Potential QkD Protocols and Secure Links within Quantum Networks

Wu Liu*, Zho Jiang

College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China.

Keywords:
Covert communication;
EnCipherment;
Interaction;
Networks;
Protocols

Corresponding Author Email:
liuw.u@zju.edu.cn

DOI: 10.31838/IJCCTS.12.01.08

Received: 10.04.24

Revised: 16.05.24

Accepted: 11.06.24

Abstract

Quantum Key Distribution (QKD) acts as a revolutionary model for secure communication in quantum networks due to its capacity to offer maximum security compared to other methods of data transfer that are informed by the principles of quantum mechanics. This abstract also tries to discuss the essential requirements of QKD for both BB84 and E91 focusing on Q states and entangled photon pairs that allow two separated parties to establish mutually agreed secure keys. Quantum mechanics does not allow the cloning of states – the no-cloning theorem – which increases security of the channel and QKD immunity to traditional hacking. In addition, exploring the incorporation of QKD into current [communication] systems and discussing the issues, as well as the progress made in the encouraging implementation of those protocols in very long distances. The study focuses on designing effective QKD systems that can cater for increasing demands for secure communication in fields such as finance, health care and defense. This piece of work will try to look at both theoretical and practical approaches to QKD so as to lay down the foundation for the future of secure connection in quantum network thus fulfilling its goal of ensuring that sensitive information is protected against such threats as we see the world going becoming more and more reliant on technology.

How to cite this article: Liu W, Zho Jiang Z (2024). Potential QkD Protocols And Secure Links Within Quantum Networks . International Journal of communication and computer Technologies, Vol. 12, No. 1, 2024, 60-67

Introduction

A new technology known as Quantum Key Distribution (QKD), is fast changing the nature of secured communication networks. Through integrating physics into the technology, the internet connection provides unmeasurable security by developing encryption keys that are immune to hacking. As the quantum computers evolve basic cryptographic techniques become more exposed so QKD becomes an important innovation in data protection. The QKD quantum protocols have implications to aspects of network security and the exploration of such area is beneficial. Starting from the history of cryptography, right up to the relative components of QKD networks are explored in this article. It analyses the routing methodologies, different network architectures and performs a detailed security evaluation to manufacture an appreciation for the QKD capability inBook tracing the evolution of communications for security to digital future.[1-2]

Evolution of Cryptography to QKD

This paper briefly explains the transition from classical cryptography to Quantum Key Distribution or QKD and how the progress has been made in the sphere of secure communication. This evolution affects how information is protected in a world that is more and more relying on computerisation (Figure 1).

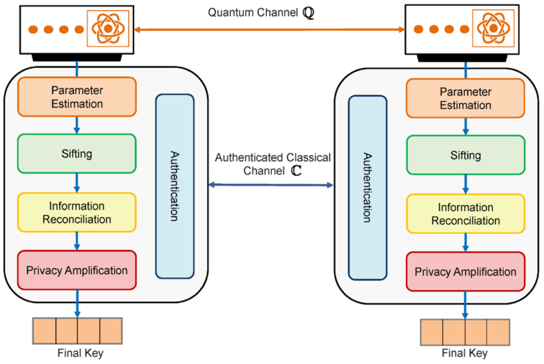

Fig. 1: Exploring QKD Quantum Protocols for Secure Communication Networks

Classical Cryptography

Traditional cryptography that is based on the mathematical algorithms has been used to provide secure communications for a long time. It is based on the problem that it is practically impossible to solve mathematical problems like the factorization of very large numbers. This approach has been helpful in enhancing security of data that should not be accessed by anyone who does not have permission to do so. In classical cryptography the process by which the plaintext is mapped onto the ciphertext is governed by a key. The security of this method relies with the fact that only those who are authorized have the key which is used to gain in to the system/ program. However, classical cryptography has certain problems of dealing with key distribution and where to store those keys in extensive networks. There are two main types of classical cryptography: symmetric and asymmetric. In symmetric cryptography, the same key, the private key, is used for the process of encryption and decryption. Although this method is highly effective, it has a shortcoming as the key has to be distributed between the sender and the receiver of the message. Asymmetric cryptography, also known as public key cryptography, addresses this issue by using a pair of keys: A pair of keys, one for the general use in encrypting the data and the other for decryption. While this will make management of key distribution easier, it compounds the computational aspect slightly.[3]

Public Key Cryptography

Public key cryptography which was first discovered in 1976 by Whitfield Diffie and Martin Hellman in United States has initiated a revolution in safe communication. This method is favourable for two strangers to exchange encrypted messages as a means of negotiating without having to input any secret key in advance. In public key systems, each user has a pair of mathematically related keys: It consists of a public key which are given out to anyone and a private key which is kept secret from everyone. It is impossible to decrypt data encrypted with the use of the public key hence this requires the private key. This asymmetrical aspect is realized on various applications based on the method such as secure electronic mail, digital signatures, and trades on the web. But the security of public key cryptography is based on one or another decisional computational problem. Currently, such systems can become penetrable with the help of computing resources, and this issue can intensify with the development of quantum computing.

Post-Quantum Cryptography

Since the appearance of quantum computers is a threat to current cryptographic models, post-quantum cryptography (PQC) has emerged. PQC is to design schemes that are robust against both classical and quantum computers. PQC algorithms rely on mathematical problems for which researchers expect quantum computers will have issues working on. These are lattice cryptography, multivariate cryptography and hash based signatures. The United States' National Institute of Standards and Technology (NIST) has taken up the role of promoting PQC algorithms standardization for general use. Although the PQC can be proposed as a solution to the threat, it does not bet on quantum principles, but on computational security. This is where QKD steps in, to provide another regime for secure communication all together. QKD relies on principles of the theory of quantum mechanics including the no cloning theorem and the Heisenberg uncertainty relation to deliver ultimate security. However, QKD distinguishes from classification or post-quantum cryptography in that QKD is built on the principle of quantum mechanics rather than on the assumption of complexity of computations. In QKD systems the information can be encoded onto quantum states of the system like the polarizations of the photons. Mere observation or duplication of these quantum states gives rise to detectable noise, which informs the original communicating parties of the eavesdropper's existence. This transition from classical cryptography to QKD is seen to affect how secure communication is implemented in the quantum network. Although these form the backbone, the QKD appears to present a solution that is unapproachable, especially by the quantum computers.[4-5]

QKD Network Components

QKD networks are intricate systems that must include several components for them to work as expected at all times. These co0mponents collectively come into picture to produce, regulate and broadcast the quantum-secure keys for assured secure calling over long distance. It's important to understand the basic components of a QKD network; let us take a closer look

QKD Nodes

QKD nodes serve as network elements that can be considered basic in a QKD network. These nodes are primarily involved in creating, manipulating, and measuring quantum states, on which the creation of keys needs to be based. In a typical QKD network, nodes can be classified into two main types:

1. Transmitter nodes: These nodes produce quantum states for instance polarized photons and relay them through the quantum channels.
2. Receiver nodes: These nodes recognize and quantify the incoming quantum states in order to pull out the significant data.

QKD nodes use complex devices such as lasers to create the photons, modulators for coding the message and single photon detectors for evaluating the received quantum states. These nodes are: The design and implementation of these nodes 0influence the performance and security of the QKD network that exists.

Quantum Channels

Quantum channels are the physical medium through which quantum states are transmitted Quantum channel are the physical conduit through which quantum states flow between two QKD nodes. They are often deployed employing optical fibers or the free space communication link. More specifically, the selection of quantum channel has implications for the distance beyond which QKD can be conducted optimally. Quantum channels implemented by optical fibers have been shown to operate over distances to 508 km in the measurement-device-independent scenario and 1002 km in the twin field-case. Nevertheless, the transmission distance remains a critical issue for QKD networks, because the quantum states utilized are susceptible to noise and loss in the channel condition. While the free-space quantum channels, especially using satellites, can realize a longer distance. This also has led to a revolution in the field where it permits intercontinental quantum key distribution. For example, the QUESS space mission that began in August 2016 synchronizes an international communication channel based on QKD between China and Austria, spanning a distance of 7500 kilometers of ground link.

Key Management Systems

Quantum Key Distributors (QKD) are the fundamental building blocks central to the management of quantum keys and are involved in the processing, storage and dissemination of these keys within the QKD network and include the Key Management Systems (KMS). These systems have an influence on the production and security of the concentric networks by guarantee that the keys are where they require and when they are required.

The core functionalities of a KMS include:

1. Secure key storage: KMS offered would support quantum keys created by qKD devices through the security of a data depository.
2. Global key distribution: This function helps organize the distribution of the keys in between two nodes not connected with the quantum channel.
3. Key lifecycle management: KMS is responsible for generation, storing, usage, archiving and deletion of quantum keys.
4. Key supply: This function is responsible for providing keys to the cryptographic applications whenever necessary.

For the purpose of increasing security, the current unification of widely used KMS solutions widely employs a post-quantum cryptography (PQC) hybrid approach. This enhances security by generating the last key from both a QKD safeguarded key and a second end-to-end secure key generated from PQC algorithms. The advent of standardised interfaces, for instance by the european telecommunications standards institute (ETSI), contributes to a revolution from the compatibility of QKD systems and application. These standards describe how cryptographic apps known as Secure Application Entities (SAEs) establish relationships with Key Management Entities (KMEs) to use QKD network services. In this paper, the growth and development of QKD networks affect the management and scalability influences of Software-Defined Networking (SDN). SDN-enabled QKD networks typically consist of three layers: This includes the application layer, and the control layer, and the QKD layer. This architecture offers the possibility to manage QKD devices and to drive quantum keys through the network at any time [6]-[7].

Routing Techniques in QKD Networks

Routing in QKD networks is a complex problem because of the physics involved and by the fact that it requires transfer of keys with strong constraints over long distances. With the development of QKD networks, different routing schemes have been offered to translate these issues and improve the performances of quantum communications.

Trusted Node Routing

The technique of trusted node routing is used in the networks of QKD to create longer distances of secure communication. In this approach the network is made of several quantum repeaters and some trusted nodes which act as a bridge between the sender and the receiver. They are responsible for division of the system into sub-areas in order to significantly enlarge the communication distances through limiting signal attenuation through fewer intermediate nodes.

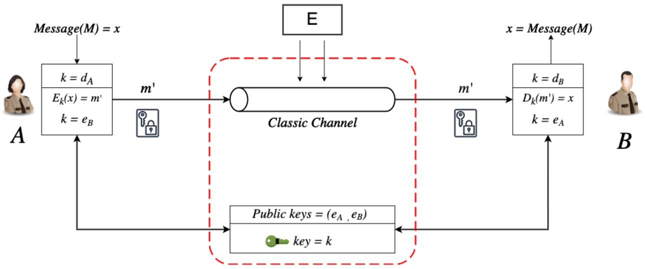

Fig. 2: Routing Techniques in QKD Networks

The trusted nodes engage in measurements established between the parties to increase the security levels while providing key distribution in larger distances. This technique affects the overall network topology because it needs positioning of the trusted nodes to facilitate generation of key rates and enhance network stability. However, as it can be observed there are several paths between Alice and Bob as a result of trusted node routing hence leading to increased key generation rates. In an additive manner key bits are determined on each connecting path thus enhancing the efficiency of the network. Nevertheless, this approach entails a serious risk since the integrity of the intermediate nodes has to be guaranteed and such a guarantee cannot be rendered in a number of practical situations.[8]

Measurement-Device-Independent QKD

MDI-QKD means a revolution to QKD routing since it eradicates detector side-channels and steps up security. In MDI-QKD, Alice and Bob both encode and send light pulses they independently generate to a third node (Charlie) where the pulses interfere and are measured using SPDs. The revenue transfer technique affects the matter of security of QKD networks in a manner that even if Charlie becomes an illicit participant, QKD protocol remains secure. Due to the 'untrusted' character of Charlie, no trust has to be put on the intermediate node for the assurance of the entire security of MDI-QKD protocol. Improvements made in MDI-QKD in recent developments have included successful transmission an acceptable distance of up to 404km and GHz systems. These developments have implications for the actual implementation of QKD networks as they facilitate the generation of higher secure key rates and better adapt QKD for mainstream use. MDI-QKD seems more suitable for constructing QKD network in central star connected topology, where high cost SPDs are placed and many users are equipped low cost compact transmitters. This poses a question of architectural influence on the QKD networks and their implementation, specifically their costs and scalability to a greater application.

Twin-Field QKD

Twin-Field QKD (TF-QKD) is a new protocol that is heralding changes in the long-distance quantum cryptography. Currently, the repeater-less bound is unsolvable with the current technology, but with the help of the intermediate node, Charlie, which measures the first-order interference of two optical fields from Alice and Bob, TF-QKD is capable of doing this. The great benefit of TF-QKD over other QKD protocols is the rate-loss scaling which is comparable to that of single-repeater QKD. This implies that the secure key rate (SKR) of TF-QKD is proportional to the root of channel transmittance and thus can achieve much longer distances than the other QKD schemes. Later theoretical simulations have provided support for the fact that the rate-loss scaling of TF-QKD is superior and the method has time and again broken records for the distance of communication, at present having commenced at 833 km. This has implications for future prospects of large-scale quantum communication networks as well as secure transfers of keys over remarkably large distances. It is worth noting that for ring topologies, the aforementioned TF-QKD networks have been proposed and, in particular, shown to work; however, more recent development has also established that it is possible to use star network configurations. These developments affect the scalability of the proposed TF-QKD networks as well as their application areas in areas such as banking, data centres, electronic voting, military security among others. As the QKD networks are being developed further, the use of the given routing techniques is influenced by the combination with SDN concepts in terms of their control and growth. SDN-enabled QKD networks typically consist of three layers: comprises of the application layer, control layer and the QKD layer. This architecture provides the ability to manage QKD devices in a dynamic manner and QK routing through the network and lays down foundation for creating robust quantum communication pathways.[9-10]

QKD Network Topologies

This paper presents the effects of the QKD network topologies on the performance, security, and expansibility of quantum communication systems. Different networks' architectures have therefore been proposed to deal with key distribution issue in long distance and many to many clients QKD networks.

Point-to-Point

P2P topology refers to a QKD network that links two nodes at a time, and it is the simplest form of deployment. In this configuration, there are two nodes connected through a direct quantum channel through which secret keys are continually produced for the immediate adjacent end nodes. P2P QKD systems are most suitable for the intercontinental quantum communication distances (>5000 km) and long-distance quantum communication distances (1000-5000 km), where a direct quantum link can be established from one place to other. In the case of P2P topology, the primary usage of the quantum channel is to help local keys be generated independently for every QKD system. These local keys build up as the core entity for secure interactions between the two conjoint nodes. However, we find that P2P topology is limited when it comes to setting up shared keys between two distant end nodes that do not have an established link via a quantum channel.

Trusted Relay

The distance constraint in P2P QKD systems have led to the development of a more practical solution provisioned known as the trusted relay topology widely used in practical QKD networks. This approach deploys intermediate nodes with trusted repeaters which enables the processing of the transfer of secret keys in stages from the source node to the designated destination nodes along the QKD line. In a trusted relay network, the entire distance is segmented into smaller distances each is less than 100km in most cases. For example, Beijing-Shanghai backbone quantum link in China has more than 2000 kilometers and 32 trusted relay nodes. Such a segmentation promotes the extension of QKD networks much further than it would have been possible under the P2P topology alone. The idea of a trusted relay entails decryption of the keys and re-encryption of the secret keys at each mediator. This operation is performed using an information theoretic secure One-Time Pad (OTP) cryptographic algorithm. The major goal is to create different secret keys for each transmission division so that the transmission from one node to another is made secure. Hence trusted relay topology affects the reach of the QKD networks but has the assumption that all the middle nodes are trusted. This requirement has triggered a revolution in the quest for other more secure forms of QKD, for examples, the MDI-QKD and TF-QKD, ideal for increasing security besides the need for the intermediate nodes.

Quantum Repeater Based

Quantum repeater-based topology concerns the distances and scalability of QKD networks consideration of the constraints posed by conventional networks. Quantum relays are important elements in the further development of QKD networks beyond their limitations achieved by 'refreshing' and forwarding quantum signals. The main roles of quantum repeaters are to minimize the impact of decoherence and signal attenuation, to provide trusted information transfer through significantly larger distances. This topology relies on three key building blocks: which are entanglement swapping entanglement purification and quantum memories. It is, however, necessary to remember that actual physical embodiments of fully functional quantum repeaters remain one of the focused topics in current and aspiring research and development projects (Table 1).[11-12]

The communicating link in a quantum repeater based network is partitioned into number of comparatively shorter segments. This ability of the repeater stations to capture quantum data in photons enables the enhancement of the entanglement generation in quantum links over long distance networks. This topology can entangle two repeater stations at a time by using entanglement swapping between the chains, and hand over the entanglement from one link to the next allowing the reliable distribution of entanglement to a large number of users over long distances. The emergence of quantum repeater-based topologies has brought revolution in quantum communication by introducing prospects of the long-distance high-fidelity quantum networks. It is further envisaged that as the different fields of research develops in the specified area that it will be instrumental in shaping the secure quantum communications architecture within the global electronic network.

Security Analysis of QKD Networks

The security of QKD networks is one of the fundamental issues that should be addressed and examined in detail to develop quantum security. Although QKD protocols provide ideal post-processing models of security that are founded on realistic physics, they can possess weaknesses that attackers can leverage. The following part discusses different kinds of attacks that may exist in the QKD context and how they affect this type of systems (Table 2).

Eavesdropping Attacks

In QKD networks, the strongest threat is eavesdropping which immediately threatens the security of distributed keys. Every time a quantum system is measured in quantum communication, it can be noticed that a change to the system occurs or, in other words, if an eavesdropper tries to intercept the transmitted quantum data, it becomes known. This property is used to form the basis of QKD's security against eavesdropping.

Several eavesdropping strategies have been identified:

1. Intercept-Resend Attack: An eavesdropper gets in between the sender and receiver of quantum information, and instead of directly stealing the information, he or she measures it and then sends an entirely new one to the intended recipient. This

Table 1: Major Quantum Key Distribution Protocols

QKD Protocol	Key Features	Security Mechanism	Advantages	Limitations
BB84 (Bennett-Brassard 1984)	Utilizes polarized photons for key exchange	Relies on quantum no-cloning theorem	Simple, well-established, high security	Requires complex optical components, limited range
E91 (Ekert Protocol)	Based on quantum entanglement	Uses Bell's inequality to ensure security	Strong security via entanglement, prevents eavesdropping	Difficult to maintain entanglement over long distances
B92 (Bennett 1992)	Simplified version of BB84, uses fewer states	Relies on quantum state discrimination	Reduced complexity, lower resource requirement	More vulnerable to certain types of attacks compared to BB84
Differential Phase Shift (DPS)	Encodes key in the phase difference between consecutive photons	Based on phase coherence	High key generation rate, robust against photon number splitting (PNS) attacks	Requires stable phase reference, more challenging to implement
Continuous Variable QKD (CV-QKD)	Uses continuous variables like amplitude and phase of light	Security based on the uncertainty principle	Can be implemented with standard telecom components	More sensitive to channel noise, complex error correction required

Table 2: QKD Deployment Challenges and Solutions

Challenge	Description	Impact on QKD Systems	Potential Solutions	Implementation Feasibility
Photon Loss	Loss of photons during transmission over optical fiber or free space	Reduces the key generation rate, limits the range	Use of quantum repeaters or trusted relay nodes	Quantum repeaters are still in development, trusted relays compromise end-to-end security
Error Correction	Errors in photon detection or transmission lead to incorrect keys	Reduces key rate and requires additional communication	Advanced error correction techniques such as LDPC codes or Cascade	Feasible with moderate complexity, but adds overhead

Challenge	Description	Impact on QKD Systems	Potential Solutions	Implementation Feasibility
Channel Noise	Noise from the environment (thermal, background light) degrades signal quality	Increases error rate, compromises security	Adaptive modulation, filtering, and noise reduction techniques	Noise filtering feasible, requires complex hardware
Distance Limitations	QKD is limited in range due to exponential loss over long distances	Limits the practical implementation in global networks	Satellite-based QKD, development of long-range quantum repeaters	Satellite-based systems are under development but costly
Quantum Hacking	Attacks exploiting imperfections in QKD hardware (e.g., side-channel attacks)	Allows potential eavesdroppers to gain information on the key	Device-independent QKD, improved hardware security standards	Hardware improvements are feasible but require significant research and development

attack is difficult to do because it is comparatively difficult to maintain quantum coherence of the intercepted quantum information.

2. Photon Number Splitting Attack: This complex process provides for beam splitting, while retaining one half of the photons in storage and transmitting the other half to the addressee. Because the attack relies on the misuse of the properties of photons in quantum communication, it can be virtually impossible to notice.
3. Trojan Horse Attack: An eavesdropper places an interfering particle into an information-transfer channel to obtain an unauthorized peek at the data without being noticed.

As for the threats, in QKD protocols such as BB84 have integrated procedures that allow determining spying attempts. Thus, entanglement and the no-cloning theorem are the measures that can help reveal an eavesdropper's interference.

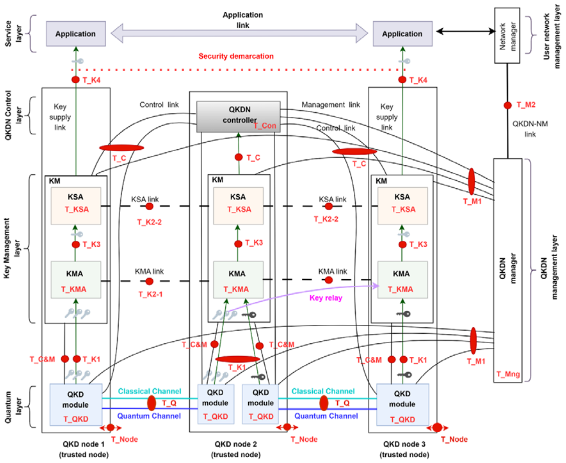

Fig. 3: Eavesdropping Attacks

Side-Channel Attacks

Side channel attacks remain a threat to QKD systems since they specifically attack implementation rather than the QKD protocol theory. княCanada: These attacks seek to exploit side channels, that is, channels through which information can be leaked unintentionally, by exploiting electromagnetic emanations, power consumption or timing signals. A side-channel attack has been proved in the current studies to use deep learning to analyse the radio frequency electromagnetic signals emanating from QKD devices. In some situations these have been able to effect most information regarding the secret key at a distance as close as a few centimeters. Therefore, emission security is well needed to be designed with the early stage of QKD devices for the prevention of side-channel attacks. It is found that better shielding and appropriate selection of components can considerably reduce the information leakage through classical side channels.

Denial-of-Service Attacks

In the case of the QKD networks, Denial-of-Service (DoS) attacks constitute the main problem. Some of the concerns basic to QKD security assertions, namely the sensitivity to eavesdropping, expose these systems to DoS threats. A misfortune in quantum communication link can be achieved by an attacker by just enhancing the error rate within the quantum transmission line. Although this kind of vulnerability is considered exaggerated because the attacker would have to tap into the optical fiber, the case shows that good network architectures can include mechanisms for rerouting quantum signals in the event of an attack. On a similar note but a more dangerous form of DoS attack can use the authentication process in QKD protocols and can possibly use up all the pre-shared secret keys for use in the authentication process. These challenges are therefore going to require a very careful key management and consideration of post-quantum public-key authentication methods in selected cases. However, this approach adds the layer of complexity and risks that need to be considered when choosing the correct strategy. Altogether, the results indicate that as this technology develops, it is critical to provide extensive security analyses which integrate both the quantum and the classic approaches to attack. By addressing these challenges, QKD networks are in a position to gradually transit towards the envisaged state whereby QKD could provide a strong basis of secure communication in the age of quantum information processing.

Conclusion

In this case, the study on the QKD quantum protocols will have implications to the proper changing of the secure communication networks. From defining a theoretical framework of cryptography to its most refined elements in QKD networks, this technology promises a solution to emerging cyber threats. The discovery of other forms of routing and network configurations has led to the revolution in expanding and enhancing the utility of quantum communication with better structures. In this regard, security issues remain the key area to consider as networks for QKD develop in the future. Have a positive effect on the reliability of QKD systems: the ongoing research includes vulnerability analysis and countermeasures, eavesdropping, and side-channel attacks. Due to the progresses in quantum repeaters and key management system, QKD is expected to occupy an important position in defending the future digital world both against classical and quantum attacks.

References

1. Sharma, P., Agrawal, A., Bhatia, V., Prakash, S. and Mishra, A.K., 2021. Quantum key distribution secured optical networks: A survey. IEEE Open Journal of the Communications Society, 2, pp.2049-2083.
2. Kumar, P., Kundu, N.K. and Kar, B., 2024. Quantum Key Distribution Routing Protocol in Quantum Networks: Overview and Challenges. arXiv preprint arXiv:2407.13156.
3. Wang, Y., Li, Q., Han, Q. and Wang, Y., 2019. Modeling and simulation of practical quantum secure communication network. Quantum Information Processing, 18, pp.1-18.
4. Bajrić, S., 2023. Enabling secure and trustworthy quantum networks: current state-of-the-art, key challenges, and potential solutions. IEEE Access, 11, pp.128801-128809.
5. Bajrić, S., 2023. Enabling secure and trustworthy quantum networks: current state-of-the-art, key challenges, and potential solutions. IEEE Access, 11, pp.128801-128809.
6. Lai, J., Yao, F., Wang, J., Zhang, M., Li, F., Zhao, W. and Zhang, H., 2023. Application and Development of QKD-Based Quantum Secure Communication. Entropy, 25(4), p.627.
7. Cavaliere, F., Prati, E., Poti, L., Muhammad, I. and Catuogno, T., 2020. Secure quantum communication technologies and systems: From labs to markets. Quantum Reports, 2(1), pp.80-106.
8. Liu, R., Rozenman, G.G., Kundu, N.K., Chandra, D. and De, D., 2022. Towards the industrialisation of quantum key distribution in communication networks: A short survey. IET Quantum Communication, 3(3), pp.151-163.
9. Alanezi, A., Abd El-Latif, A.A., Kolivand, H. and Abd-El-Atty, B., 2023. Quantum walks-based simple authenticated quantum cryptography protocols for secure wireless sensor networks. New Journal of Physics, 25(12), p.123041.
10. Curcic, T., Filipkowski, M.E., Chtchelkanova, A., D'Ambrosio, P.A., Wolf, S.A., Foster, M. and Cochran, D., 2004. Quantum networks: from quantum cryptography to quantum architecture. ACM SIGCOMM Computer Communication Review, 34(5), pp.3-8.
11. Sihare, S.R., Guided and unguided approaches for quantum key distribution for secure quantum communication. Security and Privacy, p.e453.
12. Cao, Y., Zhao, Y., Zhang, J. and Wang, Q., 2022. Software-defined heterogeneous quantum key distribution chaining: An enabler for multi-protocol quantum networks. IEEE Communications Magazine, 60(9), pp.38-44.