Employing Quantum Key Distribution for Enhancing Network Security

Qifeng Liang

Cambrian Academy, San Jose, 95118, USA

qifeng.liang@cambrianacademy.org

Abstract. The rapid advancement of quantum computing unveils significant potential in addressing various real-world challenges. Notably, the Quantum Key Distribution (QKD) protocol emerges as a promising solution for enhancing network communication security through its distinctive anti-eavesdropping mechanism. This research paper elucidates the necessity of QKD by illuminating the limitations associated with conventional network security encryption methods, including susceptibility to unstable connections, unauthorized access, eavesdropping, data tampering, and denial-of-service attacks. Furthermore, it explicates the fundamental principles of quantum physics underpinning QKD, comprising quantum superposition, quantum entanglement, and the no-cloning theorem. Several pivotal QKD protocols, specifically BB84, E91, and B92, are introduced within the body of this work. The exploration of Quantum Key Distribution applications in diverse domains, such as optical and wireless networks, the financial and medical sectors, and even satellite-based QKD, is extensive. This in-depth analysis uncovers the potential of QKD and its wide-ranging impact across various fields, while also providing insights into the challenges associated with QKD implementation.

Keywords: Quantum key distribution protocol, Network, Application

1 Introduction

The exploration of Quantum Key Distribution applications is of paramount importance, given their profound implications in real-world scenarios. QKD, underpinned by the tenets of quantum mechanics, facilitates the establishment of secure communication channels [1]. It responds to the escalating need for impenetrable encryption methodologies, holding substantial promise. Delving into QKD applications in networks is indispensable as it caters to the demand for fortified communication in diverse sectors, from government and defense to finance and healthcare. Through practical implementation research, this paper can contribute to the inception of robust encryption systems that offer rigorous protection of sensitive data. Moreover, investigating the QKD applications in networks enables the identification and mitigation of practical hurdles. Gaining insights into elements such as channel noise, scalability of systems, and seamless integration with pre-existing Exploring the applications of Quantum Key Distribution

P. Kar et al. (eds.), *Proceedings of the 2023 International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2023)*, Advances in Computer Science Research 108,
https://doi.org/10.2991/978-94-6463-300-9_53

is of paramount importance due to their profound implications in real-world scenarios. Quantum Key Distribution, founded on the principles of quantum mechanics, enables the creation of secure communication channels [1]. This method responds to the escalating need for impenetrable encryption methodologies, demonstrating significant promise. A deep dive into Quantum Key Distribution applications in network settings is indispensable as it meets the demand for fortified communication across diverse sectors, from government and defense to finance and healthcare. Through practical implementation research, this paper may contribute to the development of robust encryption systems offering rigorous protection for sensitive data. Moreover, investigating the applications of Quantum Key Distribution in networks allows for the identification and mitigation of practical hurdles. Understanding components such as channel noise, scalability of systems, and seamless integration with pre-existing infrastructure is critical for the successful real-world incorporation of Quantum Key Distribution.

Beyond merely secure communication, potential applications of Quantum Key Distribution also extend to secure quantum networks and quantum internet [2]. An examination of these applications not only propels the advancement of quantum technologies but also enables secure quantum information processing and long-range quantum communication. In summation, researching the applications of Quantum Key Distribution across networks plays a pivotal role in strengthening secure communication, addressing practical challenges, and exploring new domains of quantum technology. This research paper seeks to clarify the applications of Quantum Key Distribution across networks, thereby ensuring enhanced security and privacy in our increasingly interconnected world.

2 Overview of Network Security

The story of the internet traces back to the late twentieth century when the creation of the Institute of Electrical and Electronics Engineers' 802.11 standards defined the physical layer and media access control layer for wireless communication. Following this, improved versions such as the 802.11n, 802.11ac, and 802.11ax were developed, offering superior transmission speeds and performance in comparison to their predecessors. Wireless Local Area Network protocols can be categorized based on distinct characteristics and capabilities. Common types encompass single-band (two-point-four gigahertz), dual-band (two-point-four gigahertz and five gigahertz), and multi-band protocols. Each variety involves trade-offs among transmission distance, speed, and compatibility to cater to diverse application scenarios and user needs [3].

With the Internet assuming an increasingly pivotal role in modern society, network security has become an imperative concern. The limitations within Wireless Local Area Network protocols present substantial challenges to network security. Notably, the reliance of Wireless Local Area Networks on radio waves for transmission exposes them to physical disruptions, such as signal interference caused by obstacles like walls, which results in unstable connections and data loss. Moreover, the inherent openness of Wireless Local Area Network networks makes them vulnerable to unauthorized access, eavesdropping, data tampering, and denial-of-service attacks. Thus, a stronger security

solution to address these issues is of utmost necessity. The protocol of quantum key distribution holds potential as a groundbreaking solution. By leveraging quantum principles, this protocol provides unprecedented security capabilities that can significantly alleviate the vulnerabilities associated with Wireless Local Area Network networks.

3 Introduction to QKD Principles

3.1 Quantum Computing Properties

Superposition. Superposition is the unique ability of qubits to exist in multiple states simultaneously. In QKD, the sender can take a use of this property, due to the principle of superposition, the receiver can select different measurement bases for these qubits, leading to diverse outcomes. This inherent uncertainty thwarts any attempt by an unauthorized third party to gain precise knowledge of the transmitted keys. By leveraging quantum superposition, QKD ensures that the exchanged information remains secure and impervious to eavesdropping [4].

Entanglement. Secondly, quantum entanglement is a unique property in which two or more qubits become intrinsically linked, irrespective of their spatial separation. An example would be one of the EPR pairs, also known as Bell State:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1}$$

Where measurement of either qubit will change the state of another qubit, either to $|00\rangle$ or $|11\rangle$. In the realm of Quantum Key Distribution, this property plays a vital role. The sender can generate entangled qubits and transmit one part of the entangled pair to the receiver. The entanglement between these qubits allows for the detection of any unauthorized interception or tampering with the key. If an eavesdropper attempts to eavesdrop on the entangled qubits during transmission, their entangled states become disrupted or "collapse." This collapse of entanglement alters the correlation between the qubits, thereby triggering a change in the received qubits' states. Consequently, both the sender and receiver can detect the presence of a potential security breach. The utilization of entanglement in QKD guarantees secure and reliable key distribution, protecting the transmitted information from potential eavesdropping or unauthorized access. It demonstrates the power of quantum mechanics in enabling secure communication protocols that leverage the intrinsic properties of entangled qubits [5].

No- Cloning Theorem. The last essential component of Quantum Key Distribution is the No-Cloning theorem. This theorem serves as a fundamental principle for the functioning of QKD, stating that it is impossible to create two identical qubits. In other words, it is not possible to make a perfect copy of the state of any qubit without destroying the original information it holds.

The security of QKD heavily relies on this property. The inability to clone qubits ensures that the information encoded in them remains secure during the key transmission process. Any unauthorized attempt to copy the state of the qubits will unavoidably result in the destruction of their original states. This destructive process serves as an alert for the legitimate sender and receiver, indicating the presence of a potential security breach or eavesdropping attempt [6]. The No-Cloning theorem plays a crucial role in guaranteeing the security and integrity of the QKD protocol. It prevents adversaries from making perfect copies of the qubits and extracting the encoded key without detection. This inability to clone qubits is a fundamental characteristic of quantum systems, and it ensures that the exchanged keys remain confidential and resistant to unauthorized access. By relying on the No-Cloning theorem, QKD provides a robust mechanism for secure key distribution, protecting sensitive information from being compromised during transmission. This property, along with quantum superposition and entanglement, contributes to the overall security and resilience of QKD as a cryptographic protocol.

By leveraging the phenomenon of these properties, QKD provides a mechanism to verify the integrity of the key exchange process. Any attempt to intercept, copy or measure the entangled qubits will disturb their entanglement, leaving a detectable trace of unauthorized activity. These properties ensures that QKD offers a higher level of security compared to classical encryption methods, as any attempt to tamper with the entangled qubits will be immediately apparent to the communicating parties.

3.2 Typical QKD Protocols

Since the first QKD protocol BB84 was born in 1984, there have been more than a dozen different QKD protocols developed though out the time. This paper will introduce the three most classic QKD protocols as a reference.

BB84. BB84 is a quantum cryptographic protocol designed to secure communication channels against eavesdropping. Developed by Charles H. Bennett and Gilles Brassard in their paper titled “Quantum cryptography: Public key distribution and coin tossing” [4]. As the first QKD protocol, BB84 utilizes the principles of quantum mechanics to ensure secure key distribution between two parties. In BB84, the sender, Alice, encodes a secret key using quantum states, typically represented by photons. She randomly selects a basis (rectilinear or diagonal) for each photon, and transmits them to the receiver, Bob, through a quantum channel. However, due to the uncertainty principle, any attempt to measure the key disturbs its quantum state, making it detectable by Alice and Bob. Bob, unaware of Alice's chosen basis, randomly selects a measurement basis for each received photon(qubit). After the transmission, Alice publicly announces the bases she used. Bob discards the measurements that used different bases, and both Alice and Bob keep the remaining bits. To check for eavesdropping, Alice and Bob compare a subset of their key bits over a public channel [7]. If the error rate is low, they can proceed with the remaining bits as their secret key. Otherwise, they abort the protocol.

B92. The B92 protocol, introduced by Charles H. Bennett, one of the authors in BB84, is an alternative to the BB84 protocol proposed on 1982. In the B92 protocol, Alice randomly encodes quantum bits (qubits), typically represented by photons as well, into two non-orthogonal states, usually labeled as 0 and 1. These non-orthogonal states allow for a higher bit rate in comparison to the BB84 protocol. Upon receiving the qubits, Bob randomly chooses a measurement basis to measure each qubit. The measurement bases used by Bob are not aligned with Alice's encoding bases, which provides an advantage in terms of security. After the transmission, Alice and Bob communicate publicly to compare a subset of their measurement bases. If they used the same basis, Bob announces his measurement results. Alice and Bob can estimate the error rate based on this information. If the error rate is sufficiently low, they can extract a secure key from the remaining bits. In summation, BB84 uses four quantum states, while B92 uses two non-orthogonal states. B92 provides a higher bit rate but requires additional security measures due to the existence of an information leakage vulnerability.

E91. E91 is also a one of the most famous QKD protocol, proposed by Artur Ekert It differs from the BB84 and B92 protocols in several ways. Unlike BB84, which uses two non-orthogonal bases, and B92, which uses only one basis, E91 employs three non-orthogonal bases. This additional basis allows for higher efficiency and security. Moreover, in E91, entangled particles are utilized to generate the secret key. These entangled pairs are distributed between two parties, Alice and Bob, who perform measurements on their respective particles. The correlations observed between their measurements enable the extraction of a secure key.

The key difference lies in the security analysis. While BB84 and B92 protocols rely on the principles of quantum mechanics, the security of E91 is proven using the concept of "non-local games." This ensures resistance against eavesdropping attacks, even against adversaries with significant computational power. Overall, the E91 protocol distinguishes itself through the use of entangled particles and its rigorous security analysis based on non-local games, making it a promising approach for secure quantum communication.

4 Application of QKD in Networks

4.1 QKD in Classical Networks

Integration with Optical Networks. The integration of QKD with Dense Wavelength-Division Multiplexing (DWDM) systems has been achieved through the development of specialized components, such as quantum-compatible optical amplifiers and filters, which allow for the simultaneous transmission of quantum and classical signals over the same fiber.

The simultaneous transmission of quantum and classical signals play a important role in the practical application of QKD in the optical networks, even without additional infrastructure, it still enables secure communication. The combination of QKD and

DWDM also promote the development of advanced network architectures, such as Metropolitan area networks (MANs) and Wide Area Networks(WANs). These networks provide confidentiality and integrity of the transmitted data by providing end-to-end secure communication between multiple users. Furthermore, the integration of QKD with DWDM has also facilitated the creation of quantum repeaters, which can extend the range of QKD systems beyond the limits imposed by photon loss in optical fibers. In conclusion, the integration of Quantum Key Distribution with Dense Wavelength Division Multiplexing systems has opened up new possibilities for secure communication in optical networks. By leveraging the unique properties of photons and the multiplexing capabilities of DWDM, QKD can be seamlessly incorporated into existing network infrastructure, providing a robust and scalable solution for ensuring the security of data transmission [8].

QKD in Wireless Networks. Although QKD is primarily associated with optical networks, recent research has explored its application in wireless networks, broadening its potential use cases. One such study demonstrated the feasibility of using QKD in a wireless mesh network based on n+1 EPR pair, compare with traditional EPR protocol, "random space quantum channel selection is exploited in our(their) protocol to improve the probability of revealing Eve."

Wireless mesh networks with QKD integration can provide secure communication in various applications, such as smart cities and the Internet of Things (IoT). In smart cities, QKD can help secure data transmission between interconnected devices, like traffic sensors and surveillance cameras, ensuring the privacy and integrity of collected data. In IoT, due to the rapidly development of quantum computer, "the privacy and security details of the users is eventually being subjected to risks. It is not difficult for a person with technical knowledge to hack any information online. This demands the need for a furthermore secure platform of communication for the users. This is where the QKD comes into play". QKD can protect sensitive information exchanged between smart devices, such as home automation systems and wearable technology, safeguarding user privacy and preventing unauthorized access.

4.2 QKD in Financial Sector

One of the biggest application field of QKD is the financial sector, due to its need for handle sensitive data like detailed information of bank account, personal identity, and transaction record, more security measures must be taken, thus provide a huge stage for QKD. In fact, some banks and financial institutions have already started to implement QKD program in increase the security of their network, such as the SECOQC project in Europe successfully deploy QKD programs that connect multiple banks and financial institutions to achieve secure communication, in Vienna, The traditional encryption methods become more and more vulnerable to quantum computer as continuous development of QKD and quantum computing. As a result, the need for post-quantum cryp-

tographic solutions like QKD grows, in fact, financial institutions are increasingly recognizing the importance of adopting quantum-resistant security measures to protect their networks and data from potential breaches.

4.3 QKD in Medical Sector

Medical sector also faced challenges similar to the financial sector, the popularity of digitization of patient records brings the need for security communication between doctors and patients: patient data, including personal information, medical history, and test results, is highly sensitive and requires protection to maintain patient privacy set by the "Health Insurance Portability and Accountability Act" (HIPAA). Unauthorized access to these information can lead malicious activities. This has been a research topic highly valued by researchers, for example, Lucamarini et al. introduce a "data-sharing system with symmetric encryption for the medical industry" that helps to protect patients' sensitive data from unauthorized wiretapping and tampering, providing secure communication channels that can be used to protect the transmission of electronic health records [9].

Moreover, QKD can be used to protect the communication between medical devices and healthcare information systems: modern technology has brought Internet of Medical Things (IoMT) into people's daily life, like Continuous Glucose Monitoring(CGM), while QKD can prevent this exchange of data from potential attack. In summary, the healthcare industry can greatly benefit from the implementation of QKD technology, as it offers enhanced security for the communication of sensitive patient data. By integrating QKD into various aspects of healthcare, such as EHR sharing and IoMT, the industry can better protect patient privacy and comply with data protection regulations [10].

4.4 Satellite-based QKD

Satellite-based QKD has the potential to enable global secure communication by overcoming the distance limitations of terrestrial QKD systems, which are typically constrained by photon loss in optical fibers. By leveraging the vast coverage of satellite networks, QKD can be extended over long distances, connecting remote locations and facilitating secure communication on a global scale [11].

In 2017, China successfully demonstrated the first satellite-to-ground QKD, using the Micius satellite. The Micius satellite is equipped with a specialized quantum communication payload, which generates entangled photon pairs and transmits them to ground stations. They "achieve a kilohertz key rate from the satellite to the ground over a distance of up to 1,200 kilometres. This key rate is around 20 orders of magnitudes greater than that expected using an optical fibre of the same length. The establishment of a reliable and efficient space-to-ground link for quantum-state transmission paves the way to global-scale quantum networks.". This proves the possibility to establish secure quantum links between the satellite and ground stations, a milestone for the development of global QKD networks. Since the successful Micius demonstration, other

countries and organizations have also started exploring satellite-based QKD. For instance, the European Space Agency has initiated the Quantum Cryptography Telecommunication System project, which aims to develop a European QKD satellite system ."

In conclusion, satellite-based QKD holds great promise for enabling global secure communication by overcoming the distance limitations of terrestrial QKD systems. The successful demonstration of satellite-to-ground QKD using the Micius satellite has marked a significant milestone in the development of global QKD networks and has inspired further research and development in this rapidly evolving field.

5 Conclusion

This research paper explores the application of QKD across various fields. In optical networks, QKD can be smoothly integrated into the existing infrastructure, providing a robust and scalable solution for secure data transmission. Likewise, in Wireless Networks, QKD serves a crucial role in safeguarding sensitive data exchanged between smart devices, such as home automation systems and wearable technology. Utilizing QKD, user privacy is preserved, and unauthorized access is deterred. The paper delves into two industries where QKD can protect sensitive information: the financial and medical sectors. In the realm of finance, various banks and financial institutions have already constructed QKD programs for commercial use, for instance, the Secure Communication based on Quantum Cryptography project in Europe, aimed at establishing secure communication channels. Similarly, in the medical sector, QKD demonstrates immense potential in securing the transmission of Electronic Health Records and ensuring secure communication between medical devices and healthcare information systems.In addition to the above, QKD can be effectively combined with satellite technology. The successful demonstration of satellite-to-ground QKD using the Micius satellite represents a significant milestone in developing global QKD networks. Despite the promising potential of QKD in network security, its practical integration still confronts several challenges. One of the primary difficulties is the necessity of new protocols and hardware to incorporate QKD into the existing network facilities. Besides this, implementing QKD on a large scale can be costly as it demands specialized equipment and resources. In spite of these challenges, the future of QKD remains promising. Researchers are fervently engaged in improving QKD and developing more cost-effective and robust hardware. With the continued growth of quantum technology, it is anticipated that QKD will play a pivotal role in ensuring secure communication amidst emerging quantum threats.

References

1. Bahrami, A., Lord, A., & Spiller, T. (2020). Quantum key distribution integration with optical dense wavelength division multiplexing: a review. IET Quantum Communication, 1(1), 9-15.

2. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, 175-179.
3. Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 68(21), 3121-3124.
4. Dong, J., & Teng, J. (2010). Quantum key distribution protocol of mesh network structure based on n+1 EPR pairs. Journal of Systems Engineering and Electronics, 21(2), 334-338.
5. Ekert, A. K. (1991). Quantum cryptography based on Bell’ s theorem. Physical Review Letters, 67(6), 661-663.
6. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I., & Tittel, W. (2013). Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. Physical review letters, 111(13), 130501.
7. Liao, S. K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., & Pan, J. W. (2017). Satellite-to-ground quantum key distribution. Nature, 549(7670), 43-47.
8. Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature, 557(7705).
9. Ali-Khan, I., Broadbent, C. J., & Howell, J. C. (2007). Large-alphabet quantum key distribution using energy-time entangled bipartite states. Physical review letters, 98(6), 060503.
10. Sangouard, N., Simon, C., De Riedmatten, H., & Gisin, N. (2011). Quantum repeaters based on atomic ensembles and linear optics. Reviews of Modern Physics, 83(1), 33.
11. Shirko, O., & Askar, S. (2023). A novel security survival model for quantum key distribution networks enabled by software-defined networking. IEEE Access, 11, 21641-21654.