and the key is demonstrably secure, it can then be utilized for data encryption. Quantum physics enables a formal proof that intercepting the key without causing any disturbance is not feasible. [2]

2. Quantum Computing-

Executing mathematical computations, browsing the web, simulating the national economy, predicting the weather, and similar tasks impose a limitation on the performance of even the quickest and most advanced computers. The challenge lies not so much in the speed of microprocessors, but rather in the inherent inefficiency of computers. Contemporary (classical) computers function according to software that breaks a task down into basic operations, which are then executed sequentially, one at a time. Attempts have been made to encourage multiple computers (or at least multiple microprocessors) to tackle different facets of a problem simultaneously, but advancements in parallel computing have

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

been gradual and inconsistent. The primary reason is largely due to the fact that the logic embedded in microprocessors is fundamentally serial (traditional computers may seem to perform multiple tasks simultaneously, like running a word processor and a spreadsheet program, but in truth, the central processor is just switching quickly between tasks). In a genuine sense, a parallel computer would have simultaneity integrated into its very essence. It would be capable of executing numerous operations at the same time, searching instantly through an extensive list of options, and identifying the one that resolves the issue. Such computers are indeed available; they are known as quantum computers [1]. A Quantum computer is no longer a theoretical concept. As stated by numerous specialists, it is considered the most critical technology globally, and nations are competing to achieve dominance in quantum technology with a quantum computer capable of a sufficient number of qubits and fault tolerance. The competition for control over "Quantum Computing" technology extends beyond nations, as it is heavily influenced by major technology companies such as Microsoft, IBM, Google, D-Wave, and Toshiba. Quantum computing gained prominence following the release of the paper "Simulating Physics with Computers" by the American theoretical physicist Feynman. The basic unit of information in a quantum computer is termed a quantum bit, or "qubit," which is more quaternary in nature than binary like the conventional bit utilized in a regular computer. Its conformity to the principles of quantum movements directly results in this qubit feature. As in a classical state bit, a qubit can exist in states that correspond to the logical states 0 or 1, but it can also exist in states that correspond to a blend of superposition of those classical states. To put it another way, a qubit can be either a zero, a one, or both simultaneously. The probability of each state is represented by a numerical coefficient. This idea could seem contradictory given that quantum mechanics, which operates at the atomic level, governs everyday phenomena rather than classical physics. One electron system's spin s=1/2 may be used to physically perceive a qubit, with the two states +1/2 and –1/2 representing two eigenstates of Sz (the z component direction of an external magnetic field of spin ½). An alternative is to employ a single photon beam, with the total states being the horizontal or vertical polarization state with respect to a selected axis. As a result, a qubit can have two values: 0 or 1, which correspond to two different electron spin eigenstates [1].

3. Classic Cryptography: An Insecure System

Without cryptography, information security is unthinkable today. There are several ways to utilize cryptography to safeguard the integrity and confidentiality of data. Products for information security, including software and hardware, use cryptography in a variety of inventive methods with the sole goal of security. Cryptographic operations like encryption and decryption, key generation, authentication, signatures, and more are described by cryptographic algorithms, which are well-defined processes or sequences of rules or stages, or a set of mathematical equations.

Symmetric and asymmetric cryptographic algorithms are the two basic categories into which cryptographic algorithms fall. [2,3]

- **Algorithms for symmetric cryptography:** Both the sender and the recipient encrypt and decode data using the same key in symmetric cryptography techniques. Symmetric key algorithms are incredibly effective and simple to use. Key management in symmetric cryptography is a difficult problem, though. Before starting the conversation, the two participants must exchange the key. Symmetric ciphers are primarily vulnerable to linear cryptanalysis, differential cryptanalysis, chosen-plaintext assault, and known-plaintext attack. [2,3]

- **Asymmetric Cryptography method:** This type of method uses a pair of keys that are used by both the sender and the recipient. The private key is the one that is kept private, while the public key is the one that is made public. A public-key algorithm is another name for an asymmetric cryptography method. [2,3]

Therefore, Quantum Key Distribution is a more accurate term for quantum cryptography. The fundamental idea behind quantum key distribution (QKD) is really simple. It takes use of the fact that, in accordance with quantum physics, a quantum item is irreparably perturbed just by being observed. For instance, the white paper has to be lighted when you read it. It will be somewhat heated by the impact of the light particles, changing it as a result. For a macroscopic item like paper, this impact is negligible. With a minuscule item, on the other hand, the circumstances are completely different. Because the eavesdropper is compelled to examine the digital bit, its interception will always result in a disturbance if the value of the bit is encoded on a single quantum object [2,4]. The sender and destination exchange bits in an incorrect order as a result of this disruption. By looking for these mistakes, both parties can confirm if an eavesdropper was successful in obtaining details on their key. It is crucial to emphasize that one learns whether or not the communication was intercepted

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

a posteriori since this verification occurs after the bits are exchanged. For this reason, the technique is utilized to trade keys rather than important data. Data encryption is possible when the key exchange has been verified and the key has been shown to be safe. The formal proof that the key cannot be intercepted without disturbance is made feasible by quantum physics. What does it actually mean to encode a digital bit's value on a quantum object? Light is frequently employed in telecommunication networks for information exchange. A pulse is released for every piece of data, and it travels to the receiver via an optical fiber—a thin glass fiber used to transmit light signals—where it is recorded and converted back into an electrical signal. Millions of light particles known as photons are usually present in these bursts. The identical methodology is used in quantum key distribution, with the exception that there is only one photon in each pulse. According to the principles of quantum physics, a single photon is a very small quantity of light—your eyes detect billions of photons per second while you read this white paper. Specifically, it cannot be divided in two. This implies that an eavesdropper cannot intercept half of a photon and use the other half to determine the value of the bit it contains. He must watch the photon in order to determine the bit's value, which means he will break the connection and make himself known [2]. An improved approach would be for the eavesdropper to detect the photon, record the bit value, and then create a new photon based on the outcome to deliver to the recipient. By making the eavesdropper introduce mistakes, the two legitimate parties work together to stop him from doing so in QKD. To do this, protocols have been developed. [2,4]

3.1 Advantages/Disadvantages of QKD

Some advantages of quantum cryptography include the following [2,3]:

- **Unconditional Security:** QKD's security is theoretically unquestionable because it is founded on the core concepts of quantum physics. There will be noticeable disruptions introduced by any effort to measure or intercept the quantum states employed in QKD.
- **Future-Proof Security:** Unlike classical cryptography techniques, which can be compromised by increases in processing power (for instance, quantum computers breaking RSA or ECC), quantum cryptography protocols are safe from future technological advancements because they are based on physical principles.
- **Tamper Detection:** QKD is equipped with an eavesdropping detection system. Errors in the key will be introduced by any illegal measurement or observation of the quantum channel, and they can be found at the reconciliation stage.

Although QKD has a lot of potential, there are a number of obstacles to its actual application [2,4]:

- **Photon Loss and Noise:** Signal degradation and a reduction in the effective communication distance can result from photon loss and noise in quantum channels, like optical fibers. The normal operating range of current QKD systems is a few hundred kilometers, while attempts are being made to increase this range.
- **Quantum Repeaters:** These devices are being developed to get around distance restrictions. By entangling photons over great distances, these devices can increase the range of quantum communication and enable the safe transfer of keys across much bigger networks.
- **Integration with Classical Networks:** Complex hardware and protocols are needed to integrate QKD with the current classical communication networks. In order to offer workable and scalable solutions, hybrid systems that blend conventional and quantum cryptography approaches are being investigated.
- **Infrastructure and Cost:** Deploying the specialized equipment needed for QKD can be costly and complicated. Work is being done to create quantum communication systems that are more reliable and affordable.

.

3.2 National Concerns

Government agencies and IT behemoths worldwide are fully aware of the significance of the Quantum- Safe algorithm. That day is drawing near, and the threat is real. The design, development, testing, and migration plan for quantum-safe algorithms have therefore been initiated by several nations and standard bodies [3,4].

The framework, policy documents, whitepapers, technical details, standards documents, and economical migration methods to post-quantum cryptography are being published by the working group, forum, and standard organizations. The following are some of the groups spearheading the standardization process:

- **PQC Standardization by the National Institute of Standards and Technology (NIST):** The National Institute of Standards and Technology (NIST) has assumed the lead in requesting, assessing, and standardizing quantum-resistant public-key cryptography algorithms. In 2016, NIST issued a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

request for proposals and started the process of identifying the standards and specifications for quantum- safe algorithms. In 2017, the first round of entries was revealed, and 69 of the 82 submissions received were named as first round possibilities. 2018 saw the first NIST QPC standardization meeting and analysis of the first round of candidates. 26 candidates were announced for the second phase of the NIST PQC standardization meeting, which took place in 2019. During the third round in 2020, the NIST named seven finalists and eight alternate candidates. In July 2022, NIST finished the third round of the procedure. Four algorithms have been chosen for standardization, and four more have been given consideration for the fourth evaluation round. The realistic timetable for the creation and implementation of NIST PQC standards [3,4].

- **The European Telecommunication Standards Institute (ETSI):** This organization is currently developing post-quantum-safe algorithms through its Cyber Quantum-Safe Cryptography (QSC) group. Recommending a quantum-safe cryptographic method and its application is the goal of the QSC working groups. Performance, implementation capabilities, and design consideration for particular applications are the main points of emphasis. The organization has released suggestions, problems, and cost-effective migration options to post-quantum cryptography. Since 2013, ETSI has also been hosting workshops on post-quantum cryptography [3,4].

Researchers and scientists are putting a lot of effort into creating and standardizing quantum-safe cryptography methods. However, aside from the work done by NIST, not much information is in the public domain. The NIST procedure for requesting, assessing, and standardizing quantum-resistant cryptographic algorithms is quite thorough, and comprehensive data is released. Therefore, it was decided to compare the seven finalists and eight alternative quantum-resistant algorithms that NIST had released during the third round in 2020. The analysis's goal is to evaluate the potential algorithms' viability for implementation by looking at their CPU cycle and memory use. The Open Quantum Safe (OQS) project is used to analyze the algorithms' performance. Quantum-resistant encryption methods are being developed and prototyped as part of this research. An open-source library for quantum-resistant cryptographic algorithms called "liboqs" was created by OQS. The NIST Post-Quantum Cryptography standards for Key Encryption Mechanisms (KEM) and Signature Schemes is the primary emphasis of OQS [3,4].

Additionally, the OQS offers benchmarking data for a number of quantum-resistant algorithms, which are utilized in this study to compare the memory consumption and runtime behavior of the algorithms.

Based on the algorithms' execution on Amazon Web Services (AWS) using a CPU Model Intel(R) Xeon(R) Platinum 8259CL CPU at 2.50 GHz, runtime behavior and memory usage metrics are gathered. The Open Quantum Safe (OQS) project is used to analyze the algorithms' performance. Quantum-resistant encryption methods are being developed and prototyped as part of this research. An open-source library for quantum-resistant cryptographic algorithms called "liboqs" was created by OQS. The NIST Post-Quantum Cryptography standards for Key Encryption Mechanisms (KEM) and Signature Schemes is the primary emphasis of OQS. Additionally, the OQS offers benchmarking data for a number of quantum- resistant algorithms, which are utilized in this study to compare the memory consumption and runtime behavior of the algorithms. Based on the algorithms' execution on Amazon Web Services (AWS) using a CPU Model Intel(R) Xeon(R) Platinum 8259CL CPU at 2.50 GHz, runtime behavior and memory usage metrics are gathered [3,4].

3.3 Methodologies

The method for code-based cryptography (e.g., McEliece) depends on the difficulty of decoding a linear error-correcting code, which may be selected with a certain structure or within a particular family (e.g., quasi-cyclic codes, or Goppa codes). Daniel J. Bernstein proposed Classic McEliece, a code-based post-quantum public-key cryptosystem (PKC) candidate for NIST's global standardization in 2017. [2,3]

According to McEliece's theory, the Goppa code and the linear transformation result in a public key. The sender must provide a certain quantity of random noise in order to encrypt the message. The Goppa code is the sole way to eliminate the noise [66,70]. Without knowing how to factor in the public key, recovering the message is a computationally difficult task for the attacker. Some possible quantum-safe algorithms among the many code-based cryptography techniques that are available include [2,3,4]:

- Robert McEliece debuted Classic McEliece in 1978. The suggested algorithm for the **Key Encapsulation Mechanism (KEM)** is code- based. Since its introduction, the algorithm has seen very few modifications. The purpose of altering the algorithm's security settings is to speed up calculation. It is possible to configure the classic McEliece settings to correspond to each of the five NIST

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

security levels. The Classic McEliece method requires a very high public key size, but its calculation time is incredibly quick.

- A code-based key encapsulation technique is called **Bit Flipping Key Encapsulation**, or **BIKE**. Bit flipping decoding methods may be used to decode quasi-cyclic moderate density parity-check (QC-MDPC) codes, which are its foundation. NIST security levels 1 and 3 may be met by BIKE.

- A code-based public-key technique called **HQC (Hamming Quasi-Cyclic)** was created to offer security against both conventional and quantum computers. NIST 1, 3, and 5 security levels are intended to be attained with the HQC algorithm.

Cryptographic hash functions are non-reversible operations that generate a fixed-length output from an input string of arbitrary length. The Merkle signature and other digital signatures are frequently created using hash-based encryption. It combines the Merkle tree with a one-time signature. Numerous one-time signature (OTS) algorithms are grouped together to form the hash-based signature (HBS). HBS efficiently combines many OTS using a tree data structure. A single OTS is selected from the collection by an HBS and used to sign a message. The crucial point is that security is jeopardized if the HBS selects the same OTS again. Quantum-safe cryptographic methods that rely on hashing include [2,3,4]:

- **SPHINCS+:** a stateless hash-based signature system. It is a modified form of SPHINCS with the specific goal of making the signature smaller. Three distinct signature systems are suggested in the SPHINCS+ NIST submission: The combination of SPHINCS and SHAKE256, Haraka and SPHINCS+, SPHINCS and SHA-256. NIST announces SPHINCS+ as an alternative in the third algorithm selection round. The approach satisfies NIST 1, 3, and 5 security standards and may be used for digital signatures.

The computational difficulty of lattice issues, which are based on the shortest vector problem (SVP), is the foundation of lattice-based encryption. Here, our objective is to produce the shortest nonzero vector in an input lattice represented by an arbitrary basis [3,4].

In other words, given the basis of a lattice, the attacker's objective is to determine the shortest vector from the origin. An response with a zero vector is ineffective. The technique offers extremely strong security proofs based on worst- case hardness and is implemented quite efficiently. The following is a possible lattice-based quantum- safe algorithm [3,4]:

- The two cryptographic primitives included in CRYSTALS-KYBER are **Dilithium**, a robustly EUF-CMA-secure digital signature method, and **Kyber**, an IND-CCA2-secure key- encapsulation mechanism (KEM). Both techniques are based on the lattice-based hard problem. The technique has a tiny public key and is computationally quick. Its characteristics are adjusted to correspond with NIST security levels 1, 3, and 5.

- **NTRU**: Mathematicians Joseph H. Silverman, Jill Pipher, and Jeffrey Hoffstein created it in 1996. A post-quantum secure version of NTRU was created in 2013 by Damien Stehle and Ron Steinfeld. Its foundation is the difficulty of resolving the Ring-learning-with-errors (Ring- LWE) problem. Shor's algorithm can't be used to attack the algorithm.

- **SABER:** a member of the family of lattice- based cryptography algorithms. The algorithm's security depends on how challenging the Module Learning with Rounding issue (MLWR) is. The SABER-suite offers three security levels:

- LightSABER (NIST Level 1) • SABER (NIST Level 3)
- FireSABER (NIST Level 5)

FrodoKEM is based on the algebraically unstructured lattice. The algorithm has fewer parameter restrictions but a large public key size [43]. FrodoKEM is designed for IND- CCA security at three levels:

FrodoKEM-640, which targets Level 1 in the NIST. FrodoKEM-976, which targets Level 3 in the NIST. FrodoKEM-1344, which targets Level 5 in the NIST.

A modified version of the original NTRU, NTRU Prime has removed a number of the lattice security review's complexities.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

The foundation of **CRYSTALS-DILITHIUM** is Lyubashevsky's "Fiat-Shamir with Aborts" approach, which employs rejection sampling to create compact and secure lattice-based Fiat- Shamir schemes. Of all the lattice-based signature schemes that rely only on uniform sampling, Dilithium is said to have the shortest public key and signature size.

Gentry, Peikert, and Vaikuntanathan's theoretical framework served as the foundation for the creation of the lattice-based signature system known as **FALCON**. The approach's security stems from the fact that, even with the aid of quantum computers, there is presently no effective general-case solving algorithm for the underlying hard issue of the short integer solution problem (SIS) over NTRU lattices.

5 CONCLUSION-

We are at a unique point in time where we are seeing the traditional algorithms we have trusted for so long begin to break down while at the same time we are seeing the new age of security and computing go from being concepts to actively being tested to being deployed in government organizations to reaching the average person. This is the first time in decades of computer innovation that we have reached a limit that was thought to be impossible to penetrate just a few years ago. The security of our digital lives is no longer in the hands of mathematical algorithms that were predicted to be impossible to compute for millions of years. The mere fact that a machine has the capacity to break encryption all together is enough to alert everyone on the planet to get ready and make the required adjustments before the entire world becomes an open book, even though quantum computers need far more power and qubits than we currently have available to truly break encryption globally.

Being the first to adapt will undoubtedly be rewarding for organizations, but fending off quantum-powered threats and attacks won't be easy. To fully transition to a post-quantum world, we will need to make significant changes to not only our systems and infrastructure but also our awareness, training, education, and trends. The cost of organizations transitioning into the quantum era will be greatly decreased if these changes are made early on.

Having stakeholders who understand this and take the necessary precautions to get ready for this extremely difficult stage will be crucial in protecting businesses, trade secrets, workflows, and most importantly, the people who created it all.

REFERENCES:

[1] Prashant, “A Study on the basics of Quantum Computing” Department d’Informatique et de recherché operationnelle, Universite de Montreal, Montreal. Canada.

[2] IDQ, “Understanding Quantum Cryptography”, May 2020, info@dquantique.com, www.idquantique.com

[3] Manish Kumar, “Post-quantum cryptography Algorithm's standardization and performance analysis”, ScienceDirect, Array, Volume 15, September 2022, 100242.

[4] Swastik Kumar Sahu, Kaushik Mazumdar, “State-of-the-art analysis of quantum cryptography: applications and future prospects”, 06 August 2024

[5] Sec. Quantum Engineering and Technology Volume 12 - 2024 | https://doi.org/10.3389/fphy.2024.1456491 Department of Electronics Engineering, Indian

[6] Institute of Technology ISM Dhanbad, Dhanbad, India