International Journal of Innovation Studies

SECURE DATA TRANSMISSION TECHNIQUES IN QUANTUM COMPUTING NETWORKS

1.Vanajakshi. N. M
Assistant Professor,
Department of Electronics and Communication Engineering
Government Engineering College, Chamarajanagara,
Karnataka, India.
Pin code - 571313
E-mail: vanaja.sp@gmail.com

2.Venkatachalapathy M.V
Assistant Professor,
Department of Electronics and Communication Engineering
Government Engineering College, Chamarajanagara,
Karnataka, India.
Pin code - 571313
E-mail: mvvcpathy@gmail.com

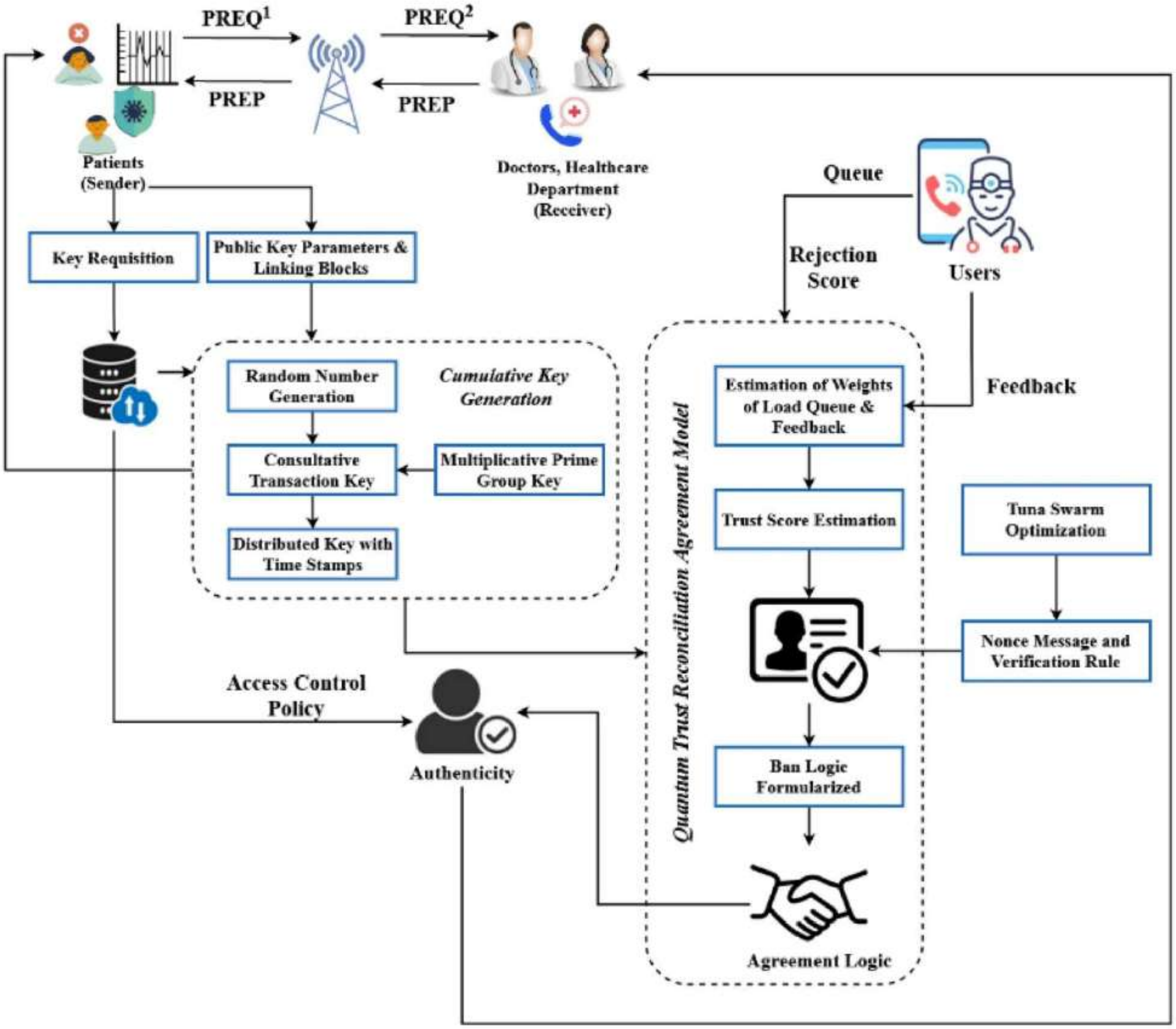

PREQ¹
PREQ²
PREP
PREP
Patients (Sender)
Doctors, Healthcare Department (Receiver)
Queue
Rejection Score
Users
Key Requisition
Public Key Parameters & Linking Blocks
Random Number Generation
Cumulative Key Generation
Consultative Transaction Key
Multiplicative Prime Group Key
Distributed Key with Time Stamps
Quantum Trust Reconciliation Agreement Model
Estimation of Weights of Load Queue & Feedback
Feedback
Trust Score Estimation
Tuna Swarm Optimization
Nonce Message and Verification Rule
Access Control Policy
Authenticity
Ban Logic Formularized
Agreement Logic

Fig1. A quantum trust and consultative transaction-based blockchain cybersecurity model

Abstract: Quantum computing is set to bring about a significant change in safe data transfer by utilising the fundamental principles of quantum physics to completely modify cryptographic systems. This analytical article explores advanced methods for securely transmitting data in quantum computing networks, with a specific focus on quantum key distribution (QKD), quantum encryption, and post-quantum cryptography.

Quantum Key Distribution (QKD) is a significant breakthrough that enables two parties to generate a shared, unpredictable secret key that is exclusive to them. This key may be utilised to encode and decode communications securely. QKD, unlike traditional cryptography systems, use the properties of quantum physics, such as superposition and entanglement, to guarantee the detection of any eavesdropping attempts. This paper investigates different Quantum Key Distribution

(QKD) protocols, such as BB84 and E91, by assessing their security assumptions, implementation difficulties, and practical uses. QKD's resilience against both quantum and classical attacks establishes it as a fundamental element of forthcoming secure communication infrastructures.

Quantum encryption enhances the capacity for safe data transfer by employing quantum states to encode information, providing encryption systems that are theoretically impossible to crack. This study examines the progress made in quantum encryption methods, such as quantum bit commitment and quantum oblivious transmission, and emphasises their significance in improving privacy and security in quantum networks. An analysis is conducted on the incorporation of quantum encryption into current communication protocols, with a focus on the advantageous collaboration and technical challenges.

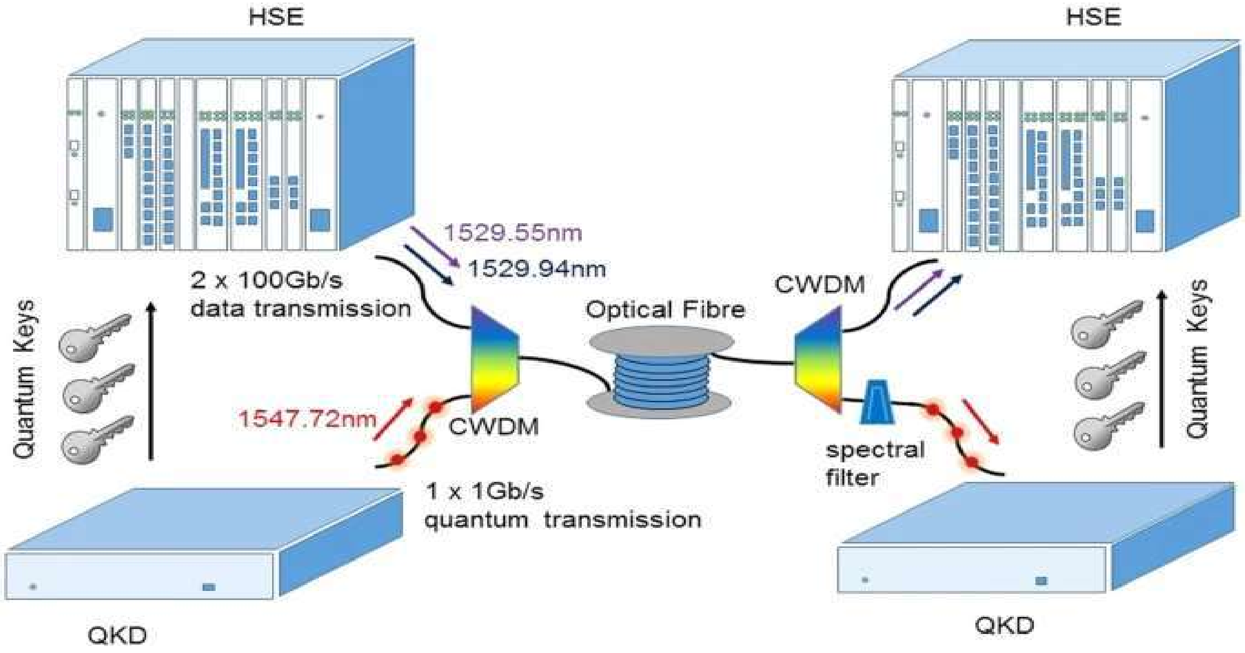


Fig2. Quantum secured system for ultra-high data bandwidth encryption

The study not only discusses quantum-specific approaches but also emphasises the increasing significance of post-quantum cryptography (PQC). As quantum computers advance, they present substantial risks to traditional cryptography systems, requiring the creation of algorithms that can endure quantum assaults. This section presents a comprehensive analysis of the top contenders in the field of Post-Quantum Cryptography (PQC), including lattice-based, hash-based, code-based, and multivariate polynomial cryptosystems. It evaluates their level of security, efficiency, and appropriateness for different applications. The discussion also covers the contribution of standardisation agencies such as NIST in promoting the research and implementation of Post-Quantum Cryptography (PQC).

Moreover, the research investigates the incorporation of conventional and quantum cryptography techniques to enhance security in hybrid quantum-classical networks. Integration is essential to provide a smooth shift to quantum-secure communications, enabling the progressive adoption of quantum technology alongside current infrastructures. This text thoroughly examines the difficulties associated with interoperability, scalability, and security maintenance throughout this shift.

This paper offers a thorough analysis of current research and technical breakthroughs to gain a full grasp of the difficulties and possibilities in developing safe and scalable quantum communications. The results of our research emphasise the crucial importance of using algorithms that are resistant to quantum computing, and the continuous requirement for new ideas and advancements to protect the integrity and privacy of data in the age of quantum technology. The study finishes by highlighting the need of multidisciplinary collaboration in addressing the complex issues associated with secure data transmission in quantum computing networks, and suggests future avenues for research. The continuous advancement of quantum technology offers exceptional prospects and notable obstacles, highlighting the necessity for constant research and development in this rapidly changing domain.

Keywords: Quantum Computing, Secure Data Transmission, Quantum Key Distribution (QKD), Quantum Encryption, Post-Quantum Cryptography (PQC), Quantum Bit Commitment, Quantum Oblivious Transfer, Lattice-Based Cryptography, Hash-Based Cryptography, Code-Based Cryptography.

1. Introduction

Quantum computing has attracted considerable interest for its ability to address intricate issues that are now unsolvable for traditional computers (1). Quantum computers have the potential to profoundly transform several industries, such as encryption and secure communications. Conventional cryptography techniques, which depend on the computational complexity of certain mathematical problems, are facing growing challenges from the capabilities of quantum computers (2). This requires the creation of novel methods for secure data transfer that utilise the distinct laws of quantum physics.

Quantum computing has attracted considerable interest for its ability to address intricate issues that are now unsolvable for traditional computers (3). Quantum computers have the potential to profoundly transform several industries, such as encryption and secure communications (4). Conventional cryptography techniques, which depend on the computational complexity of certain mathematical problems, are facing growing challenges from the capabilities of quantum computers (5). This requires the creation of novel methods for secure data transfer that utilise the distinct laws of quantum physics.

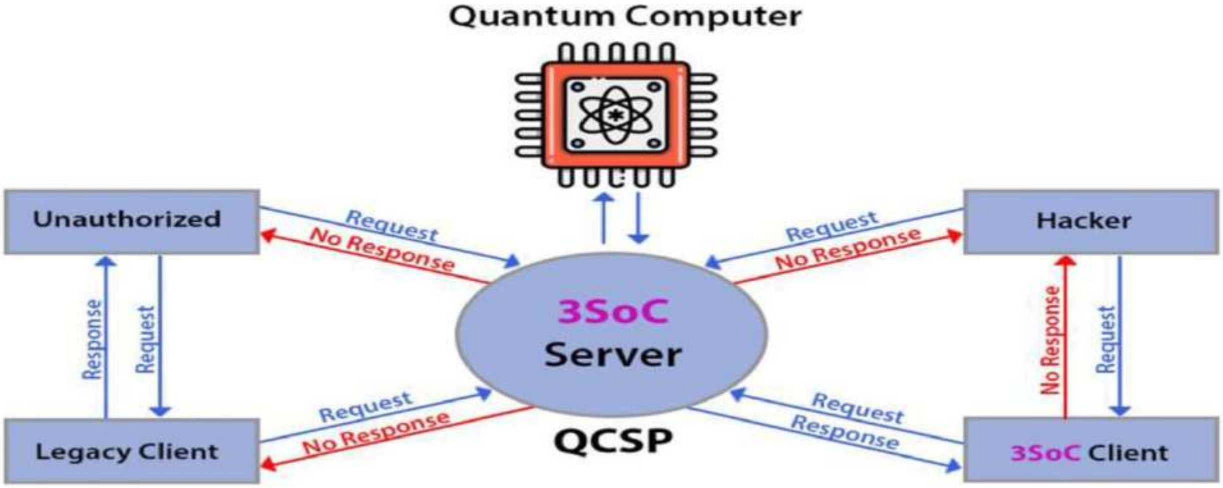


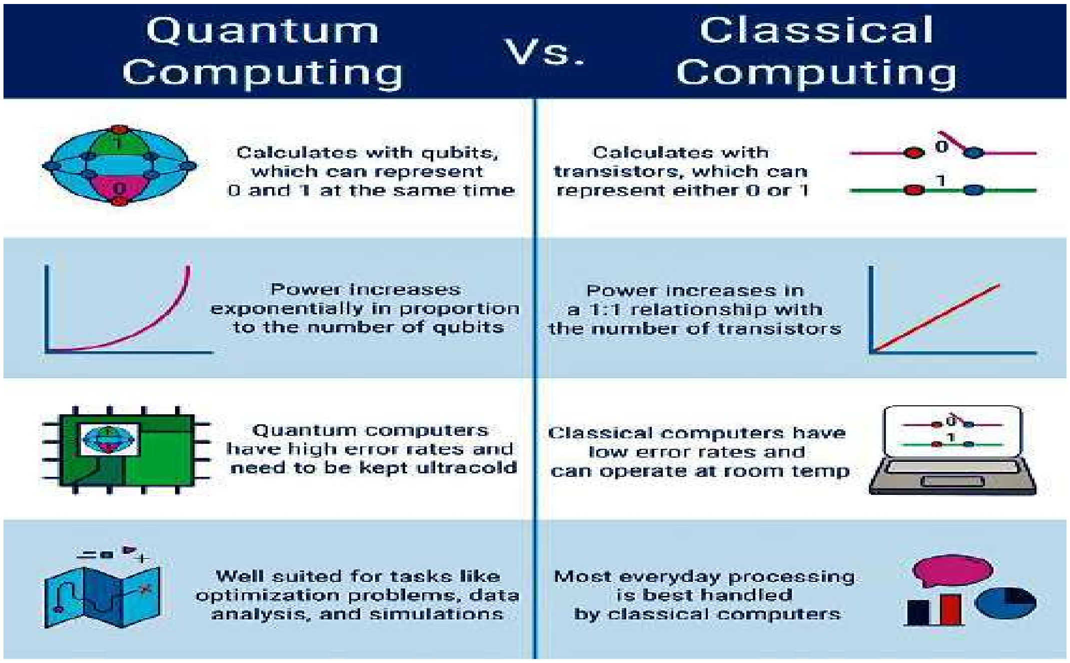
Fig 3. Quantum computer service provider (QCSP) providing quantum computing via 3SoC Intranet to subscribers.

Quantum computing has attracted considerable interest for its ability to address intricate issues that are now unsolvable for traditional computers (6). Quantum computers have the potential to profoundly transform several industries, such as encryption and secure communications (7). Conventional cryptography techniques, which depend on the computational complexity of certain mathematical problems, are facing growing challenges from the capabilities of quantum computers (8). This requires the creation of novel methods for secure data transfer that utilise the distinct laws of quantum physics.

Quantum Key Distribution (QKD) is a remarkable breakthrough in the field of secure communications. Quantum Key Distribution (QKD) utilises the fundamental concepts of quantum physics, such as superposition and entanglement, to allow two parties to create a mutually shared and confidential key (9). QKD, unlike conventional key distribution methods, guarantees the detection of any eavesdropping attempt, hence offering a degree of security that cannot be achieved with standard cryptographic approaches (10). The BB84 protocol, devised by Charles Bennett and Gilles Brassard in 1984, is among the oldest and most thoroughly examined quantum key distribution (QKD) techniques (11). The binary information is encoded using the polarisation states of photons, which guarantees that any attempt to intercept the information will disrupt the quantum states and expose the existence of an eavesdropper. In a similar vein, the E91 protocol, introduced by Artur Ekert in 1991, employs entangled particle pairs to provide safe key distribution, therefore bolstering the resilience of QKD against possible security vulnerabilities.

There has been substantial advancement in the actual use of Quantum Key Distribution (QKD) throughout time. QKD has been successfully proven in experimental configurations using both fibre optic cables and free-space connections, enabling secure communication across distances greater than 100 km (12). Recent progress has also concentrated on satellite-based Quantum Key

Distribution (QKD), with projects like the Chinese Micius satellite showcasing the practicality of worldwide quantum communication networks (13). These advancements demonstrate the potential of Quantum Key Distribution (QKD) to become the fundamental basis of future secure communication networks, offering unmatched protection against both conventional and quantum threats.



Quantum Computing	Vs.	Classical Computing
Calculates with qubits, which can represent 0 and 1 at the same time		Calculates with transistors, which can represent either 0 or 1
Power increases exponentially in proportion to the number of qubits		Power increases in a 1:1 relationship with the number of transistors
Quantum computers have high error rates and need to be kept ultracold		Classical computers have low error rates and can operate at room temp
Well suited for tasks like optimization problems, data analysis, and simulations		Most everyday processing is best handled by classical computers

Fig 4. Difference between Quantum Computing and Classical Computing

In addition to quantum key distribution (QKD), quantum encryption methods provide other opportunities for improving data security. Quantum encryption is the process of encrypting information using quantum states, which offers a potentially invulnerable encryption method (14). Researchers are now investigating methods like quantum bit commitment and quantum oblivious transfer to enhance the confidentiality and protection of quantum networks (15). Quantum bit commitment enables a party to conceal a value from another party while committing to it, and subsequently disclose the value at a later time (16). This approach is essential for a range of cryptographic protocols, such as safe multi-party computing and zero-knowledge proofs. Quantum oblivious transfer allows a sender to transmit one specific message out of a set of many messages to a receiver (17). It guarantees that the receiver will only get the chosen message and will not gain any knowledge about the other messages. These techniques leverage the characteristics of quantum states to provide encryption systems that are inherently resistant to both classical and quantum assaults.

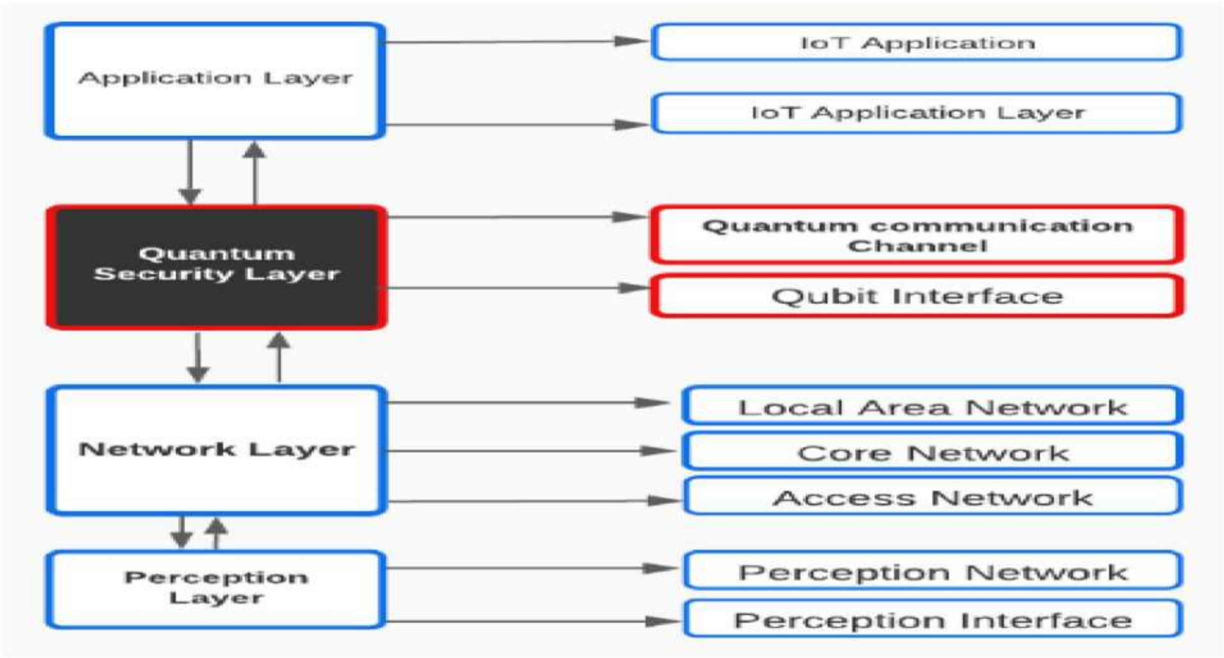


Fig 5. Proposed network architecture abstract diagram.

With the ongoing progress of quantum computing, the risk it presents to traditional cryptography methods becomes increasingly evident. Shor's technique has the capability to factorise big integers in an efficient manner, which results in the cracking of commonly used public-key cryptosystems such as RSA (18). This has generated considerable interest in post-quantum cryptography (PQC), which aims to create cryptographic algorithms that are resistant to quantum assaults. Currently, researchers are investigating many methods for Post-Quantum Cryptography (PQC), including as lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate polynomial cryptosystems (19. Lattice-based encryption focuses on the difficulty of solving lattice problems, which are thought to be impervious to both conventional and quantum assaults (20). Hash-based cryptography use hash functions to create safe digital signatures, whereas code-based cryptography utilises error-correcting codes for the purpose of encryption and decryption. Conversely, multivariate polynomial cryptosystems require solving sets of multivariate polynomial equations, a task that remains challenging even for quantum computers (21). These algorithms are designed to offer security assurances that remain unaffected even when faced with quantum computational capabilities, thereby assuring the ongoing safeguarding of sensitive information in a post-quantum era.

In order to achieve quantum-secure communications, it is necessary to use a hybrid strategy that combines classical and quantum cryptography techniques. Employing this hybrid approach is crucial to guarantee compatibility and interoperability between current infrastructures and forthcoming quantum technology. The problems related to this integration are ensuring security throughout the shift, attaining scalability, and resolving interoperability concerns. Hybrid quantum-classical networks seek to merge the advantages of traditional cryptography systems with the security improvements provided by quantum technology. This strategy enables a step-by-step adoption of quantum secure communication techniques, guaranteeing a seamless transition and reducing interruptions to current systems.

Quantum Key Distribution (QKD)

2.1 Overview of QKD Principles

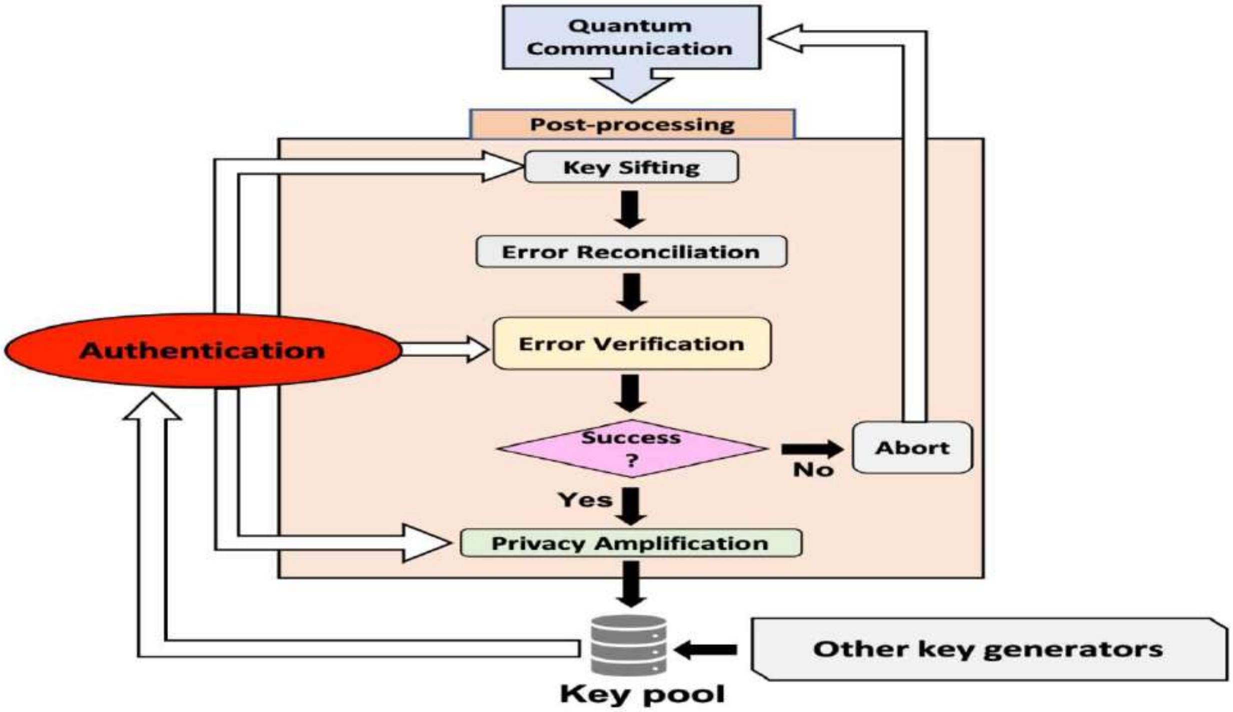


Fig 6. Schematic presentation of the main steps and the flow of data in a QKD protocol.

Quantum Key Distribution (QKD) is an innovative technique that use the principles of quantum physics to safely transmit encryption keys between two entities. QKD, in contrast to traditional key distribution methods, employs quantum bits (qubits) that may concurrently exist in various states due to the concepts of superposition and entanglement (22). This guarantees that any effort to intercept or quantify the qubits would disrupt their condition, thereby notifying the communication parties of the existence of an eavesdropper. The inherent security characteristic of QKD renders it fundamentally impervious to both classical and quantum computing assaults.

2.2 Key Protocols: BB84, E91

BB84 and E91 are two very important quantum key distribution (QKD) techniques.

- The BB84 system, created by Charles Bennett and Gilles Brassard in 1984, is the pioneering and extensively utilised Quantum Key Distribution (QKD) system (23). Photon polarisation states are utilised to encode binary data. Alice, the transmitter, delivers photons to Bob, the receiver, in one of four polarisation states: horizontal, vertical, +45 degrees, or -45 degrees. Bob use randomly selected bases to measure the polarisation states (24). Following the transmission, Alice and Bob openly compare the bases they used (not the specific measurements) and eliminate any findings where their bases do not align. The remaining data constitutes a mutually exclusive secret key (25). Alice and Bob can ensure the security of the key by detecting any flaws introduced during an eavesdropping attempt.

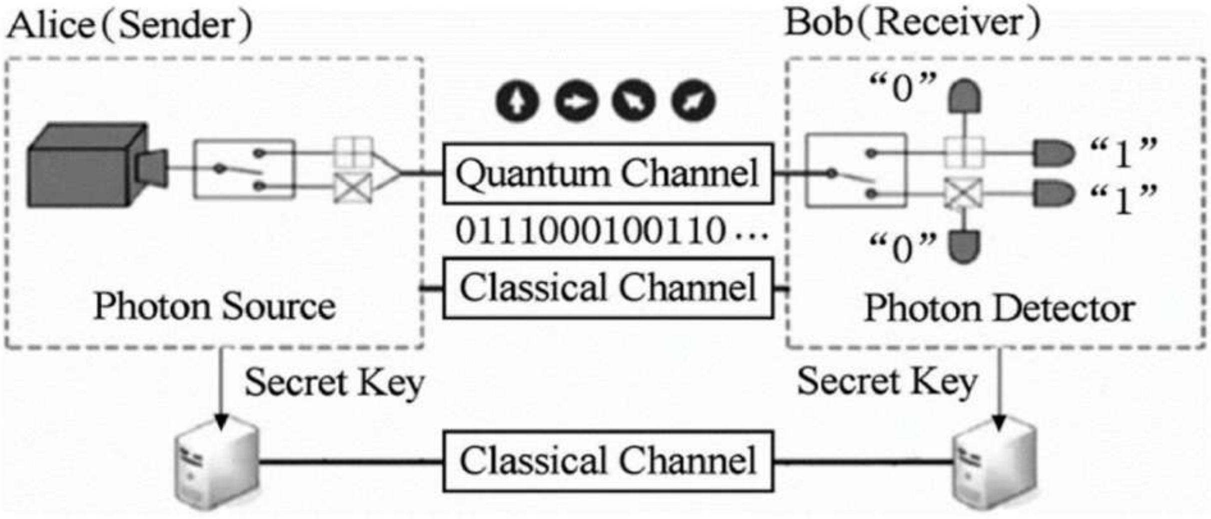


Fig 7. Quantum key distribution (QKD) based on polarization encoding.

In the BB84 protocol, the probability of detecting an eavesdropper can be quantified using the following equation:

$$\mathrm{QBER} = \frac{Ne}{N}$$

where QBER is the Quantum Bit Error Rate, Ne is the number of errors detected, and N is the total number of bits transmitted.

- The E91 protocol, proposed by Artur Ekert in 1991, utilises quantum entanglement to accomplish safe key distribution. This protocol involves the generation of entangled photon pairs by a source, where one photon is sent to Alice and the other to Bob. Alice and Bob's measurement of their photons using randomly selected polarisation bases yields fully correlated findings as a result of the entanglement (26). By doing a comparative analysis of a selection of their data, they are able to identify any efforts of eavesdropping, as any external interference would disrupt the entanglement and create inaccuracies. The remaining associated metrics are utilised to construct the secure key.

The security of the E91 protocol is based on the violation of Bell's inequality, which can be expressed as:

$$S=|E(a,b)+E(a,b')+E(a',b)-E(a',b')|\leq 2$$

where E(a,b)E(a, b)E(a,b) represents the correlation function of measurements along different axes aaa and bbb. If SSS exceeds 2, it indicates the presence of quantum entanglement, thereby ensuring the security of the key distribution.

2.3 Implementation Challenges and Solutions

Implementing QKD in practical systems poses several challenges:

- Photon Loss and Noise: When transmitting across long distances, whether by fibre optics or free space, there is a decrease in the number of photons and an increase in unwanted signals, known as noise (27). These factors can negatively impact the performance of the Quantum Key Distribution (QKD) system. Possible solutions involve the utilisation of very sensitive single-photon detectors and the application of error correction and privacy amplification techniques to address and reduce these problems.

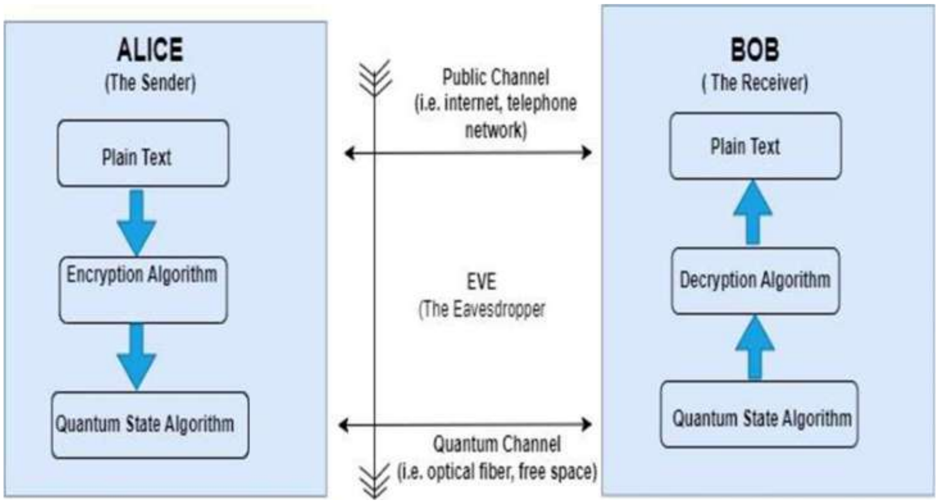


Fig8. Basic Block Diagram of QKD System

- Quantum Channel Security: Safeguarding the integrity of the quantum channel against potential threats, such as photon number splitting (PNS) assaults, necessitates the implementation of sophisticated procedures and enhancements in hardware (28). Decoy state protocols can enhance protection against PNS attacks by introducing supplementary states that expose the existence of an eavesdropper.

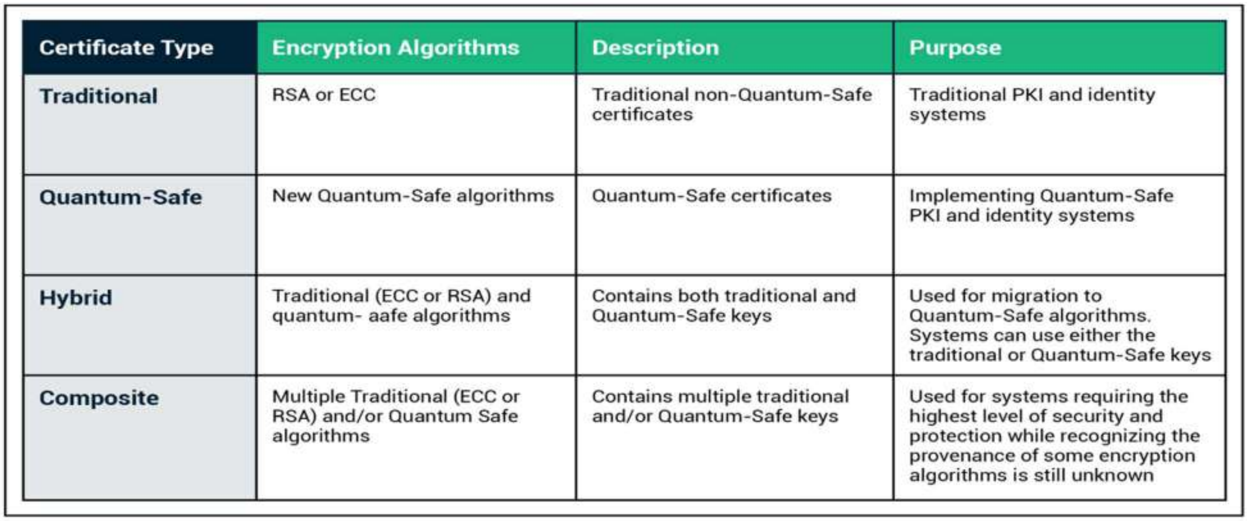
- Integration with Classical Networks: The process of combining QKD systems with current classical communication infrastructure necessitates thoughtful examination of compatibility and interoperability. Integrating conventional and quantum cryptography approaches can be facilitated by developing hybrid systems.

- Cost and Scalability: The exorbitant expense of QKD equipment and the difficulty of expanding the technology for broad adoption are major obstacles. Technological advancements, such the creation of integrated photonic circuits for quantum key distribution (QKD), are anticipated to lower expenses and enhance scalability.

3. Quantum Encryption Techniques

3.1 Introduction to Quantum Encryption

Quantum encryption refers to a variety of methods that utilise the principles of quantum physics to ensure the security of data. Quantum encryption differs from classical encryption by utilising the intrinsic characteristics of quantum states, such as superposition and entanglement, to guarantee the secrecy and integrity of information, rather than relying on mathematical techniques and processing complexity (29). Quantum encryption is theoretically impervious to the weaknesses that pose a danger to classical cryptographic systems, particularly in light of the emergence of potent quantum computers that can crack conventional encryption methods.



Certificate Type	Encryption Algorithms	Description	Purpose
Traditional	RSA or ECC	Traditional non-Quantum-Safe certificates	Traditional PKI and identity systems
Quantum-Safe	New Quantum-Safe algorithms	Quantum-Safe certificates	Implementing Quantum-Safe PKI and identity systems
Hybrid	Traditional (ECC or RSA) and quantum- aafe algorithms	Contains both traditional and Quantum-Safe keys	Used for migration to Quantum-Safe algorithms. Systems can use either the traditional or Quantum-Safe keys
Composite	Multiple Traditional (ECC or RSA) and/or Quantum Safe algorithms	Contains multiple traditional and/or Quantum-Safe keys	Used for systems requiring the highest level of security and protection while recognizing the provenance of some encryption algorithms is still unknown

Fig 9. Quantum safe Certificates

3.2 Quantum Bit Commitment

Quantum bit commitment is a cryptographic technique wherein a party, known as the committer, can select a bit (either 0 or 1) and commit to it in a manner that conceals the value from the other party, referred to as the receiver, until the committer chooses to disclose it. This procedure consists of two primary stages: the commitment phase and the revelation phase.

- **Commitment step:** During this step, the individual responsible for committing encodes the selected bit into a quantum state and transmits this state to the recipient. The quantum state is constructed in a manner that renders the receiver unable to ascertain the value of the bit without assistance from the committer (30). For example, the person responsible for the action could utilise quantum superposition or entanglement to make the bit unclear or difficult to understand.

- **Reveal Phase:** During this phase, the committer shares the required information with the receiver, enabling them to decode the quantum state and confirm the value of the bit. If the person who made the commitment attempts to alter the information after the commitment phase, the rules of quantum mechanics guarantee that the receiver will be able to detect any such effort.

Quantum bit commitment plays a vital role in several cryptographic protocols, such as safe multi-party computing and zero-knowledge proofs. Implementing safe quantum bit commitment protocols is a complex task, since they need to be resistant to quantum assaults and prevent the committer from tampering with the bit after the commitment phase.

The security of quantum bit commitment can be quantified using the following equation:

$$H(B|A)=0$$

where $H(B|A)$ is the conditional entropy of bit B given A, indicating that the bit commitment scheme is perfectly binding and hiding.

3.3 Quantum Oblivious Transfer

Quantum oblivious transfer (QOT) is a protocol that enables a sender to transmit a specific piece of information to a receiver, while ensuring that the receiver gains knowledge just about the selected piece and remains ignorant about the other options (31). Simultaneously, the sender remains unaware of whatever specific piece of information was transmitted.

During a typical Quantum One-Time (QOT) protocol, the transmitter generates a collection of quantum states that represent various bits of information and transmits them to the receiver. The recipient thereafter selects the specific quantum states to get information by conducting measurements in a certain basis. As a result of the principles of quantum physics, the act of measuring guarantees that the recipient can only get information about the chosen piece, while the other parts remain unmeasured and unknown.

Quantum oblivious transmission serves as a crucial component for more intricate cryptographic operations, including secure multi-party computing and private information retrieval. It offers a strong and reliable method for securely exchanging data in situations when both parties desire to maintain the confidentiality of specific information.

The success probability of quantum oblivious transfer can be expressed as:

$$\mathrm{P(success)} = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right)$$

3.4 Comparative Analysis using Classical Encryption Methods

Quantum encryption approaches provide several benefits compared to classical encryption methods, principally attributable to the distinctive characteristics of quantum mechanics:

- Enhanced Security Assurances: Quantum encryption offers superior security assurances in comparison to traditional techniques. The fundamental tenets of quantum physics, such as the no-cloning theorem and the uncertainty principle, guarantee that any endeavour to intercept a quantum communication channel may be identified (32). Unlike classical encryption, which depends on the presumed complexity of certain mathematical problems that may potentially be solved by future advancements in computing, particularly with the use of quantum computers, this approach is different.

- Key Distribution: Quantum Key Distribution (QKD) facilitates the safe creation and exchange of encryption keys among many parties. QKD, unlike traditional key distribution systems, guarantees that any effort to intercept the communication would result in identifiable mistakes, enabling the parties involved to take necessary actions. Conversely, traditional ways of distributing keys are susceptible to interception and need supplementary security measures to safeguard the keys.

- Enhanced Security in the Long Run: Quantum encryption techniques are specifically designed to provide robust protection against potential future developments in technology, such as the emergence of quantum computers (33). On the other hand, several traditional encryption techniques, such as RSA and ECC, may be easily exploited by quantum computers using algorithms like Shor's algorithm. This algorithm is capable of rapidly breaking down big numbers and solving discrete logarithm issues.

The efficiency of quantum encryption can be evaluated using the following equation for the quantum bit error rate (QBER):

$$\text{QBER} = \frac{Ne}{Nt}$$

where N_e is the number of erroneous bits, and N_t is the total number of transmitted bits.

- Complexity and Implementation: Quantum encryption, while its enhanced security, poses substantial difficulties in terms of intricacy and execution. Quantum systems need advanced apparatus, such as single-photon generators and detectors, and are susceptible to ambient influences like as noise and photon loss (34). On the other hand, classical encryption methods are firmly established, simpler to execute, and now more feasible for wider use.

To summarise, quantum encryption techniques are a major breakthrough in cryptography, providing unmatched security by leveraging the distinct characteristics of quantum physics. Despite the difficulties in implementing and scaling them, continuous research and technical progress are increasingly resolving these obstacles, therefore enabling the development of secure quantum communication networks in the future.

4. PQC: Post-Quantum Cryptography

4.1 Importance of PQC in the Quantum Era

The emergence of quantum computing presents a substantial menace to existing encryption methods. Algorithms such as Shor's method have the ability to factor big numbers and handle discrete logarithm issues in an efficient manner. These challenges are the foundation of the security for commonly used public-key cryptosystems like RSA and Elliptic Curve Cryptography (ECC) (35). As quantum computers progress, these encryption techniques will become susceptible to assaults, jeopardising the security of digital communications and data. Post-Quantum Cryptography (PQC) seeks to create cryptographic algorithms that can withstand assaults from both conventional and quantum computers, therefore guaranteeing the security of information in the long run throughout the quantum era.

4.2 Overview of PQC Algorithms

4.2.1 Lattice-Based Cryptography

Lattice-based encryption is predicated on the difficulty of solving lattice problems, namely the Learning With Errors (LWE) issue and the Shortest Vector issue (SVP). These challenges are thought to be immune to assaults from quantum computers. Lattice-based schemes have several benefits, including as robust security assurances, streamlined implementations, and the ability to handle sophisticated cryptographic features like completely homomorphic encryption. Some noteworthy cryptographic algorithms that are based on lattices include:

- NTRUEncrypt: A cryptographic algorithm that uses the difficulty of solving specific mathematical issues involving lattices to provide secure public-key encryption. It is renowned for its high level of effectiveness and ability to withstand quantum assaults.

- Kyber: is a key encapsulation mechanism (KEM) included in the NIST PQC standardisation process. It is used for secure key exchange.

The security of lattice-based cryptography can be expressed using the following equation:

Security Level=$\log_2$ (Volume of the Lattice)−Dimensionality of the Lattice

4.2.2 Hash-Based Cryptography

Hash-based cryptography employs cryptographic hash functions to create safe digital signatures. These techniques are deemed secure against quantum assaults because to their reliance on the collision resistance of hash functions, which stays unaffected even in the presence of quantum computers. Notable instances include:

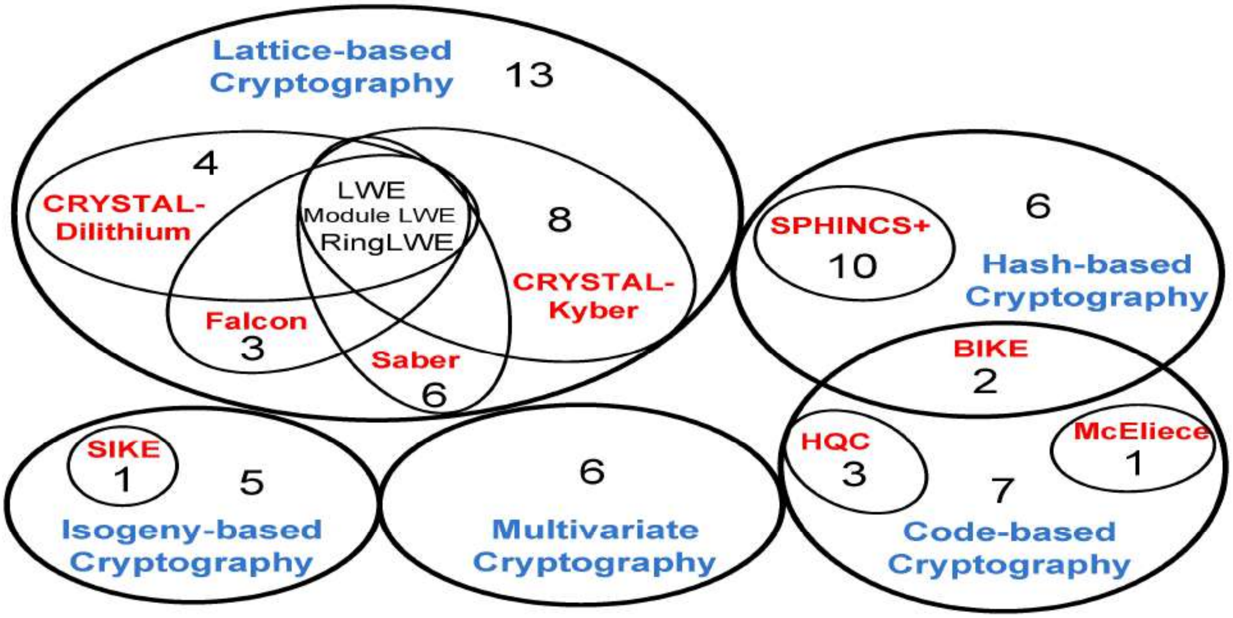


Fig 10. The Venn diagram describes the fields of PQC research related to the references.

The Merkle Signature Scheme (MSS): A cryptographic technique that enables the creation of secure digital signatures by utilising hash trees, also known as Merkle trees. While it offers robust security, it necessitates the administration of extensive key pairs.

XMSS (eXtended Merkle Signature Scheme): An enhanced version of the MSS that provides forward security and improved performance, making it well-suited for practical use.

The security of hash-based cryptography is often evaluated using the pre-image resistance property, expressed as:

$$\mathbf{H(x) \neq H(x')}$$

where H is the hash function, and x and x′ are different inputs.

4.2.3 Code-Based Cryptography

Code-based encryption utilises the difficulty of deciphering random linear codes, a challenge that is thought to be impervious to both classical and quantum assaults. The most widely recognised cryptographic scheme based on code is:

The McEliece Cryptosystem: It a cryptographic algorithm that relies on the complexity of decoding generic linear codes. It offers robust security, however it is limited by the need for high key sizes.

The security of code-based cryptography can be quantified using the following equation:

$$\mathbf{P(success)=1-2^{-(n-k)}}$$

where n is the length of the code and k is the dimension of the code.

4.2.4 Multivariate Polynomial Cryptosystems

Multivariate polynomial cryptosystems are based on the computational challenge of solving systems of multivariate quadratic equations, which is a challenging task for both conventional and quantum computers. Prominent strategies in this classification encompass:

The Rainbow signature scheme is a multivariate quadratic public-key signature technique that is well-known for its efficiency and very modest signature sizes.

- HFE (Hidden Field Equations): The system is a cryptographic method that uses multivariate polynomials over finite fields to generate public and private keys. It provides high-level security but has difficulties with the size of the keys and the complexity of the process.

4.3 Security Analysis and Efficiency

The primary objective of PQC algorithms is to offer strong protection against quantum assaults while still ensuring practical efficiency. Security study entails assessing the resilience of these algorithms against several forms of assaults, encompassing both conventional and quantum opponents (36). Efficiency is quantified by evaluating the utilisation of processing resources, the dimensions of critical sizes, and the extent of communication overhead.

- Security: PQC algorithms are specifically intended to be resistant to the computational power of quantum computers. Lattice-based techniques, for instance, are based on issues that are conjectured to be challenging even for quantum algorithms (37). Hash-based techniques rely on well-studied hash functions, assuring their resilience.

- Efficiency: While certain PQC algorithms, including lattice-based and hash-based cryptography, offer adequate efficiency, others, such as code-based cryptography, may encounter issues owing to huge key sizes (38). Current research is dedicated to enhancing these algorithms to increase their feasibility for real-world implementations.

The efficiency of PQC algorithms can be evaluated using the following equation for computational complexity:

$$\mathbf{T(n)=O(n^c)}$$

where T(n) is the time complexity, n is the input size, and c is a constant.

5. Hybrid Quantum-Classical Cryptographic Methods

5.1 Need for Hybrid Approaches

Traditional cryptography approaches face a substantial challenge with the emergence of quantum computing. Classical cryptography, which has been the foundation of data security for many years, mainly depends on mathematical problems that are currently not possible for classical computers to answer efficiently (39). Quantum computers pose a significant danger to cryptography systems due to their capacity to execute intricate computations at unparalleled velocities (40). Algorithms such as RSA, ECC, and some types of symmetric encryption are susceptible to compromise. Given the circumstances, it becomes clear that there is a requirement for hybrid cryptographic approaches. Hybrid cryptographic approaches combine the advantages of conventional and quantum encryption, providing a temporary solution during this crucial moment. Quantum cryptography, particularly quantum key distribution (QKD), offers an impregnable security measure rooted on the laws of quantum physics (41). Quantum Key Distribution (QKD) enables the safe transmission of encryption keys by detecting any unauthorised interception or tampering with the key. The intrinsic security advantage of quantum cryptography makes it a compelling complement to traditional cryptographic systems (42). Due to the limited availability and ongoing development of quantum computer technologies, a full shift to quantum cryptography is not currently possible in the near future. Integrating quantum cryptography techniques with current classical methods provides a strong and temporary solution that improves security without requiring an immediate and complete transition to quantum-only systems. This hybrid solution tackles the weaknesses of traditional systems by using the latest developments in quantum cryptography to enhance data security against potential quantum attacks.

5.2 Integration Strategies for Classical and Quantum Cryptographic Systems

The fusion of conventional and quantum cryptography systems entails a multifaceted strategy that amalgamates the most advantageous characteristics of both technologies to attain heightened security (43). An essential approach to integration is the utilisation of quantum key distribution (QKD) in conjunction with traditional encryption techniques. Quantum Key Distribution (QKD) facilitates the secure creation and transfer of cryptographic keys, which may then be employed in conventional encryption methods to safeguard data. This combination guarantees that even in the event of data interception, the encryption keys will remain protected, therefore preserving the total integrity of the encrypted information (44). Furthermore, the hybrid architecture relies heavily on the implementation of post-quantum cryptography (PQC). Post-Quantum Cryptography (PQC) entails the creation of cryptographic algorithms that possess the ability to withstand attacks from quantum computers. The algorithms mentioned, such as lattice-based, hash-based, code-based, and multivariate polynomial-based cryptographic approaches, are specifically designed to be used in current classical cryptographic systems (45). By incorporating Post-Quantum Cryptography (PQC) algorithms into their present systems, organisations may proactively safeguard against potential quantum attacks in the future, all while ensuring compatibility with their existing infrastructure. Hybrid cryptography systems are utilised in many domains for practical applications. In the financial industry, where ensuring the security of data is of utmost importance, hybrid systems can offer an elevated level of safeguarding for important transactions and communications (46). Similarly, in the field of healthcare, hybrid cryptographic techniques may guarantee the privacy and accuracy of patient records and medical data. Hybrid systems can provide government agencies with advantages by safeguarding secret information and communications from potential risks (47). These implementations demonstrate the practicality and efficiency of hybrid cryptographic systems in real-world applications, offering a model for further use in other sectors.

The security of hybrid systems can be represented as:

$$\mathbf{H=Q\times C}$$

where H is the overall security, Q is the security provided by the quantum system, and C is the security provided by the classical system.

5.3 Challenges of Interoperability and Scalability

Although hybrid cryptographic systems provide enormous potential benefits, their implementation encounters notable hurdles, notably in terms of interoperability and scalability. Interoperability is essential for the smooth integration of quantum and conventional cryptography systems (48). This requires overcoming several technological challenges, including disparities in fundamental concepts, protocols, and operational needs between classical and quantum systems. To achieve smooth integration, it is necessary to provide standardised protocols and interfaces that enable effective communication between conventional and quantum components. Furthermore, it is crucial to resolve software and hardware compatibility concerns in order to provide seamless interactions between established conventional systems and developing quantum technology (49). Scalability is a significant issue, particularly when using hybrid cryptographic techniques in extensive settings. Quantum cryptography techniques, like QKD, sometimes need specialised hardware and infrastructure, which may be costly and difficult to expand. Efficient optimisation of quantum infrastructure, such as quantum repeaters and secure communication channels, is necessary to facilitate the operation of extensive networks and handle substantial data loads. Moreover, it is essential to assess the performance of hybrid systems to verify their ability to meet the requirements of extensive operations while maintaining both security and efficiency. Standardisation and interoperability are crucial for the effective deployment of hybrid cryptographic systems. Establishing industry standards for hybrid cryptographic approaches can facilitate widespread acceptance and guarantee seamless interoperability between diverse systems (50). Establishing standards and driving innovation in hybrid cryptographic technology requires collaboration among academics, business, and government organisations. The full potential of hybrid cryptographic systems may be realised by resolving concerns around standardisation, compatibility, and interoperability. Future endeavours should prioritise the creation of remedies for these obstacles, investigating inventive methods to improve the compatibility and expandability of hybrid system (51). Hybrid cryptographic approaches can offer strong and scalable security solutions in the quantum age, protecting data and communications from existing and potential threats.

6. Conclusion

6.1 Summary of Key Findings

This research has explored the dynamic topic of safe data transmission in quantum computing networks, emphasising the essential requirement for hybrid cryptographic techniques. Classical cryptography systems, albeit resistant to present computational threats, are susceptible to the enhanced capabilities of quantum computers. The incorporation of quantum cryptography techniques, namely quantum key distribution (QKD), with conventional encryption methods provides a robust defence mechanism. This hybrid strategy guarantees improved security by using the advantages of both platforms. Furthermore, the significance of post-quantum cryptography (PQC) in anticipating forthcoming quantum risks was emphasised, highlighting its capacity to strengthen current cryptographic systems. The practical applications in many industries provide additional evidence of the feasibility and efficiency of these hybrid systems.

6.2 The Importance of Continued Innovation in Quantum Cryptography

Sustained advancement in quantum cryptography is crucial for maintaining a competitive edge against the increasing risks presented by quantum computing. With the progress of quantum technology, it is imperative that our cryptography systems adapt to effectively address the emerging problems. Research and development should prioritise the improvement of quantum cryptography algorithms, their integration with classical systems, and the resolution of scalability and interoperability challenges. Standardised protocols and interfaces are crucial for encouraging widespread adoption and guaranteeing smooth integration. Moreover, the cooperation of academia, business, and governmental agencies will be essential in advancing these breakthroughs, setting up strong security benchmarks, and promoting a safe technology environment.

6.3 Final Thoughts on the Future of Secure Data Transmission in Quantum Computing Networks

The effective integration of conventional and quantum cryptography algorithms is crucial for ensuring safe data transfer in quantum computing networks. This hybrid approach not only offers a strong temporary solution during the transitory phase of technology advancement but also lays the foundation for the next generation of secure data transfer systems. To fully unlock the promise of these hybrid systems, it is crucial to tackle the obstacles of interoperability, scalability, and standardisation. As we go through the challenges of this technological transition, it is crucial to prioritise continued research, innovation, and cooperation in order to protect our data and communications from existing and future dangers. Incorporating conventional and quantum encryption algorithms will guarantee our continued advantage, offering a robust and impervious system for transmitting data in the quantum era.

7. Refrences

Dyakonov, M. (2019). When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing. Ieee Spectrum, 56(3), 24-29.

Hossain, K. A. (2023). The potential and challenges of quantum technology in modern era. Scientific Research Journal, 11(6).

Dyakonov, M. (2019). When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing. Ieee Spectrum, 56(3), 24-29.

Aithal, P. S. (2023). Advances and new research opportunities in quantum computing technology by integrating it with other ICCT underlying technologies. International Journal of Case Studies in Business, IT and Education (IJCSBE), 7(3), 314-358.

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography.

Dyakonov, M. (2019). When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing. Ieee Spectrum, 56(3), 24-29.

Aithal, P. S. (2023). Advances and new research opportunities in quantum computing technology by integrating it with other ICCT underlying technologies. International Journal of Case Studies in Business, IT and Education (IJCSBE), 7(3), 314-358.

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.

Trizna, A., & Ozols, A. (2018). An overview of quantum key distribution protocols. Inf. Technol. Manage. Sci, 21.

Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., ... & Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: a survey. Theoretical Computer Science, 560, 62-81.

Javed, M., & Aziz, K. (2009, December). A survey of quantum key distribution protocols. In Proceedings of the 7th International Conference on Frontiers of Information Technology (pp. 1-5).

Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., ... & Voznak, M. (2020). Quantum key distribution: a networking perspective. ACM Computing Surveys (CSUR), 53(5), 1-41.

Bedington, R., Arrazola, J. M., & Ling, A. (2017). Progress in satellite quantum key distribution. npj Quantum Information, 3(1), 30.

Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., ... & Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: a survey. Theoretical Computer Science, 560, 62-81.

Yang, Z., Zolanvari, M., & Jain, R. (2023). A survey of important issues in quantum computing and communications. IEEE Communications Surveys & Tutorials.

D'Ariano, G. M., Kretschmann, D., Schlingemann, D., & Werner, R. F. (2006). Quantum bit commitment revisited: the possible and the impossible. arXiv preprint quant-ph/0605224, 10.

Yadav, V. K., Andola, N., Verma, S., & Venkatesan, S. (2022). A survey of oblivious transfer protocol. ACM Computing Surveys (CSUR), 54(10s), 1-37.

Sharma, M., Choudhary, V., Bhatia, R. S., Malik, S., Raina, A., & Khandelwal, H. (2021). Leveraging the power of quantum computing for breaking RSA encryption. Cyber-Physical Systems, 7(2), 73-92.

Asif, R. (2021). Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. IoT, 2(1), 71-91.

Khalid, A., Oder, T., Valencia, F., O'Neill, M., Güneysu, T., & Regazzoni, F. (2018, May). Physical protection of lattice-based cryptography: Challenges and solutions. In Proceedings of the 2018 on Great Lakes Symposium on VLSI (pp. 365-370).

Wang, H., Zhang, H., Wang, Z., & Tang, M. (2011). Extended multivariate public key cryptosystems with secure encryption function. Science China Information Sciences, 54, 1161-1171.

Amer, O., Garg, V., & Krawec, W. O. (2021). An introduction to practical quantum key distribution. IEEE Aerospace and Electronic Systems Magazine, 36(3), 30-55.

Zavala, M., & Barán, B. (2021, October). QKD BB84. A Taxonomy. In 2021 XLVII Latin American Computing Conference (CLEI) (pp. 1-10). IEEE.

Waks, E., Inoue, K., Santori, C., Fattal, D., Vuckovic, J., Solomon, G. S., & Yamamoto, Y. (2002). Quantum cryptography with a photon turnstile. Nature, 420(6917), 762-762.

Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. Reviews of modern physics, 92(2), 025002.

Lvovsky, A. I. (2018). Quantum physics: an introduction based on photons. Springer.

Khalighi, M. A., & Uysal, M. (2014). Survey on free space optical communication: A communication theory perspective. IEEE communications surveys & tutorials, 16(4), 2231-2258.

Kashyap, S., Bhushan, B., Kumar, A., & Nand, P. (2022). Quantum blockchain approach for security enhancement in cyberworld. In Multimedia Technologies in the Internet of Things Environment, Volume 3 (pp. 1-22). Singapore: Springer Singapore.

Singh, A., Dev, K., Siljak, H., Joshi, H. D., & Magarini, M. (2021). Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. IEEE Communications Surveys & Tutorials, 23(4), 2218-2247.

Kent, A. (2011). Unconditionally secure bit commitment with flying qudits. New Journal of Physics, 13(11), 113015.

Kaniewski, J. (2015). Relativistic quantum cryptography. arXiv preprint arXiv:1512.00602.

Sidhu, J. S., Joshi, S. K., Gündoğan, M., Brougham, T., Lowndes, D., Mazzarella, L., ... & Oi, D. K. (2021). Advances in space quantum communications. IET Quantum Communication, 2(4), 182-217.

Majot, A., & Yampolskiy, R. (2015). Global catastrophic risk and security implications of quantum computers. Futures, 72, 17-26.

Hanzo, L., Haas, H., Imre, S., O'Brien, D., Rupp, M., & Gyongyosi, L. (2012). Wireless myths, realities, and futures: from 3G/4G to optical and quantum wireless. Proceedings of the IEEE, 100(Special Centennial Issue), 1853-1888.

Peeran, M., & Shanavas, A. M. (2022). E-governance security via public key cryptography using elliptic curve cryptography. Materials Today: Proceedings, 49, 3568-3573.

Kumar, A., Bhatia, S., Kaushik, K., Gandhi, S. M., Devi, S. G., Diego, A. D. J., & Mashat, A. (2021). Survey of promising technologies for quantum drones and networks. Ieee Access, 9, 125868-125911.

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. ACM Computing Surveys (CSUR), 51(6), 1-41.

Balamurugan, C., Singh, K., Ganesan, G., & Rajarajan, M. (2021). Post-quantum and code-based cryptography—some prospective research directions. Cryptography, 5(4), 38.

Easttom, W. (2022). Modern cryptography: applied mathematics for encryption and information security. Springer Nature.

Lindsay, J. R. (2020). Surviving the quantum cryptocalypse. Strategic Studies Quarterly, 14(2), 49-73.

Brijwani, G. N., Ajmire, P. E., & Thawani, P. V. (2023). Future of quantum computing in cyber security. In Handbook of Research on Quantum Computing for Smart Environments (pp. 267-298). IGI Global.

Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2019). Quantum cryptography with realistic devices. arXiv preprint arXiv:1903.09051.

Zhao, X., Xu, X., Qi, L., Xia, X., Bilal, M., Gong, W., & Kou, H. (2024). Unraveling quantum computing system architectures: An extensive survey of cutting-edge paradigms. Information and Software Technology, 167, 107380.

Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108.

Kachurova, M., Shuminoski, T., & Bogdanoski, M. (2022). Lattice-based cryptography: A quantum approach to secure the iot technology. In Building Cyber Resilience against Hybrid Threats (pp. 122-133). IOS Press.

Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., & Ravi, L. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. Future generation computer systems, 112, 724-737.

Lo, C. C., & Chen, W. J. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Applications, 39(1), 247-257.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), 237-243.

van Deventer, O., Spethmann, N., Loeffler, M., Amoretti, M., van den Brink, R., Bruno, N., ... & Wilhelm-Mauch, F. K. (2022). Towards European standards for quantum technologies. EPJ Quantum Technology, 9(1), 33.

Obert, J., Cordeiro, P., Johnson, J. T., Lum, G., Tansy, T., Pala, N., & Ih, R. (2019). Recommendations for trust and encryption in DER interoperability standards (No. SAND-2019-1490). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); Kitu Systems, San Diego, CA (United States); SunSpec Alliance, San Jose, CA (United States); Cable Labs, Louisville, CO (United States).

Rohit, R. V., Kiplangat, D. C., Veena, R., Jose, R., Pradeepkumar, A. P., & Kumar, K. S. (2023). Tracing the evolution and charting the future of geothermal energy research and development. Renewable and Sustainable Energy Reviews, 184, 113531.