Proceedings of the 3rd International Conference on Mathematical Physics and Computational Simulation
DOI: 10.54254/2753-8818/92/2025.21793

A Review of Quantum Key Distribution Technology and Its Applications

Jingyi Chen[1,a,*]

[1]*Beijing University of Posts and Telecommunications & Queen Mary University of London International college, Beijing, 100876, China*
a. 2022213124@bupt.cn
**corresponding author*

Abstract: With the rapid development of information technology, the traditional encryption technology has gradually become fragile. Quantum key distribution (QKD) is based on the principle of quantum mechanics and has absolute security in theory, so it has attracted much attention. This paper emphasizes the importance of QKD in the field of information security. After briefly introducing the principle and practical application process of QKD technology, the differences and application scenarios of classical protocols are compared and analyzed. The applications of QKD in the fields of finance, energy and communication are summarized. In addition, it explores the potential future applications of QKD in healthcare and smart cities, providing valuable insights into the study of QKD technology and its applications.

Keywords: Quantum key distribution, quantum communication, application field, information security

1. Introduction

Since the introduction of the first QKD protocol BB84 by Bennett and Brassard in 1984, QKD technology has made significant progress over the past 30 years, and the future research trend is to integrate deep learning or artificial intelligence techniques into intelligent network management. This paper reviews the application research of QKD from four aspects: basic principle, classic protocol type, application field and future prospect. The key role of QKD in the field of information security is emphasized. This paper compares, summarizes and discusses the current research results in the field of QKD by reviewing the existing literature. It aims to enrich and improve the theoretical framework of quantum information science, lay a theoretical foundation for the development of quantum communication technology, and promote its application in specific fields. This study highlights the value and future application potential of the QKD field.

2. The foundational principles of QKD

QKD is a key distribution technology based on the principle of quantum mechanics, its core is to use the characteristics of quantum states to achieve unconditional security of key sharing. Its basic principle mainly includes the following key points:

(1) Quantum non-cloning theorem: This theorem states that no unknown quantum state can be accurately copied or cloned. This feature ensures that eavesdropper cannot obtain key information by

DOI: 10.54254/2753-8818/92/2025.21793

cloning quantum states during quantum key distribution. When Eve attempts to replicate the photon state in transit, its operation must result in a change in the quantum state, exposing the eavesdropping behavior [1].

(2) Heisenberg's uncertainty principle: This principle states that it is impossible for an observer to accurately measure multiple physical quantities (such as position and momentum) of a particle at the same time. In the QKD protocol, qubits are usually encoded in different ground states. According to Heisenberg's uncertainty principle, measurements of qubits introduce perturbations, especially when the measurement basis is inconsistent with the sending basis. If an eavesdropper attempts to intercept and measure the qubits in transmission, it will inevitably cause changes in the quantum state, thus breaking the confidentiality of the key. Ultimately, the sender and receiver can find out if the communication is being eavesdropped on by comparing a portion of the measurements [1,2].

(3) Quantum entanglement: When two or more quantum systems are in a particular state, their states are closely related, no matter how far apart they are. Once one quantum of an entangled state is measured, the state of the other quantum system is determined instantaneously, a phenomenon known as "non-locality". The role of quantum entanglement in QKD is very important. Quantum states in the BB84 protocol can be encoded through entanglement, making it impossible for eavesdroppers to obtain useful information even if they try to measure quantum states. The "non-locality" nature of entangled states means that measuring the quantum state of one party can immediately affect the state of the other party, thus providing a very strong safeguard mechanism for QKD [1,2].

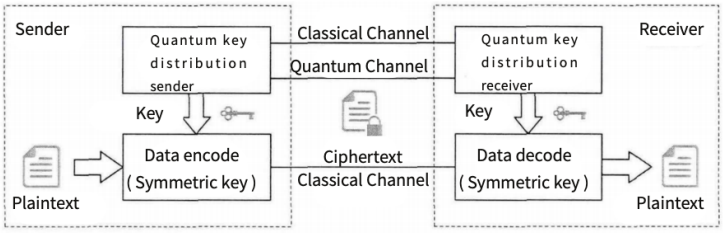

Figure 1: QKD working principle schematic [3].

Unlike traditional communication, the process of quantum secure communication involves two channels, as shown in Figure 1. The quantum channel is used to transmit quantum signals, responsible for delivering and distributing the quantum key to both communicating parties. The classical channel is used to transmit classical signals, facilitating synchronization and key agreement between the sender and receiver. Using the obtained quantum key, the sender encrypts the plaintext with a symmetric encryption algorithm and transmits the ciphertext to the receiver via the classical channel, where it is then decrypted. During this process, any eavesdropping or tampering would result in deviations in the quantum state measurements, which would be detected by the communicating parties, thereby ensuring the absolute security of the communication process [4].

3. The two classical protocal types

The basic goal of the QKD protocol is to generate a shared key for encrypted communication. The protocol specifies how to generate these keys through the transmission of quantum states and ensures the security of the process. QKD protocols can be divided into DV-QKD and CV-QKD. This paper compares the two protocols in Table 1.

DOI: 10.54254/2753-8818/92/2025.21793

Table 1: Comparison table between DV-QKD and CV-QKD

Dimension	DV-QKD	CV-QKD
Core Carrier	Single-photon polarization/phase states	Orthogonal amplitude or phase of optical fields
Typical Protocols	BB84, B92, E91, SARG04, COW	GG02, squeezed-state protocols, multi-dimensional negotiation schemes
Security	Relies on single-photon detection, resistant to PNS requires decoy states	Theoretically secure with Gaussian modulation, requires reverse coordination optimization
Key Rate	kbps range (decreases with distance)	Mbps order (medium and short distance advantage)
Transmission Distance	Laboratory demonstrations up to 833 km, commercial range up to hundreds of kilometers	Typically < 200 km, with gradual improvements
Technical Challenges	Single-photon source generation, low detection efficiency	Noise suppression, efficient coordination algorithms
Application Scenarios	Satellite communication, military secrecy M	Metropolitan networks, data centers

At present, the DV-QKD protocol has experienced many years of experimental verification and technical progress, and the related hardware equipment and experimental schemes have been well optimized and perfected. In addition, the measurement of single photons cannot be perfectly replicated, and any attempt to eavesdrop will destroy the quantum state, so that the communication parties can find it in time, providing absolute security in theory. The transmission distance of DV-QKD is also much greater than that of CV-QKD. In summary, DV-QKD has become the most widely used protocol at present [5]. In Table 2, several well-known protocols of the DV-QKD type are compared and analyzed.

Table 2: Comparative analysis of multiple DV-QKD protocols

Protocal	BB84	B92	E91	SARG04	COW
Security	High (resistant to intercept-resend attacks)	Relatively high (requires only two non-orthogonal states)	Very high (based on entangled states)	High (resistant to photon number splitting attacks)	Medium-high (based on phase reference)
Key Rate	Medium-low	Low	Low	Medium	Medium
Transmission Distance	Long distance (requires relays)	Medium-short distance	Short distance	Medium-long distance	Long distance (fiber-optic suitable)
Application Scenarios	General secure communication, satellite links	Scenarios with simplified preparation	High-security laboratory environments	Scenarios resistant to PNS attacks	Fiber-optic networks, resistant to channel disturbances

DOI: 10.54254/2753-8818/92/2025.21793

Table 2: (continued).

Limitations	Requires single-photon source, low efficiency	Low efficiency, high error rate	Complex entangled source preparation	Requires complex post-processing	High requirements for light source stability

Due to its high security, long transmission distance, high key rate, mature technology and equipment, and low implementation difficulty, BB84 has become the most widely used protocol [6].

4. The application fields and their significance

In the financial sector, with the popularity of online banking and securities trading, the requirements for the confidentiality and integrity of data transmission are constantly increasing. Encrypted communication between financial institutions has become a key means to prevent information leakage and tampering. QKD technology realizes key distribution between different nodes of the bank (such as branches, ATMs, etc.) through quantum channels, and is used to encrypt transaction data. These quantum keys are transmitted through classical channels to the bank's encryption system, further ensuring the security of the data. The advantage of the QKD system is not only real-time eavesdropping detection, any attack that attempts to interfere with the quantum channel will immediately trigger an alarm, the system will automatically discard the current key and generate a new key, but also the combination of hash function and digital signature to ensure the integrity of the data transmission process. The risk of transaction tampering is effectively reduced by 99.9%, and customers' trust in the bank is significantly increased. QKD networks are being built around the world, such as the Beijing-Shanghai Project in China and initiatives in Europe. The construction of these networks provides infrastructure support for the application of QKD in the financial field. Financial institutions can access these networks and use QKD technology to secure key distribution, so as to ensure the security of financial business communication. Multiple financial institutions can achieve secure information interaction through QKD network [7].

In the energy sector, the safety and efficiency of smart grids are equally critical. Power system optical fiber network can carry QKD devices as quantum channel while transmitting traditional power data. QKD nodes transmit authentication keys through quantum channels, and the universal authentication method realizes inter-device authentication through encryption challenges and verification functions, which is suitable for open source and proprietary protocols. For message queue telemetry transmission (MQTT) protocols, message formats and authentication processes are usually designed using QKD keys, quantum random number generators and GMAC algorithms to prevent replay and delay attacks [8]. In addition, to deploy relay stations at key nodes such as substations, the key distribution distance is generally extended by means of trusted relay, optical fiber and satellite communication to ensure the continuity and security of key distribution. Through the quantum channel, the key between the power dispatching center and the substation can be updated in real time, so as to ensure the security of instruction transmission. However, QKD still faces high investment costs when deployed on a large scale. In addition, the quantum channel is sensitive to environmental factors, such as temperature and vibration, so it is necessary to further optimize the stability of the device, such as the use of low-thermal expansion coefficient materials and the introduction of shock-absorbing bracket technology.

In the field of communication networks, the high-speed and low-delay characteristics of 5G put forward higher requirements for communication security. As a quantum-level encryption scheme, QKD technology can effectively resist quantum computing attacks. Combining QKD with 5G

DOI: 10.54254/2753-8818/92/2025.21793

networks can improve network security through a quantum-secure enhanced communication architecture. QKD network consists of infrastructure layer, control layer and application layer. The infrastructure layer consists of QKD nodes and links, which are responsible for generating and storing keys. The control management layer controls and manages the network through the QKD network controller and manager to ensure the normal operation of the network. The application layer provides encryption application services for users and allocates keys according to user requirements. In an NE, a QKD node contains a variety of physical devices, each of which performs a different function. QKD links are used to connect transceivers and are composed of quantum channels and classical channels. In addition, there are key manager links, QKD network controllers and managers, etc., which together support the operation of the network [9]. QKD devices are deployed in key nodes of 5G networks such as core networks, edge computing nodes (MECs), and base stations, and generate keys through quantum state transmission. These keys can be used to encrypt traditional IPSecVPN session keys, forming "classical + quantum" double encryption; Even if the quantum computer successfully breaks the traditional encryption algorithm, the quantum key provided by QKD can still ensure the communication security [10]. Satellite QKD uses satellites as relays to expand the coverage of the QKD network, and China's Micius satellite has carried out relevant experiments. In specific applications, QKD technology shows great potential for secure backtracking between 5G base stations and establishing quantum-encrypted channels between edge nodes and the cloud. These measures effectively prevent man-in-the-middle attacks and ensure the security of user privacy data transmission.

5. The future prospects of QKD applications

The first is the combination of medical data: wireless body sensor networks (WBSN) can remotely monitor patients' health, and hospital information integration platforms (such as electronic medical record systems) can transmit sensitive patient data in real time to medical technology workstations or the cloud via quantum-encrypted routers. However, the transmitted data is vulnerable to attacks, and there are security threats such as data loss and disguised attacks. Traditional password calculation has the ability to resist attacks, but the key transmission is not secure [11]. QKD provides end-to-end quantum encryption for this data, preventing middlemen from eavesdropping or tampering. QKD is deeply integrated with hospital network devices such as quantum encryption routers, and dynamically updates keys using optical fiber or free-space quantum channels to ensure the absolute security of data in transmission links. Through the combination of QKD and 5G/WDM (wavelength division multiplexing) technology, a quantum secure communication channel with low delay and high bandwidth is realized to meet the real-time requirements. The healthcare industry is subject to multiple data protection regulations, and QKD provides theoretically unbreakable encryption capabilities that can help organizations meet regulatory requirements. In the future, in scenarios such as remote surgical guidance and AI-assisted diagnosis, QKD can encrypt high-definition video streams and medical instructions to avoid operational risks caused by network delays or attacks. QKD will be combined with AI-assisted diagnosis and medical blockchain to build a "quantum secure medical cloud" to achieve cross-institutional data security sharing. Miniaturized QKD modules can be integrated into portable medical devices, facilitating the popularization of quantum encryption in pre-hospital emergency care. The challenge facing QKD in the future is that most of the existing medical devices are based on traditional protocols, and QKD-compatible interfaces and middleware need to be developed. There are electromagnetic interference, equipment vibration and other problems in hospital environment, so it is necessary to optimize the anti-interference ability of quantum channel.

QKD can also be combined with the Internet of Things, applied to traffic monitoring in smart cities, sensors in the industrial Internet of things, and device identity authentication through the generated

DOI: 10.54254/2753-8818/92/2025.21793

quantum key to prevent forged node access. Quantum encryption router, as the core component of the Internet of Things access platform, will assign unique quantum keys to massive devices to achieve lightweight security protocols. For example, the data generated by the edge nodes of smart cities needs to be encrypted and uploaded to the cloud in real time, and QKD is combined with the edge computing framework to achieve localized dynamic management of keys. Relying on the fusion quantum secure communication system, the quantum key is obtained to encrypt various terminals, systems and links, and provide technical support for the construction of digital government [12]. In the face of the huge number of devices in the Internet of Things, QKD needs to support efficient key distribution and rotation mechanism, and can use "QKD+ blockchain" technology to record the key life cycle through distributed ledger to improve management efficiency. The research and development of quantum security chip (QSoC) will promote the landing of QKD in smart home, industrial control and other scenarios. Combined with 6G and satellite quantum communication, the "ground and air integration" security coverage of global Internet of Things devices is realized. The combination of IoT and QKD also faces many challenges. Existing QKD devices are bulky and power consuming, making it difficult to embed small IoT terminals. QKD needs to adapt to resource-limited IoT terminals and develop low-energy quantum-secure chips. IoT lacks a unified protocol, so QKD needs to achieve seamless cross-protocol key distribution [13].

6. Conclusion

The research focuses on QKD, a cutting-edge technology that has become a cornerstone of future secure communications. It aims to deepen the understanding of quantum information science and promote the development of the theory. Through the analysis of quantum QKD principle and security mechanism, it lays a foundation for promoting quantum communication and its practical application. A detailed comparison of existing QKD protocols highlights their advantages, limitations, and applicability to a variety of scenarios. By ensuring the confidentiality and integrity of data through quantum mechanics, QKD offers significant advantages in the financial, energy and telecommunications sectors. Going forward, its potential in healthcare and the Internet of Things could redefine security standards. However, challenges remain, including high costs, standardization needs, and compatibility issues. To give full play to the role of QKD, we need to focus on innovation, cost reduction, standard, promote its wide application, and promote the transformation of information security.

References

[1] *Dejing Lin, Baigang Lin. Theory and technology of three major cryptosystems: symmetric cryptography, public key cryptography and quantum cryptography [J]. Telecommunication Technology, 2003(03):6-12.*

[2] *Fei Peng, Zengyao Tian, Xiaohua Zhang, et al. Research on security enhancement method of Power Information System based on quantum security [J]. Journal of Chongqing University, 2019, 47(02):62-74.*

[3] *Yuan Cao. Quantum key distribution network and application of key technology research [D]. Beijing university of posts and telecommunications, 2021. The DOI: 10.26969 /, dc nki. Gbydu. 2021.000142.*

[4] *M. Sasaki. Quantum Key Distribution and Its Applications, IEEE Security & Privacy, vol. 16, no. 5, pp. 42-48, September/October 2018. doi: 10.1109/MSP.2018.3761713.*

[5] *P. Y. Kong. A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security, IEEE Systems Journal, vol. 16, no. 1, pp. 41-54, March 2022. doi: 10.1109/JSYST.2020.3024956.*

[6] *O. Amer, V. Garg and W. O. Krawec. An Introduction to Practical Quantum Key Distribution, IEEE Aerospace and Electronic Systems Magazine, vol. 36, no. 3, pp. 30-55, 1 March 2021. doi: 10.1109/MAES.2020.3015571.*

[7] *Lai J., Yao F., Wang J., Zhang M., Li F., Zhao W., Zhang H. Application and Development of QKD-Based Quantum Secure Communication. Entropy. 2023; 25(4):627. https://doi.org/10.3390/e25040627*

[8] *Alshowkan, M., Evans, P.G., Starke, M. et al. Authentication of smart grid communications using quantum key distribution. Sci Rep 12, 12731 (2022). https://doi.org/10.1038/s41598-022-16090-w*

DOI: 10.54254/2753-8818/92/2025.21793

[9] *Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng and L. Hanzo. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet, IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894, Secondquarter 2022. doi: 10.1109/COMST.2022.3144219.*

[10] *Adnan M.H., Ahmad Zukarnain Z., Harun N.Z. Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions. Future Internet. 2022; 14(3):73. https://doi.org/10.3390/fi14030073*

[11] *V. AD, V. K. Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. Pers Ubiquitous Comput. 2023;27(3):875-885. doi: 10.1007/s00779-021-01546-z. Epub 2021 Mar 18.*

[12] *Chao Leng, Zhongyan Du, Topic Wang, et al. Research on quantum secure communication technology and its application in Smart city [J]. Post and Telecommunications Design Technology, 2023(04):33-37.*

[13] *Jifei Zhang, Chunhong Zhang, Lin Chao. End-to-end encryption transmission algorithm for Internet of Things information based on quantum key distribution [J/OL]. Journal of heilongjiang institute of engineering, 2025, (01): 1-7. https://doi.org/10.19352/j.cnki.issn1671-4679.2025.01.004.*