

Research on the Application of Quantum Encryption Technology in the Industrial Internet

Chenglu Jiang^{1,a,*}

¹*China Agricultural University, Beijing, China*
a. 3095994208@qq.com

**corresponding author*

Abstract: The Industrial Internet offers significant advantages in terms of intelligence and efficiency, playing a crucial role in driving the digital transformation of the industrial economy. Today, the Industrial Internet is increasingly utilized worldwide, bringing substantial benefits to society. However, its application also presents numerous information security challenges. If unresolved, these issues could result in varying degrees of losses. Therefore, it is essential to adopt appropriate methods for encrypting communication signals transmitted within the Internet architecture. Taking the 5G fronthaul architecture as an example, this paper proposes augmenting the passive WDM (Wavelength Division Multiplexer) transmission of communication signals with quantum signal transmission. Quantum encryption technology is employed to encrypt the communication signals initially transmitted via passive WDM. Alice and Bob are implemented in the DU (Distribution Unit) machine room and AAU (Active Antenna Unit) site, respectively, with quantum signal transmission established between them. Using the BB84 protocol in quantum encryption technology, keys are generated to encrypt communication signals, enhancing the security of the entire Internet and mitigating the risks associated with information leakage. This paper explores the specific processes and principles of network architecture and communication signal encryption. It presents a schematic diagram demonstrating the integration of quantum encryption technology into the 5G fronthaul network architecture. Additionally, the paper analyzes the benefits of incorporating quantum encryption technology into network architecture, laying a foundation for the deployment of quantum communication networks and advancing the secure development of the Industrial Internet.

Keywords: Industrial Internet, 5G fronthaul architecture, Quantum cryptography

1. Introduction

Following the financial crisis, a new wave of global industrial reform emerged. The rapid advancement of new information technologies has accelerated their integration into the manufacturing industry, profoundly influencing its development. The Industrial Internet has experienced remarkable growth, with the concept first introduced by General Electric in 2012. As a cornerstone of the Fourth Industrial Revolution, the Industrial Internet represents a critical technology for achieving the digital transformation of the industrial economy. It is a platform designed as a service system that collects, aggregates, and analyzes massive amounts of data to meet the demands of digitalization, networking, and intelligent manufacturing processes [1]. The Industrial Internet's

advantages, including its high intelligence and efficiency, make it essential for driving the digital transformation of the industrial economy. To ensure continued progress, global innovation and development efforts in the Industrial Internet must accelerate, enabling the shift from scale- and cost-based benefits to those focused on quality and efficiency.

As a transformative concept, the Industrial Internet offers substantial benefits and promising development prospects. It seamlessly integrates next-generation information technologies with industrial applications. Industry is one of the leading application domains for the Internet of Things (IoT), where the convergence of industrial control systems (operational technology) and the Internet revolutionizes infrastructures and services. This integration enhances dependability, efficiency, and safety, offering effective real-time solutions, particularly for critical systems [2]. Through comprehensive interconnectivity across devices, systems, factories, regions, and industries, the Industrial Internet enables broader, more efficient, and precise optimization of production and service resources. This, in turn, supports the transition of the industrial economy from reliance on scale and cost advantages to a focus on quality and efficiency [3]. However, the Industrial Internet is not without its challenges, particularly in the realm of security. Its security concerns can be categorized as follows:

Equipment Security: The transition from mechanization to high intelligence in industrial equipment has introduced a new paradigm comprising embedded operating systems, microprocessors, and application software. This evolution exposes numerous intelligent devices to network attacks, increasing the attack surface, the speed of diffusion, and the impact of vulnerabilities.

Control Security: The high integration of industrial control systems (ICS) with networks renders them susceptible to cyberattacks. Attackers can exploit system permissions, alter engineering data, disrupt control processes, or even shut down on-site equipment using vulnerabilities or malware, potentially causing severe production accidents and economic losses.

Network Security: The interconnected nature of Industrial Internet systems makes them prime targets for network attacks. Exploiting network vulnerabilities, attackers can gain access to servers, extract critical enterprise information, and even penetrate control networks to manipulate instrument settings, resulting in production incidents.

Data Security and Privacy: The Industrial Internet handles vast amounts of sensitive data, including production processes, product designs, and customer information. Data breaches can lead to significant corporate losses and may also jeopardize national security.

Supply Chain Security: The Industrial Internet ecosystem often involves numerous suppliers and partners. Vulnerabilities at any point in the supply chain can be exploited, compromising the security of the entire system.

Among the security challenges facing the Industrial Internet, the most prominent is the issue of information security within the network architecture. Wherever information is transmitted, the potential for information leakage exists. For instance, a technical channel for voice information leakage can occur in optical fiber communication due to parasitic modulation in the optical flow of conventional connection systems [4]. Currently, companies often rely on distributed systems and networked communication facilities to transmit critical information that requires protection. As a result, safeguarding enterprise information has become increasingly critical, making information security an essential aspect of industrial maintenance. Information security refers to the measures taken to protect hardware, systems, and the use, storage, and transmission of data, ensuring the integrity, confidentiality, and availability of information and operational programs [5]. Operational Technology (OT) networks and devices—comprising all components used in industrial environments—were not originally designed with security as a priority. Instead, efficiency and ease of use were the primary design considerations. However, with the digitization of industry, an increasing number of devices and industrial networks are now connected to public networks. While this connectivity benefits the administration and organization of industrial environments, it also

significantly expands the attack surface, providing potential entry points for attackers. Previously, accessing production networks typically required breaching an Information Technology (IT) perimeter, such as a public website, before moving laterally to Industrial Control Systems (ICSs) to affect the production environment [6]. This article focuses on the narrower aspect of information security protection, rather than hardware protection. In this context, 5G technology plays a pivotal role in advancing the Industrial Internet. It is a key tool for new infrastructure construction and serves as an essential supporting technology to facilitate the digital transformation of small and medium-sized enterprises through cloud access. Regional-level Industrial Internet platforms can offer cost-effective digital transformation solutions, enhancing management efficiency, reducing production control costs, and improving the overall competitiveness of enterprises. Additionally, such platforms enable local governments to enhance governance and service capabilities by leveraging data [7]. In industrial production, the growing volume of production data necessitates mass data transmission and processing. 5G, a cutting-edge communication technology, combines Ultra-Reliable Low Latency Communication (uRLLC) with Multi-access Edge Computing (MEC) to meet these demands. This combination provides substantial potential for services requiring higher bandwidth, lower latency, and increased computational capacity. The Local Area Network (LAN)-type service supported by the 5G system reduces network distance, further decreasing latency and improving data security [8]. Thus, 5G is closely intertwined with the Industrial Internet. The integration of 5G and the Industrial Internet not only enhances data transmission efficiency but also strengthens security.

The primary innovation of this paper is the application of the 5G forward transmission architecture as an example. Building on the original passive Wavelength Division Multiplexing (WDM) transmission for communication signals, this approach introduces quantum signal transmission between the DU machine room and the AAU base station. By utilizing quantum encryption technology to generate encryption keys for communication signals, this architecture enhances security. This paper will first provide a brief overview of the BB84 quantum encryption protocol employed in this approach. Subsequently, it will present a detailed diagram of the 5G forward transmission architecture, explaining the specific role and principles of quantum encryption technology within this framework. The advantages of incorporating quantum encryption technology into passive WDM communication signal transmission will also be analyzed. Finally, the paper includes the formula for the quantum key rate, offering readers a means to evaluate the effectiveness of the quantum key rate.

2. Related Works

In recent years, the Industrial Internet has been booming at an unprecedented speed, injecting a steady stream of strong momentum into the process of new industrialization. The policy framework for the Industrial Internet continues to improve, the proportion of industrial categories covered is steadily increasing, and the scale of applications is rapidly expanding. Simultaneously, the support provided by digital infrastructure has seen continuous enhancement. Digital infrastructure is a prerequisite for promoting the digital, networked, and intelligent development of the manufacturing industry. Globally, efforts are accelerating in the construction of broadband networks, 5G base stations, industrial virtual networks, and other infrastructure to achieve extensive connectivity and efficient management of industrial equipment. The market scale of the Industrial Internet is consistently expanding, positioning it as a new engine for driving high-quality economic development. As a critical component of the Industrial Internet, industrial Internet platforms are also undergoing development, application, and improvement. These platforms play a vital role in promoting the digital transformation of the manufacturing industry and advancing the digitalization of all aspects of production and operations. The integrated application of the Industrial Internet is deepening, with application scenarios extending from isolated uses in “research, production, supply, marketing, and

service” to comprehensive integration. Currently, the Industrial Internet is widely applied in key industries such as electronic equipment manufacturing, equipment manufacturing, steel, and mining, resulting in typical application scenarios like machine vision quality inspection, predictive maintenance of equipment, and intelligent factory logistics. Simultaneously, the Industrial Internet has driven the high-end, intelligent, and green development of the manufacturing sector, providing essential support for the deep integration of the real economy and the digital economy.

In parallel, quantum communication technology has also advanced rapidly in recent years, merging quantum mechanics and information science to achieve absolutely secure communication that cannot be intercepted or cracked. Quantum networks represent a paradigm shift in communication as they leverage the principles of quantum physics to enable efficient and secure data transfer [9]. Quantum communication can be categorized into two forms: quantum key distribution (QKD) and quantum teleportation. QKD exploits the no-cloning properties of quantum states to generate binary codes, ensuring the confidentiality of classical communication. This technology has already entered the industrialization stage. Communication security must evolve to counter the massive computational power of emerging quantum computers. Quantum secure direct communication (QSDC) is a promising branch of quantum communication, offering provable security and overcoming the threats posed by quantum computing, while directly conveying secret messages via a quantum channel [10]. Quantum teleportation, on the other hand, uses quantum entanglement to directly transmit quantum bits. Although still in the basic research stage, it is expected to enable direct communication between quantum computers in the future.

The Industrial Internet platform generates vast amounts of data, which must also be securely transmitted and processed. To enhance the security of information transmitted through the Industrial Internet, quantum communication technology offers a highly effective solution.

3. BB84-QKD

Quantum cryptography is a prominent and well-researched field, particularly in response to the emergence of quantum computing platforms. The BB84 quantum key exchange protocol, first proposed in 1984, has since inspired further developments, including the E91 and B92 protocols [11]. The BB84 protocol represents a significant milestone in quantum cryptography, developed by physicist Charles Bennett and cryptographer Gilles Brassard. It leverages the unclonable and measurable collapse properties of quantum states to provide a secure and reliable method of key distribution between communication parties.

In the BB84 protocol, information transmission relies on the polarization states of photons. The sender transmits a series of carefully prepared photons to the receiver via a quantum channel, with each photon in a specific polarization state representing key information. The receiver randomly selects a measurement basis (such as horizontal/vertical or diagonal) to measure the incoming photons and records the results. Only the measurements where both parties have selected the same basis are retained as the original key. Subsequently, both parties perform information reconciliation and secure amplification through classical channels to correct errors and reduce the potential information available to eavesdroppers, ultimately producing a secure shared key. The unclonability of quantum states ensures that any interception or replication attempt alters the state of the photons, thereby alerting both communicating parties.

The protocol execution involves several steps, including signal transmission, random measurement, basis comparison and filtering, as well as information reconciliation and secure amplification. Through these steps, the parties generate a secure and reliable shared key, which can be used for subsequent encrypted communication. The security of the BB84 protocol is founded on the fundamental principles of quantum physics, enabling it to resist various classical and quantum eavesdropping attacks. Furthermore, the protocol offers advantages such as ease of implementation

and the absence of requirements for quantum state storage, making it widely adopted in the field of quantum secure communication. As quantum technology continues to advance, the BB84 protocol will remain a critical tool for ensuring information security.

4. The Application of Quantum Security Technology in 5G Fronthaul Architecture

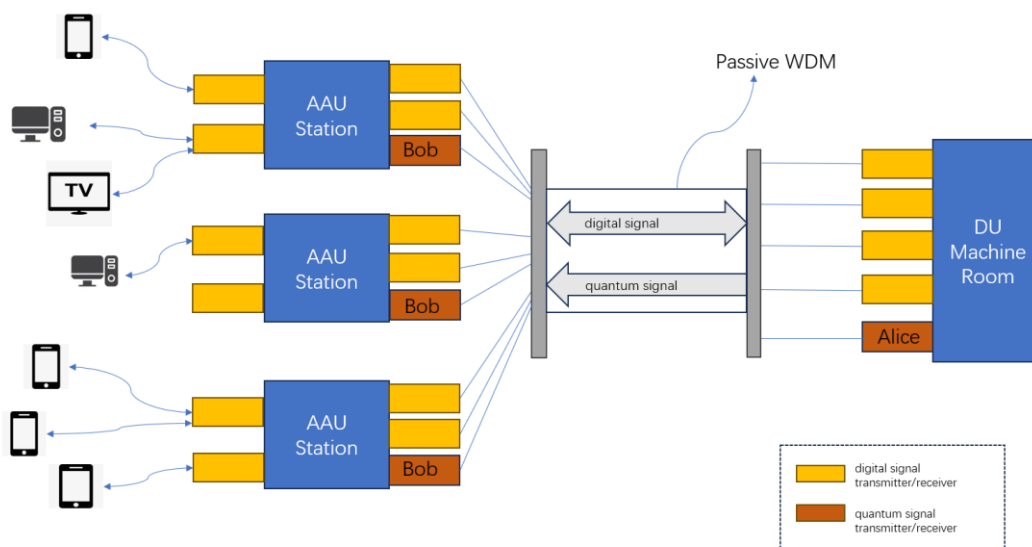


Figure 1: The Application of Quantum Security Technology in 5G Fronthaul Architecture.

The 5G fronthaul technology solutions include fiber optic direct connection, passive WDM, active WDM/OTN, and Slice Packet Network (SPN), among others. Among these, passive WDM offers advantages such as increased fiber optic transmission capacity, reduced construction costs, and improved system flexibility, making it the primary method for constructing 5G fronthaul networks. This framework is primarily based on passive WDM, with quantum encryption technology added to enhance the limited protection capabilities of passive WDM networks.

The architecture diagram includes three main components: the DU site, the AAU site, and the user end. Among these, DU sites are the least numerous, AAU sites are intermediate in number, and user devices, such as mobile phones and computers, are the most numerous. The DU site primarily aggregates all signals, while the AAU site functions as a sub-base station, each connected to multiple user devices. Between DU and AAU sites, there are two types of transmission signals: communication signals and quantum signals. Communication signals are bidirectional, while quantum-encrypted signals are unidirectional. Both types of signals are transmitted via passive WDM; however, their transmitters and receivers operate independently. Transmission signals between the AAU site and the user end are bidirectional communication signals. Given the large volume of communication signals transmitted between DU and AAU sites, it is essential to encrypt these signals effectively.

The encryption method for information transmission between the DU and AAU sites relies on the BB84 protocol in quantum encryption communication technology. The primary encryption process is as follows: Assume that the quantum signal transmitter at the DU site is A, and the quantum signal receivers at the AAU site are B1, B2, B3, and so on. First, A randomly generates a sequence of 0s and 1s, selects the corresponding basis based on the arrangement of the 0s and 1s, determines the polarization state of the photons, and emits the photons (one photon at a time). For each photon emitted by A, B randomly selects a basis. Upon receiving a photon, B performs basis pairing. If the pairing is successful, the corresponding number (0 or 1) is recorded. Since A emits multiple photons

over time, B can accumulate successful pairings and ultimately generate a secure key. Moreover, the keys generated by B1, B2, B3, etc., are unique, ensuring that the leakage of a key from one AAU site does not compromise the keys of other sites. This method significantly enhances the security of information transmission between base stations.

In summary, applying quantum key technology to the 5G fronthaul architecture provides several advantages. On one hand, A continuously sends photons, and B can accept photons for basis pairing at any time, improving the efficiency of key generation. The key capacity is substantial, and the unique keys generated by each AAU prevent the leakage of one key from affecting others, ensuring high security. On the other hand, because this architecture builds on the existing passive WDM communication signal transmission framework, with the addition of Alice and Bob components, the upgrade costs are low and do not require extensive modifications.

5. Secure Key Rate Analysis

As previously mentioned, introducing quantum encryption technology into network architecture provides the advantages of large capacity and high key generation efficiency. To facilitate the application and evaluation of quantum encryption technology in the actual industrial Internet network architecture, this paper briefly outlines the key rate analysis method:

The lower limit S of the secure key quantity for the BB84 protocol is expressed as:

$$S \geq Q_{\mu} \{-H_2(e_{\mu}) + \Omega[1 - H_2(e_1)]\} \quad (1)$$

When photons are emitted from the DU site, the key rate cannot reach 100% due to factors such as quantum channel attenuation, detection efficiency, photon counting rate, and quantum bit error rate. Below is a brief analysis of the key rate:

The attenuation of a fiber optic quantum channel is exponential. Assuming the attenuation coefficient of the quantum channel between A and B is α dB and the length is l km, the attenuation between the two is:

$$t_{AB} = 10^{-\frac{\alpha l}{10}} \quad (2)$$

Assuming the detection efficiency of B is η_D , the probability that photons sent from the DU site are detected by the AAU station is:

$$\eta = t_{AB} \eta_D \quad (3)$$

Since single-photon detectors in the infrared band cannot distinguish the number of photons, the probability of B producing a detection result when A sends an n -photon state is:

$$\eta_n = 1 - (1 - \eta)^n \quad (4)$$

Let Y_n represent the conditional probability that B produces a detection result when A emits an n -photon state. Y_0 is the background count rate, which accounts for the counts at B when A emits a vacuum state. This background count is primarily caused by the detector's dark counts and other background noise. The n -photon states detected by B mainly originate from two sources: signal states and background noise. Assuming that the background noise is independent of the signal state, we have:

$$Y_n = Y_0 + \eta_n - Y_0 \eta_n \approx Y_0 + \eta_n = Y_0 + 1 - (1 - \eta)^n \quad (5)$$

Quantum bit error rate: Let e_{Det} be the probability of erroneous detection results caused by signal light. Then, the total error rate is:

$$E_{\mu} Q_{\mu} = e_0 Y_0 + e_{Det} (1 - e^{-\eta \mu}) \quad (6)$$

Since background light is generally considered completely random, $e_0=1/2$.

Using the above methods, we can calculate the secure key rate, evaluate the performance of Quantum Key Distribution (QKD), and assess how integrating quantum encryption technology with the 5G fronthaul architecture enhances the security of the industrial Internet.

6. Conclusion

Given the current prevalence of information leakage in industrial Internet architectures, this paper proposes a scheme to integrate quantum encryption technology into passive WDM network architectures. It provides a schematic diagram and a detailed introduction to the application of quantum security technology in 5G front-end architectures, while analyzing the advantages of combining quantum encryption technology with network architectures. Although this study focuses on the 5G front-end architecture as an example, quantum encryption technology can be adapted and applied to other network architecture systems as needed. In the industrial Internet sector, information exchange between signal receivers and transmitters occurs within the Internet network architecture. The proposed system can be effectively applied to various network configurations, significantly enhancing the security of signal transmission and improving the efficiency of key generation. Additionally, quantum encryption technology can be incorporated into the existing architecture without requiring modifications to the original communication signal transmission methods, thereby reducing the cost of system upgrades.

References

- [1] Wang, Q., Ma, G., He, S., Huang, Q., & Gu, W. (2020). *Industrial intelligent optimization system based on industrial Internet platform*. 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 523–526. <https://doi.org/10.1109/ICSESS49938.2020.9237724>
- [2] Serpanos, D. (2024). *Industrial Internet of Things: Trends and challenges*. *Computer*, 57(1), 124–128. <https://doi.org/10.1109/MC.2023.3331552>
- [3] Zhang, H. (2023). *Research status and prospect of industrial Internet based on cloud computing and the Internet of Things*. 2023 IEEE 7th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 47–51. <https://doi.org/10.1109/ITOEC57671.2023.10292061>
- [4] Grishachev, V., Kalinina, Y., & Kazarin, O. (2019). *Fiber-optic channel of voice information leakage*. 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, Russia, 1512–1514. <https://doi.org/10.1109/EIConRus.2019.8656670>
- [5] Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). *Information security: A review of information security issues and techniques*. 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–6. <https://doi.org/10.1109/CAIS.2019.8769504>
- [6] Anton, S. D. D., Fraunholz, D., Krohmer, D., Reti, D., Schneider, D., & Schotten, H. D. (2021). *The global state of security in industrial control systems: An empirical analysis of vulnerabilities around the world*. *IEEE Internet of Things Journal*, 8(24), 17525–17540. <https://doi.org/10.1109/JIOT.2021.3081741>
- [7] Zhang, H., Ouyang, X., Wang, Y., & Zhao, W. (2022). *A new architecture of regional-level industrial Internet platform based on a 5G network*. 2022 2nd International Conference on Networking Systems of AI (INSAI), Shanghai, China, 175–179. <https://doi.org/10.1109/INSAI56792.2022.00041>
- [8] Jia, Z., Li, D., Zhang, W., & Pang, L. (2020). *5G MEC gateway system design and application in industrial communication*. 2020 2nd World Symposium on Artificial Intelligence (WSAI), Guangzhou, China, 5–10. <https://doi.org/10.1109/WSAI49636.2020.9143280>
- [9] J. K. S., & S. G. C. (2023). *Quantum network for quantum communication*. 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 1–5. <https://doi.org/10.1109/CSITSS60515.2023.10334148>
- [10] Pan, D., et al. (2024). *The evolution of quantum secure direct communication: On the road to the Qinternet*. *IEEE Communications Surveys & Tutorials*, 26(3), 1898–1949. <https://doi.org/10.1109/COMST.2024.3367535>
- [11] Nguyen, T.-T., Khac, T.-L. V., & Luc, N.-Q. (2023). *Simulation of the BB84 quantum key exchange protocol*. 2023 15th International Conference on Knowledge and Systems Engineering (KSE), Hanoi, Vietnam, 1–4. <https://doi.org/10.1109/KSE59128.2023.10299471>