IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, April 2024

Quantum Cryptography: Advancements, Challenges, and Applications in Modern Communication

Vimmi Malhotra[1], Sahil Yadav[2], Vishal[3]
Assistant Professor, Department of Computer Science Engineering[1]
UG Students, Department of Computer Science Engineering[2,3]
Dronacharya College of Engineering, Gurgaon, India

Abstract*: This research paper explores the fascinating field of Quantum Cryptography, a cutting-edge technology that leverages principles of quantum mechanics to secure information transfer. The objective of this study is to delve into the underlying principles of Quantum Cryptography, specifically Quantum Key Distribution (QKD), and discuss its potential applications and challenges. The methodology involves a comprehensive review of existing literature and recent advancements in the field. The key findings reveal that Quantum Cryptography presents a promising solution for secure communication, offering robust defence against potential eavesdroppers. However, practical implementation faces several challenges, including technological limitations and the need for standardization. The implications of this study underscore the transformative potential of Quantum Cryptography in shaping the future of secure communication and highlight the need for further research and development in overcoming existing challenges.*

Keywords: Quantum Cryptography

I. INTRODUCTION

In the realm of cutting-edge modern security, cryptography serves as an important pillar. As we navigate deeper into the digital age, the call for sturdy and impenetrable cryptographic structures becomes more and more essential. This paper embarks on an exploration of the significance of cryptography in safeguarding information in our contemporary world. But it's essential to observe that classical cryptographic systems aren't without their limitations. With the advent of effective computational capabilities, these conventional structures face potential threats. The vulnerabilities of those systems turn out to be more obvious as computational power continues to evolve, casting a shadow on the reliability of classical cryptographic structures.

In reaction to those challenges, a brand new contender has emerged on the horizon: quantum cryptography. This generation, which leverages the standards of quantum mechanics, promises a stage of safety where some distance surpasses its classical opposite numbers. The advent of quantum cryptography marks a tremendous milestone in the subject of information security, supplying a beacon of hope in the face of the constraints of classical cryptographic systems. This paper sets the stage for a comprehensive exploration of quantum cryptography, delving into its ability, the challenges it faces, and the results it holds for the destiny of fact protection.

1.1 Basics of Quantum Mechanics:

Quantum mechanics, the theoretical framework that underpins the conduct of particles on the quantum degree, introduces several key ideas that are fundamental to the understanding and application of quantum cryptography.

The principle of superposition, a cornerstone of quantum mechanics, posits that a quantum machine can exist in more than one state simultaneously until it is measured. This precept is leveraged in quantum cryptography to create quantum bits, or qubits, which, unlike classical bits that can be either zero or 1, can exist in a superposition of states. This allows for a higher degree of complexity and record density in quantum cryptographic systems.

DOI: 10.48175/IJARSCT-17591

We delve into the phenomenon of quantum entanglement and every other unusual component of quantum mechanics. While particles end up entangled, the country of one particle becomes instantly correlated with the state of the opposite, no matter the gap isolating them. Thisspooky movement at a distance', as Einstein famously defined it, paperwork the premise for quantum key distribution (QKD), a method used in quantum cryptography to safely percentage encryption keys.

The Heisenberg Uncertainty Principle states that it's not possible to simultaneously determine the exact position and momentum of a particle. In the context of quantum cryptography, this principle guarantees the safety of a quantum channel. Any attempt to snoop on a quantum verbal exchange could disturb the device and reveal the presence of the intruder.

Those standards of quantum mechanics, while carried out in cryptography, offer a powerful device for comfortable verbal exchange. They allow for the introduction of cryptographic systems that are not handiest comfortable in opposition to modern computational abilities but additionally towards future advancements in computing power, which includes the tons-anticipated quantum computers.

1.2 Basics of Classical Cryptography:

Classical cryptography encompasses a number of cryptographic strategies that have been used for comfortable communication long before the appearance of modern cryptographic methods.

At the coronary heart of classical cryptography are two essential strategies: symmetric and asymmetric encryption. Symmetric encryption, also called secret-key encryption, entails the use of an equal key for each encryption and decryption. This technique is straightforward and fast, making it suitable for encrypting large amounts of data. However, it offers a great challenge in terms of key distribution: the important thing must be securely shared among the communicating events without being intercepted.

However, uneven encryption, additionally called public-key encryption, uses extraordinary keys: a public key for encryption and a private key for decryption. This approach removes the important distribution trouble of symmetric encryption, as the general public key can be freely allotted without compromising safety. However, uneven encryption is computationally extensive, making it much less appropriate for encrypting large quantities of records.

Even though classical cryptographic strategies have proven powerful in many eventualities, they are not without their vulnerabilities and demanding situations. As stated, key distribution is a full-size task in symmetric encryption. Additionally, the security of classical cryptographic structures relies closely on the computational issue of sure troubles, including factoring big numbers in the case of RSA, a popular uneven encryption algorithm. but, with the advent of quantum computers, those issues should doubtlessly be solved extra efficaciously, posing a hazard to the safety of classical cryptographic structures.

1.3 Ideas of Quantum Cryptography:

Quantum cryptography represents a paradigm shift in relaxed conversation, leveraging the concepts of quantum mechanics to achieve unheard-of security.

The cornerstone of quantum cryptography is quantum key distribution (QKD). In contrast to classical cryptographic strategies, which rely on the computational issue of positive troubles, QKD uses the principles of quantum mechanics to ensure protection. The maximum protocol of QKD is the BB84 protocol, proposed by means of Bennett and Brassard in 1984. In this protocol, the sender (Alice) sends quantum states to the receiver (Bob), who measures them. The secret is then generated based on these measurements. Any attempt by an eavesdropper (Eve) to intercept the key will inevitably disturb the quantum states because of the Heisenberg uncertainty principle, alerting Alice and Bob to the presence of an eavesdropper.

One of the primary benefits of QKD over classical cryptographic techniques is its safety. In classical cryptography, the safety of the important thing is predicated on the computational issue of certain troubles. but, with the arrival of powerful computer systems and doubtlessly quantum computer systems, these troubles might be solved extra efficaciously, posing a risk to the security of classical cryptographic systems. On the other hand, the safety of QKD is guaranteed by the legal guidelines of quantum mechanics, which might be believed to be inviolable. Consequentially, the key generated by QKD is theoretically unconditionally cozy.

But it’s essential to note that at the same time as QKD holds awesome promise, it additionally faces sizable challenges. A realistic implementation of QKD calls for the capability to ship and acquire quantum states with high precision, which is technologically difficult. Moreover, the key generated by using QKD is usually shorter than the message to be encrypted, which calls for using a method known as privateness amplification to create a longer key.

II. QUANTUM COMMUNITY ARCHITECTURES

Quantum Key Distribution (QKD) protocols leverage the standards of quantum mechanics to ensure comfortable conversation. Right here, we talk about three distinguished QKD protocols: BB84, E91, and SARG04.

- **BB84 Protocol:** The BB84 protocol, developed with the aid of Charles Bennett and Gilles Brassard in 1984, is the first quantum cryptography protocol. On this protocol, the sender (Alice) sends quantum states to the receiver (Bob), who measures them. The secret's then generated primarily based on these measurements. Any attempt by an eavesdropper (Eve) to intercept the key will unavoidably disturb the quantum states because of the Heisenberg Uncertainty Precept, alerting Alice and Bob to the presence of an eavesdropper. The security of the BB84 protocol is assured by way of the legal guidelines of quantum mechanics, making it theoretically unconditionally relaxed.
- **E91 Protocol:** The E91 protocol, proposed by Artur Ekert in 1991, is another sizable QKD protocol. It uses the principle of quantum entanglement and the identities prescribed through Bell’s Take a Look at Entangled Qubits. Within the E91 scheme, Alice and Bob use a quantum channel to alternate qubits, permitting them to generate a shared key that is proof against eavesdropping. The security of the E91 protocol is also guaranteed by the laws of quantum mechanics.
- **SARG04 Protocol:** The SARG04 protocol, named after Valerio Scarani, Antonio Acín, Gregoire Ribordy, and Nicolas Gisin, is a 2004 quantum cryptography protocol derived from the BB84 protocol. Researchers developed SARG04 to improve the robustness of the primary protocols in quantum cryptography towards the photon-variety-splitting attack when attenuated laser pulses are used in place of single-photon sources. Within the SARG04 scheme, Alice wishes to ship a non-public key to Bob. She starts offevolving with strings of bits, and every bit is long. She then encodes those strings as a string of qubits. The security of the SARG04 protocol is also guaranteed by means of the laws of quantum mechanics.

2.1 Quantum Cryptography Implementations:

Quantum cryptography, in particular Quantum Key Distribution (QKD), has seen huge improvements in both the experimental and business domains. These implementations are more and more being deployed in diverse sectors, along with government, finance, and healthcare, due to their superior safety functions.

Experimental and commercial QKD networks: Experimental QKD networks were hooked up worldwide to test the feasibility and safety of quantum cryptography in real-world situations. These networks often contain collaborations among universities, research institutions, and industry partners. They function as testbeds for brand new QKD protocols, quantum repeaters, and different quantum technologies. On the economic front, numerous companies have advanced QKD structures that are now commercially available. These structures are usually designed to comfort fiber-optic networks, and they include all the important components for key distribution, together with quantum random variety mills, quantum transmitters (Alice), quantum receivers (Bob), and classical put-up-processing gadgets.

Deployment in the Government, Finance, and Healthcare Sectors: The authorities region has been a vast adopter of QKD generation, on the whole, for securing touchy communications. For example, quantum networks have been deployed for relaxed communication among authority buildings. In the finance zone, QKD is getting used to secure transactions and shield sensitive monetary data. The generation ensures that eavesdropping attempts on statistical transmission can be detected, accordingly presenting an excessive level of protection for monetary transactions. The healthcare area additionally sees the ability of QKD to shield affected person records. With the increasing digitization of fitness records, the need for secure record transmission is more important than ever. QKD provides a way to do this by imparting theoretically unbreakable encryption.

Hardware necessities for success Implementation: The successful implementation of a QKD device requires numerous hardware additives. Those consist of a source of quantum states (commonly a laser), a quantum channel (which

DOI: 10.48175/IJARSCT-17591

includes a fiber-optic cable), detectors for measuring quantum states, and devices for appearance mistake correction and privacy amplification. Additionally, the machine requires a classical conversation channel for sifting and reconciliation procedures. The hardware should be cautiously calibrated and maintained to ensure the integrity of the quantum states. In spite of those challenges, ongoing technological improvements continue to improve the practicality and accessibility of QKD systems.

2.2 Processing and Authentication in Quantum Cryptography:

Quantum Key Distribution (QKD) systems contain numerous post-processing techniques to ensure the security and integrity of the quantum keys. Those strategies encompass error correction, privacy amplification, and record reconciliation.

- **Error Correction:** In QKD systems, blunder correction is a critical publish-processing step. Because of the inherent noise in quantum channels and imperfections in quantum devices, errors can occur in the course of the transmission of quantum states. Those errors can result in discrepancies in the keys generated by Alice and Bob. Mistake correction protocols are used to hit upon and correct those mistakes, making sure that Alice and Bob share the same key. Numerous error correction algorithms were evolved for QKD structures, including Cascade, Winnow, and LDPC codes.
- **Privateness Amplification:** privacy amplification is any other essential post-processing approach in QKD. Even after error correction, there might be some residual facts about the key that an eavesdropper could probably have. Privateness amplification is used to reduce these statistics to an arbitrarily small level. It entails making use of a normal hash feature for the important thing, which reduces its duration but ensures that any last records an eavesdropper would possibly have are negligible.
- **Statistics Reconciliation:** Statistics reconciliation is intently related to error correction. It involves Alice and Bob publicly comparing a subset of their keys to estimate the quantum bit blunders price (QBER). This lets them gauge the level of discrepancies in their keys because of either eavesdropping or noise in the quantum channel. Based totally on the anticipated QBER, they can then observe mistake correction protocols to correct the mistakes and reconcile their keys.
- **Quantum Key Authentication:** similarly to these put-up-processing strategies, quantum key authentication is another crucial issue in QKD. Authentication guarantees that the quantum keys are indeed exchanged among Alice and Bob and not between Alice and an eavesdropper impersonating Bob or vice versa. Diverse authentication schemes had been proposed for QKD, inclusive of two-way authentication protocols and one-manner hash functions.

III. HACKING AND COUNTERMEASURES

Quantum Key Distribution (QKD) structures, which can be the cornerstone of quantum cryptography, are not proof against threats. Two huge threats to QKD structures are photon-range splitting and intercept-resend assaults.

Photon-wide variety splitting attacks take advantage of a vulnerability in QKD systems that use vulnerable coherent pulses. In this type of attack, an eavesdropper, often known as Eve, splits off a part of the quantum signal and measures it, leaving the relaxation of the signal to be maintained for the intended recipient. This allows Eve to benefit from records that are approximately the key without introducing detectable mistakes.

Intercept-resend attacks are another hazard to QKD structures. In this form of assault, Eve intercepts the quantum signal dispatched from the sender, measures it, and then resends a new signal to the recipient based on the end result of her measurement. This sort of assault can be detected because measuring a quantum device changes its state, introducing mistakes into the transmitted key.

Countermeasures to those threats evolved into comfortable QKD structures. One such countermeasure is the use of decoy states. Decoy states are extra quantum states that can be dispatched in conjunction with the real quantum signal. Those decoy states are used to hit upon eavesdropping through Eve. If Eve attempts to measure the quantum sign, she can also measure the decoy states, so one can screen her presence.

Another countermeasure is using measurement-tool-impartial QKD (MDI-QKD). In MDI-QKD, the measurement tool is placed in a location that is independent of the sender and receiver, and the security of the important thing now does not depend on the trustworthiness of the measurement tool. This makes it impossible for Eve to gain facts about the key by using the controlling size tool.

3.1 Effect of quantum cryptography on classical cryptography :

Quantum computing poses a significant hazard to classical cryptographic algorithms by leveraging quantum algorithms that may efficaciously clear up positive mathematical problems that underpin the security of these algorithms. One of the most first-rate threats comes from Shor's algorithm, which could element large numbers exponentially quicker than the first-rate-regarded classical algorithms. This poses an immediate risk to widely used asymmetric encryption algorithms, along with RSA, which is predicated on the problem of factoring large numbers for its security.

Further, quantum computers could efficaciously clear up the discrete logarithm trouble, which bureaucracy the basis for many cryptographic schemes, which include the virtual signature set of rules (DSA) and elliptic curve cryptography (ECC). As a result, those broadly deployed cryptographic algorithms would become vulnerable to attacks, undermining the safety of digital signatures and key exchange protocols.

To deal with those vulnerabilities, researchers have been exploring the improvement of quantum-resistant cryptographic primitives, also referred to as put-up-quantum cryptography (p.c.). Those cryptographic algorithms are designed to resist assaults from both classical and quantum computers. One technique entails leveraging mathematical problems that might be believed to be hard even for quantum computers to solve correctly, along with lattice-based cryptography, code-primarily based cryptography, hash-based total cryptography, and multivariate polynomial cryptography.

Lattice-based Cryptography, for example, is based on the difficulty of certain troubles associated with lattices in multidimensional spaces. Those issues are believed to be resistant to quantum algorithms like Shor's algorithm. Similarly, code-based cryptography relies on the hardness of decoding random linear codes, which is also believed to be tough for quantum computers.

The National Institute of Standards and Technology (NIST) has been making major efforts to standardize put-up-quantum cryptographic algorithms, soliciting submissions and carrying out evaluations to pick out the most promising applicants. The goal is to expand a brand new technology of cryptographic algorithms that could face up to the chance posed with the aid of quantum computer systems, making sure the lengthy-term protection of virtual conversation and facts systems.

3.2 Rising technologies :

The combination of quantum cryptography with rising technology, together with artificial intelligence (AI) and blockchain, is a charming region of research that holds big potential for advancing virtual security paradigms. Quantum cryptography, which leverages the standards of quantum mechanics to create comfortable records, ought to provide a strong layer of protection for these technologies.

Synthetic intelligence, for example, is more and more being utilized in touchy packages throughout numerous sectors, which include healthcare and finance. Those AI structures cope with sizable amounts of exclusive records, making them appealing targets for cyber threats. The combination of quantum cryptography may want to offer greater security measures for these structures, ensuring the confidentiality and integrity of the facts they system. This will now not only defend these structures from cyber threats but also bolster their consideration in AI programs, thereby accelerating their adoption across unique sectors.

Similarly, blockchain generation, which underpins virtual currencies and smart contracts, is predicated heavily on cryptographic algorithms for securing transactions. The mixing of quantum cryptography ought to extensively enhance the security of these transactions. This could result in the improvement of extra-secure and strong digital currencies and clever contracts, thereby strengthening the blockchain atmosphere.

The synergies between quantum cryptography and these emerging technologies could lead to the improvement of novel protection paradigms. For example, the aggregate of AI and quantum cryptography may want to result in the improvement of wise safety structures able to autonomously detect and mitigate quantum-based threats. Further, the combination of blockchain and quantum cryptography ought to result in the introduction of quantum-resistant blockchains, thereby destiny-proofing these structures in opposition to capacity quantum assaults.

DOI: 10.48175/IJARSCT-17591

3.3 Research demanding situations and possibilities for advancing quantum cryptography:

Advancing quantum cryptography presents a completely unique set of research challenges and opportunities, underscoring the interdisciplinary nature of the sphere and the need for ongoing collaboration and improvement.

One of the primary research-demanding situations in quantum cryptography is the need for practical and scalable quantum technology. Even as quantum cryptography promises extraordinary safety, its real-world implementation is frequently hindered by technological constraints. For instance, maintaining the coherence of quantum states over lengthy distances remains a good assignment. Overcoming these technological hurdles would require concerted efforts in quantum physics, engineering, and computer technology.

Another venture lies in the integration of quantum cryptography with existing protection infrastructures. Given the pervasive use of classical cryptographic structures, an easy transition towards quantum-resistant cryptographic structures is critical. This necessitates studies into hybrid cryptographic systems that could perform securely in both classical and quantum regimes.

The sphere of quantum cryptography also offers several research possibilities. As an instance, the improvement of post-quantum cryptographic algorithms, which can be proof against quantum assaults, is an energetic region of study. Those algorithms could ensure the security of digital communications in a future where quantum computer systems are not unusual.

The interdisciplinary nature of quantum cryptography gives possibilities for collaboration among unique fields. The development and implementation of quantum cryptographic structures require knowledge of quantum mechanics, laptop technology, data science, and engineering. Therefore, fostering interdisciplinary collaboration could boost improvements in this area.

IV. QUANTUM CRYPTOGRAPHY IN IMPORTANT INFRASTRUCTURE

Providing cybersecurity sources to CIs is a crucial mission because their constituting factors are interconnected among them and with other CI industries, implying that a weak point in any point of the network could produce a cascading impact that could bring about massive economic, social, and human value, as we've defined inside Section II. An adversary relying entirely on novel cryptographic methods poses demanding situations because of instances wherein cryptographic protocols have been determined to be insecure years after their notion. This is partially because cryptography relies on mathematical assumptions, approximately hassle hardness, and an area of evolving technological know-how. percent security proofs are especially tricky due to uncertainties surrounding the class of issues solvable via quantum computers and their relationship to different complexity classes. Even with formal proofs of hardness, real protocol implementations may not guarantee safety. As a result, many nations are exploring numerous opportunities based totally on their own analyses and hobbies, as opposed to relying completely on tips from entities like NIST.

In the context of essential infrastructure (CI), cybersecurity is crucial given the interconnected nature of CI factors, in which a weak point in any part of the network could result in cascading consequences with sizeable financial, social, and human costs. percent solutions are important for CI networks, but the project lies in making sure stringent communications necessities with low computational assets and legacy gadgets, even as well as checking out proposed solutions in actual environments.

A super-PC set of rules for CI implementation must offer low computational time to satisfy latency constraints; that's vital for operational generation (OT) structures in which controlling operations require millisecond-level latencies. But comparing percent protocols based totally solely on latency facts is hard because of variations in testing conditions and implementation contexts. At the same time that high-level comparisons can be made using metrics like key and ciphertext lengths and computational prices, there may be a need for fair comparative metrics specially tailored to industrial and important infrastructure networks.

Integrating PCs into CI infrastructure calls for resilience answers able to adapt to special cryptography algorithms, considering uncertainties concerning their security in opposition to quantum assaults and varying cybersecurity necessities across nations and OT environments. The ongoing proliferation of percent standardization strategies globally underscores the need for bendy p.c. solutions to house numerous regulatory frameworks and cybersecurity demands.

DOI: 10.48175/IJARSCT-17591

Modern-day PC algorithms typically recognize the importance of achieving quantum security for confidentiality, integrity, and authenticity, ordinarily from an information technology (IT) perspective. but, for implementation in OT networks, they ought to also ensure excessive availability and adaptability. As such, it's vital to assess how existing p.c. algorithms carry out in OT environments and whether or not they meet all CI requirements or if new protocols need to be developed. This may necessitate exploring opportunity households or protocols that better match the demands of CI environments

TABLE I: Global distribution of the public investment in quantum technologies in 2023 and in 2022 . The total investment was around 27 billion euros in 2022 and increased a 33% in 2023, to 36 billion euros.

Country	Quantum Public Spend 2023 (Million e)	(Million $)	Quantum Public Spend 2022 (Million e)
China	13 500 (+0%)	15 000	13 500
UK	3 600 (+200%)	4 300	1 200
USA	3 000 (+172.73%)	3 750	1 100
Germany	3 000 (+13.33%)	3 300	2 600
South Korea	2 000 (+56143%)	2 350	35
France	1 800 (+0%)	2 200	1 800
Russia	1 250 (+119.3%)	1 450	570
Europe	1 000 (+0%)	1 100	1 000
Canada	1 000 (+0%)	1 100	1 000
India	630 (−30%)	735	900
Japan	600 (+0%)	700	600
Others	4 620 (+71.1%)	5 100	2 700
Total	36 000 (+33%)	40 000	27 000

V. CONCLUSION

The advent of quantum technology, especially quantum internet and quantum cryptography, has ushered in a new technology of communication and statistical security. The capability of the quantum internet to revolutionize international verbal exchange is substantial, offering exceptional levels of protection and velocity. The combination of quantum cryptography with emerging technology, inclusive of blockchain and IoT, has unfolded new avenues for cozy data transmission and storage. Those improvements have not only strengthened the robustness of cryptographic systems, but they have additionally paved the way for the improvement of quantum-resistant blockchains, offering better safety against cyber threats.

Reflecting on the present-day nation of quantum cryptography, it's far obvious that we're on the cusp of a good-sized technological transformation. The fast development of quantum computation and the impending awareness of quantum supremacy pose demanding situations and opportunities for the field of cryptography. Even as the emergence of quantum computers has created new demanding situations for existing security algorithms, it has also spurred the improvement of extra-efficient quantum repeater networks, improved security proofs for non-stop variable quantum key distribution, and the development of quantum-resistant cryptographic algorithms.

Looking ahead, the future prospects of quantum cryptography are promising. The integration of neural network-based AI in cryptography holds huge implications for future virtual protection paradigms. but knowing the entire ability of those technologies calls for perseverance in research and improvement. It's imperative for researchers, technologists, and policymakers to collaborate and put money into advancing quantum cryptography. This may no longer only help in mitigating the 'quantum chance' but also pave the way for a more cozy and green worldwide communique network. The interdisciplinary nature of this research region, combining factors of quantum physics, PC technological know-how, and synthetic intelligence, offers great capacity benefits and possibilities. Consequentially, a call to action for persisted research and improvement within the discipline of quantum cryptography isn't always simply vital but imperative for the advancement of global communication and information security.

REFERENCES

[1]. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

[2]. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.

[3]. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661-663.

[4]. Scarani, V., Acín, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters, 92(5), 057901.

[5]. NIST Post-Quantum Cryptography Standardization Project. (2020). Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization

[6]. Mosca, M., & Stebila, D. (2019). PQCRYPTO: The NIST Post-Quantum Cryptography Standardization Process. PQCrypto 2019: 10th International Conference on Post-Quantum Cryptography, 57-67.

[7]. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-Quantum Cryptography (1st ed.). Springer.

[8]. van de Graaf, J., & Bos, J. W. (2020). Quantum-Resistant Cryptography. Springer.

[9]. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on the Theory of Computing, 212-219.

[10]. National Academies of Sciences, Engineering, and Medicine. (2019). Quantum Computing: Progress and Prospects. The National Academies Press.

DOI: 10.48175/IJARSCT-17591