Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/119/2025.21529

# 6G Fronthaul Network Architecture Based on Quantum Technology: Integration of QKD with Passive WDM

**Yongkang Zhang**[1,a,*]

*[1]Chongqing University, Shapingba District, Chongqing, 400044, China*
*a. 20223909@stu.cqu.edu.cn*
**corresponding author*

***Abstract:*** The rapid evolution of mobile communication technology is propelling us from the era of 5G to the cusp of 6G, which promises ultra-high speeds, ultra-low latency, and seamless global connectivity. However, these ambitious goals require not only significant advancements in traditional communication technologies but also the integration of novel approaches to address emerging security and efficiency challenges. Quantum communication, particularly Quantum Key Distribution (QKD), offers a groundbreaking solution due to its inherent security based on the principles of quantum mechanics. This paper proposes an innovative architecture that combines QKD with Passive Wavelength Division Multiplexing (WDM) for 6G fronthaul networks. The architecture, which includes components for signal transmission, processing, and monitoring, uses WDM to transmit both quantum signals and classical signals over a single fiber, optimizing resource utilization, ensuring security, and enhancing reliability. The quantum signals are detected by single-photon detectors to generate secure keys, while the classical signals carry regular communication data. The passive WDM system efficiently uses fiber resources, is cost-effective, and is easy to upgrade, making it highly compatible with classical optical communication. Extensive simulation experiments are conducted to evaluate the impact of key parameters such as transmission distance, attenuation coefficient, photon count per pulse, dark count rate, and detection efficiency on the secure key rate and quantum error rate. The results indicate that careful optimization of these parameters can substantially enhance system performance, making the architecture highly suitable for high-security transmission scenarios in 6G networks. This research provides new insights into the integration of quantum and classical communications in 6G fronthaul networks, demonstrating the potential of quantum-enhanced 6G networks.

***Keywords:*** 6G, Quantum Key Distribution (QKD), Passive Wavelength Division Multiplexing (WDM), Security, Fronthaul Network

## 1. Introduction

5G, the fifth generation of mobile communication technology, has emerged as a transformative force in the digital landscape, revolutionizing the way we interact with digital devices and services [1]. It represents a significant leap from previous generations, offering ultra-high speeds, low latency, massive connectivity, and extensive coverage [2]. These characteristics enable 5G to support a seamless network experience, meeting the demands of numerous data transmission and real-time response applications as the next generation of mobile communication technology [3]. For instance, in intelligent transportation, 5G facilitates real-time communication between vehicles and traffic management systems, improving road safety and traffic flow. In remote healthcare, 5G allows for high-definition video conferencing and real-time data transmission, enabling doctors to diagnose and treat patients remotely [4][5].

In comparison to 5G, 6G, the sixth generation of mobile communication technology, is a more advanced and next-generation mobile communication system whose scope will far exceed that of traditional communication [6]. 6G builds upon the solid foundation laid by 5G while introducing numerous groundbreaking innovations and enhancements [7]. It is poised to become the core of future digital ecosystems, offering unprecedented levels of connectivity, intelligence, and responsiveness, and facilitating seamless integration of diverse technologies such as the Internet of Things (IoT), artificial intelligence (AI), and autonomous vehicles. In doing so, 6G will drive society toward greater interconnectedness, intelligence, and responsiveness [8].

The key characteristics of 6G include ultra-high speeds and ultra-low latency, ensuring real-time communication and interaction; massive connectivity, suitable for dense urban environments and large-scale IoT deployments; seamless coverage, eliminating dead zones and ensuring global user connectivity; support for emerging applications such as holographic communication, augmented and virtual reality, and intelligent transportation systems, transforming industries and enhancing user experiences; and enhanced security, providing a safer and more resilient communication network through the integration of advanced cryptographic techniques and AI-driven security measures [9]. The enhanced security aspect of 6G is a critical area of focus, with numerous studies exploring potential threats and countermeasures [10].

6G emphasizes global connectivity, aiming to create a truly interconnected world; supports emerging technologies, fostering innovation and enabling new business models; features more intelligent and automated networks, leveraging AI to optimize performance, predict and prevent failures, and enhance user experiences; supports a wider range of applications, including those requiring ultra-low latency, high reliability, and massive connectivity—such as autonomous vehicles, remote surgery, and industrial automation; and offers improved spectral efficiency, increasing data throughput through advanced modulation and coding techniques. In summary, 6G represents a leap forward in mobile communication technology, offering unparalleled levels of connectivity, intelligence, and responsiveness. It is poised to revolutionize industries, enhance user experiences, and promote a more interconnected and intelligent world [6]. Additionally, research into patterns and architectures for IoT security, which is crucial for 6G's success, has seen significant advancements in recent years [11].

Quantum communication, a cutting-edge and revolutionary communication method grounded in the intricate principles of quantum mechanics, introduces an unparalleled paradigm shift in the realm of secure and efficient data transmission [7]. This advanced form of communication boasts several distinctive advantages, including exceptional security, robust anti-jamming capabilities, and unprecedented transmission speeds. It primarily encompasses two major classifications: Quantum Key Distribution (QKD) and Quantum Teleportation, each offering unique benefits and applications.

QKD, in particular, stands as a cornerstone for achieving remarkable secure communication. By leveraging the fundamental principles of quantum mechanics, specifically the no-cloning theorem, QKD enables two parties to generate a shared, secret key that is inherently resistant to eavesdropping. The no-cloning theorem asserts that it is impossible to create an exact copy of an unknown quantum state, ensuring that any attempt to intercept the key would disrupt the quantum state and be immediately detectable. This intrinsic property of quantum mechanics forms the bedrock of QKD's unparalleled security, making it indispensable for industries that require the highest levels of data confidentiality and integrity.

DOI: 10.54254/2755-2721/119/2025.21529

Moreover, quantum communication offers significant advantages in terms of transmission speed and anti-jamming capabilities [7]. Unlike classical communication methods, which are susceptible to various forms of interference and eavesdropping, quantum communication utilizes quantum states to transmit information in a manner that is inherently resistant to these threats. This ensures that data can be transmitted quickly and securely, even in environments with high levels of noise and interference. The potential applications of quantum communication are vast and varied. In the realm of confidential communication, QKD can be used to establish secure communication channels that are impervious to even the most sophisticated cyberattacks [11]. In distributed quantum computing, quantum communication enables multiple quantum processors to communicate and collaborate efficiently, paving the way for the development of powerful and scalable quantum computing systems. Additionally, quantum communication has the potential to revolutionize the field of IoT security by providing secure and efficient data transmission between interconnected devices.

## 2. Related Works

In the realm of 5G security, several recent studies have highlighted the challenges and opportunities in ensuring the security and privacy of this advanced communication technology. One such study emphasizes the importance of embedding security capabilities from the outset of 5G architecture definition and standardization. It discusses the need for security requirements to permeate through the different layers of 5G systems—physical, network, and application layers—within a risk management framework that accounts for evolving security threats [12]. Furthermore, a comprehensive review has been conducted on the security and privacy issues in 5G-powered IoT applications [5]. This review examines the current security status of 5G IoT and summarizes potential research avenues, underscoring the importance of implementing strong security measures to counteract emerging threats.

As the transition from 5G to 6G progresses, the security paradigm becomes increasingly intricate and dynamic. While 5G has established a robust foundation for secure communications, 6G introduces novel challenges and opportunities due to its integration of pioneering technologies, including AI, visible light communication (VLC), and quantum computing. These advancements, although promising, introduce new vulnerabilities that require careful addressing. Specifically, advanced wireless technologies such as non-orthogonal multiple access (NOMA), multi-access edge computing (MEC), millimeter-wave (mmWave), massive multiple-input and multiple-output (MIMO), VLC, terahertz (THz) communication, and reconfigurable intelligent surfaces (RIS) introduce vulnerabilities to physical-layer attacks and privacy breaches. Concurrent research underscores the pivotal role of promising 6G technologies—such as AI, network slicing, blockchain, edge computing, and THz communication—in fortifying the security of the Internet of Vehicles (IoV) [13].

In the domain of 6G security, several pivotal contributions have emerged, addressing the unique challenges posed by this next-generation technology. A prominent study explores the literature concerning security, privacy, and trust issues within 6G wireless communication [10]. This work identifies crucial challenges associated with the integration of artificial intelligence and visible light communication, advocating for innovative paradigms to offer definitive 6G security solutions. Moreover, another comprehensive review addresses the security and privacy challenges in 6G networks, with a particular emphasis on the integration of distributed ledger technology (DLT), physical layer security, distributed AI/ML, VLC, THz communication, and quantum computing [10]. This paper introduces a threat model tailored for 6G cellular networks and proposes countermeasures and authentication methodologies to enhance security.

Significant progress has also been made in research on 5G and 6G security. The China Unicom Research Institute released a white paper emphasizing the security challenges of 5G and the role of

DOI: 10.54254/2755-2721/119/2025.21529

the Network Data Analytics Function (NWDAF). The China Communications Standards Association proposed a security enhancement plan for 5G dedicated networks. China Mobile led the completion of the ITU-T 6G security project, promoting the development of relevant technologies. In addition, China Telecom, in cooperation with ZTE and others, has made contributions to the security of 5G dedicated networks, with related proposals having been approved by international standards organizations.

## 3. Integration Architecture of QKD with Passive WDM

In existing fronthaul network architectures, passive WDM technology is widely used. This technology employs passive multiplexer/demultiplexer (MUX/DEMUX) devices to combine multiple optical signals into a single optical fiber for transmission, addressing issues related to insufficient fiber optic resources and cost control. The passive WDM system comprises two main components: the passive MUX/DEMUX and colored optical modules. Since MUX/DEMUX are passive devices that require no power supply, colored optical modules operating at different wavelengths are utilized on both the distributed unit (DU) and active antenna unit (AAU) sides. On this basis, we propose a method to integrate Quantum Key Distribution (QKD) with passive WDM, referred to as the "6G fronthaul network architecture based on quantum technology."

Passive WDM technology has been widely employed in existing fronthaul network architectures. Compared to active WDM systems, passive WDM systems offer several advantages in terms of cost and maintenance. They do not require an external power supply and have a relatively simple equipment structure, which reduces failure points and maintenance costs. However, passive WDM systems may present challenges in signal quality control and scalability, such as signal attenuation and crosstalk, which can be more difficult to manage in long-distance transmissions or complex network topologies. Additionally, expanding network capacity may necessitate hardware replacement, reducing flexibility.

In contrast to architectures that do not use quantum communication, QKD provides enhanced security by ensuring absolute security in the key distribution process through the principles of quantum mechanics, effectively resisting potential threats such as future quantum computing attacks. However, the introduction of QKD may increase the complexity and cost of the system. This includes the need for additional quantum channels, single-photon detectors, and other equipment, as well as the requirements for quantum signal processing and synchronization technologies. While this increases the difficulty of system deployment and operation. However, considering the urgent need for high security in 6G networks, the trade-off is justified. The core of this method lies in leveraging WDM technology to multiplex quantum signals and classical signals onto the same optical fiber for transmission, thereby conserving fiber optic resources and enhancing security.

Specifically, wavelength division multiplexing technology involves careful wavelength selection, where quantum signals typically operate at the 1310 nm wavelength and classical signals use the 1550 nm wavelength, effectively preventing quantum signals from being overwhelmed. Additionally, high-isolation WDM devices and advanced filtering techniques are employed to allow quantum signals to bypass splitters at optical branching points, minimizing loss and significantly reducing interference from classical signals.

The architecture consists of several key components: The AAU is responsible for signal transmission and reception, converting data from optical fibers into wireless signals for transmission, while simultaneously receiving signals from user equipment such as mobile phones. It integrates antenna and radio frequency processing functions and supports advanced 5G technologies like Massive MIMO. The DU handles the baseband processing of signals, performing preliminary processing on received signals before transmitting them to the next processing unit via optical fibers. The output multiplexer unit (OMU) combines multiple optical signals of different wavelengths into

DOI: 10.54254/2755-2721/119/2025.21529

a single composite optical signal for transmission, while the optical demultiplexer unit (ODU) separates the composite optical signal back into its original optical signals of different wavelengths at the receiving end. The boosting amplifier (BA) is located at the transmitting end to boost the transmission power of optical signals. The link amplifier (LA) is positioned in the middle of the optical fiber link to compensate for signal attenuation, and the pre-amplifier (PA) is situated at the receiving end to enhance the strength of the received optical signals. Additionally, the optical supervisory channel (OSC) transmits supervisory information through optical fibers, providing key parameter data about the optical signals.

In the architecture integrating QKD with passive WDM, both quantum and classical signals are transmitted. Two types of signals, initially processed on the AAU side, are introduced into the architecture through the optical transform unit. These signals are then combined by the MUX at the front of the passive WDM channel. In the middle of the channel, the BA, LA, and PA are employed sequentially to ensure the strength and reliability of the two signals. Finally, the ODU at the end of the channel separates the mentioned signals and directs them to the side of DU.

Quantum signals, utilizing photon polarization for key distribution, are sent at the 1310 nm wavelength through quantum channels and measured at the receiving end using single-photon detectors. Subsequently, operations like basis reconciliation and key error correction are carried out through classical channels to produce secure quantum keys. Meanwhile, classical signals (uplink signal and downlink signal), carrying conventional communication data, are transmitted at the 1550 nm wavelength. The passive nature of the WDM system ensures that classical signal transmission remains unaffected by quantum signals, efficiently utilizing fiber optic resources.

The architecture integrating QKD technology, based on the principles of quantum mechanics, offers unconditional security and high compatibility with classical optical communications. Additionally, passive WDM systems, which operate without a power supply and use passive optical combiners/splitters (OMUX/ODU) for wavelength multiplexing and demultiplexing, are well-suited for short-distance (<10 km) point-to-point, ring, star, and other networking scenarios. These systems conserve fiber optic resources, enhance transmission efficiency, and are widely used in existing 5G fronthaul due to their practicality and ease of upgrading.

While 6G aims to achieve global connectivity and support long-distance transmission, the proposed architecture focuses on short-distance scenarios for several reasons. First, short-distance networks are critical for dense urban environments and large-scale IoT deployments, where high connectivity and low latency are essential. Second, the integration of QKD with passive WDM in short-distance scenarios provides a secure and cost-effective solution that can be easily upgraded and deployed. This approach serves as a foundational step towards achieving broader 6G goals, while addressing the immediate needs of high-density and high-security applications.

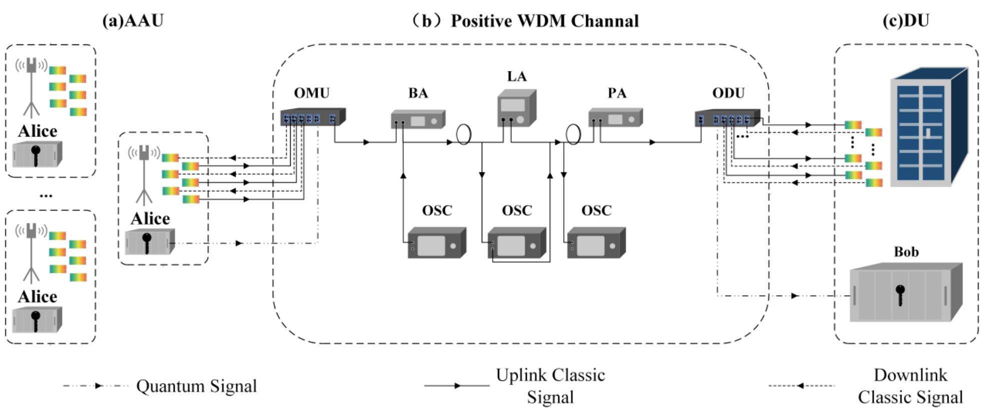


Figure 1: 6G Fronthaul Network Architecture Based on Quantum Technology

DOI: 10.54254/2755-2721/119/2025.21529

# 4. Simulate Experiment

In investigating the performance of 6G fronthaul network architectures based on quantum technology systems, particular attention was given to the QKD component. A series of simulations were conducted using the MATLAB platform to analyze the performance of this component in depth. The experimental environment was programmed in MATLAB to simulate a real QKD transmission scenario, covering key parameters such as transmission distance, attenuation coefficient, detection time, average photons per pulse, dark count, detection efficiency, optical bit error rate, and error correction efficiency. Default values for these parameters were set based on typical experimental conditions and device performance, such as a detection time of 2.01 ns, an operating frequency of 193.4 THz, and an effective area of 70 μm².

For this component, secure key rate (SKR) and quantum bit error rate (QBER) are two key indicators for measuring performance evaluation. The SKR represents the number of key bits that a QKD system can generate and securely transmit per unit of time, which directly reflects system efficiency and practicality. A higher SKR indicates that the system can generate more keys in a shorter period, better meeting the security needs of high-bandwidth communication. On the other hand, QBER refers to the proportion of erroneous bits to the total transmitted bits, typically expressed as a percentage. A lower QBER indicates higher key quality and security, which not only reduces the complexity of post-processing, but also ensures the reliability of the key distribution process.

Through the systematic adjustment of key parameters, a deeper understanding of their impact on the SKR and QBER was achieved, providing a theoretical basis and experimental guidance for optimizing the QKD system design. Transmission distance is a critical factor, as it is directly correlated with photon attenuation within the fiber. From the trend of the curves in Figure 2 (a) and Figure 2 (b), it is clearly evident that as the transmission distance increases, photon loss intensifies, leading to a concomitant rise in the error rate and a decline in the key generation rate.

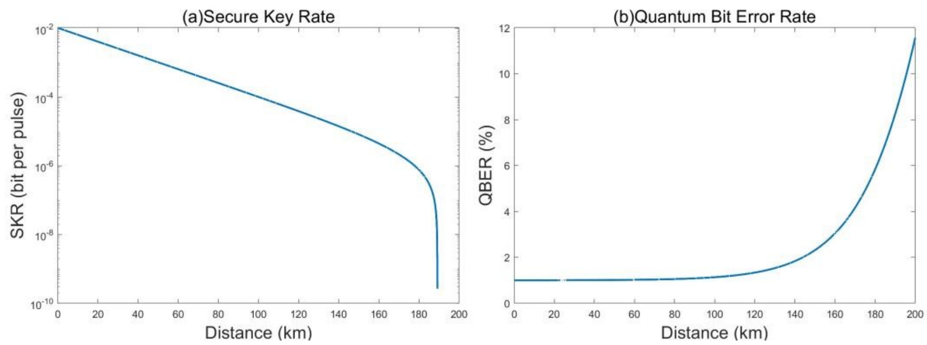


Figure 2: SKR and QBER vary with transmission distance (a, b)

The attenuation coefficient significantly impacts system performance. A lower attenuation coefficient means less photon loss during transmission, which can enhance the system's SKR. The attenuation coefficient is influenced by various factors, including fiber material, structure, operating wavelength, environmental conditions, and fiber aging. To examine the impact of the attenuation coefficient on QKD system performance, we varied it from 0.20 dB/km to 0.15 dB/km and 0.25 dB/km in Figure 3 (a) and Figure 3 (b). It is clear that as the attenuation coefficient increases, both SKR decreases and QBER increases, indicating a loss in security and reliability.

DOI: 10.54254/2755-2721/119/2025.21529

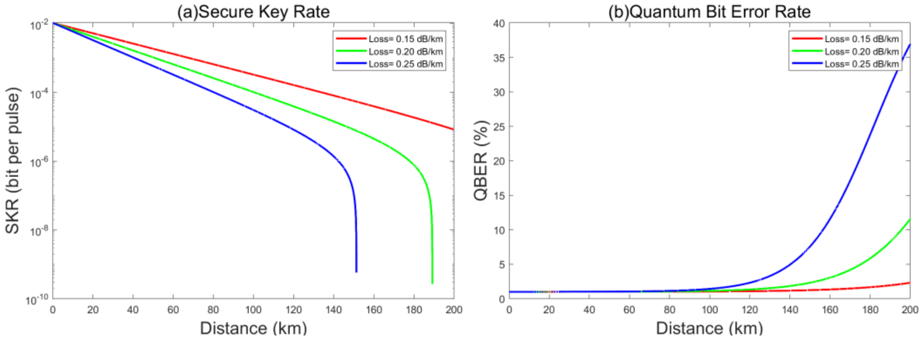


Figure 3: SKR and QBER vary with attenuation (a, b)

On the one hand, the average number of photons per pulse (u) determines the photon count in each pulse. In Figure 4 (a) and Figure 4 (b), the effect of varying u from 0.4 to 0.2 or 1.0 on SKR and QBER can be observed. While an increase in u leads to an increase in SKR, the effect is relatively limited compared to other parameters, and the change in QBER is inversely proportional. On the other hand, the dark count rate, which represents the false triggering rate of a detector in the absence of photon input, directly contributes to an increase in the error rate. Therefore, reducing the dark count rate is crucial for enhancing system performance. In Figure 5 (a) and Figure 5 (b), the dark count rate was set to $10^{-7}$, $10^{-6}$, and $10^{-5}$ to study its impact. The results show that as the dark count rate increases, or as noise increases, SKR decreases and QBER increases. This parameter is especially significant in long-distance transmission and high-noise environments.

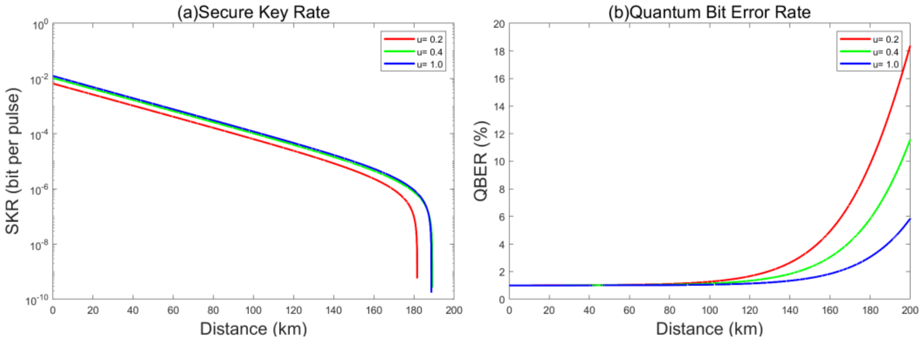


Figure 4: SKR and QBER vary with photon count per pulse (u) (a, b)

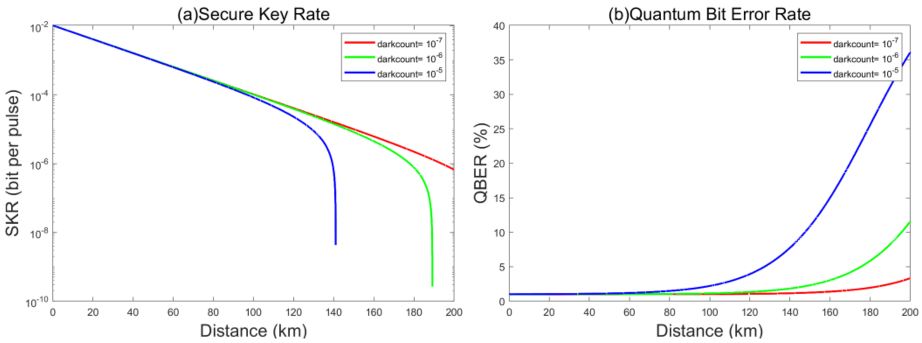


Figure 5: SKR and QBER vary with dark count rate (a, b)

Detection efficiency (eff) influences the detector's ability to detect photons. Detection efficiency is affected by the material, design, and operational conditions of the detector. To observe its influence, we set eff to 0.1, 0.2, and 0.3 in Figure 6 (a) and Figure 6 (b). As detection efficiency increases, the system is able to detect transmitted quantum signals more efficiently, resulting in a significant increase in SKR. This indicates that under the same transmission conditions, higher detection efficiency allows for the generation of more secure keys and enhances communication security. Although the effect of detection efficiency on QBER is relatively small, the study found a slight downward trend in QBER as detection efficiency increases. This suggests that improving detection efficiency not only increases SKR, but also helps to reduce the error rate in transmission, thereby improving the reliability of quantum communication.

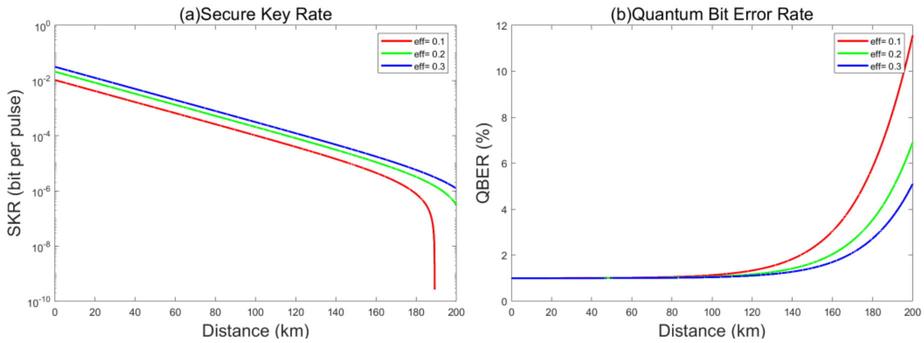

Figure 6: SKR and QBER vary with detection efficiency (eff) (a, b)

In addition to the aforementioned parameters, error correction efficiency (fE) plays a crucial role in rectifying errors. Higher error correction efficiency can improve the system's SKR. Bidirectional error correction algorithms, which correct errors in both directions of communication, significantly enhance error correction efficiency. These algorithms typically combine forward and backward error correction techniques, effectively correcting errors without adding excessive overhead. Bidirectional error correction algorithms can improve efficiency under various error rates, with fE typically set to 1.15 or higher, indicating that the algorithm can correct 15% more errors than the theoretical maximum error correction capability.

Fixed efficiency q is a characteristic parameter of the QKD protocol (BB84 was used in this research). The choice of protocol can also affect the results. The optimal operational range of the system can be determined by simulating its performance across different transmission distances. By adjusting parameters like average photon count and dark count per pulse, the balance between signal and noise can be optimized. Enhancing detection efficiency and reducing optical error rates can directly improve overall system performance. These findings are crucial for the design and optimization of quantum communication systems, especially in application scenarios that require high security and advanced detection efficiency. The overall performance of the 6G fronthaul network architecture based on quantum technology can be significantly improved by optimizing these parameters.

## 5. Conclusion

This study successfully proposes and evaluates a novel 6G fronthaul network architecture that seamlessly integrates QKD with passive WDM. The architecture represents a significant step forward in the quest to achieve ultra-high security and efficient resource utilization in next-generation mobile communication networks. By leveraging the multiplexing capabilities of WDM, the proposed system enables the simultaneous transmission of quantum and classical signals over a single optical fiber, thus conserving fiber resources while maintaining high security standards. The simulation experiments provide valuable insights into the critical parameters that influence the performance of the QKD system, including transmission distance, attenuation coefficient, photon count per pulse, dark count rate, and detection efficiency. The findings indicate that optimizing these parameters can lead to substantial improvements in the secure key rate (SKR) and reductions in the quantum bit error rate (QBER), thereby enhancing both the efficiency and reliability of the system. The proposed architecture is particularly well-suited for high-security applications in 6G networks, such as autonomous vehicles, remote surgery, and IoT security, where the integrity and confidentiality of data are paramount. Moving forward, future research will focus on further optimizing the system design to maximize performance and exploring practical deployment scenarios to fully leverage the advantages of quantum communication in next-generation mobile networks. This work contributes not only to the theoretical development of 6G fronthaul networks but also provides a valuable reference for the design and practical implementation of next-generation communication infrastructure, enhancing security and reliability in these systems.

## References

*[1] Garg, Krishna Avatar and Agya Mishra. "5G Network Advanced Techniques: A Literature Review." International Journal of Engineering 8 (2018): 264822.*

*[2] George, A.Shaji, and S.Sagayarajan. Exploring the Potential and Limitations of 5G Technology: A Unique Perspective. 20 Apr. 2023, https://doi.org/10.5281/zenodo.7869011.*

*[3] Sandeep Pirbhulal, et al. "IoT Cybersecurity in 5G and Beyond: A Systematic Literature Review." International Journal of Information Security, 28 May 2024, https://doi.org/10.1007/s10207-024-00865-5.*

*[4] Chatterjee, Ayan, et al. "A Systematic Review and Knowledge Mapping on ICT-Based Remote and Automatic COVID-19 Patient Monitoring and Care." BMC Health Services Research, vol. 23, no. 1, 30 Sept. 2023, https://doi.org/10.1186/s12913-023-10047-z.*

*[5] Meng, Zili, et al. Achieving Consistent Low Latency for Wireless Real-Time Communications with the Shortest Control Loop. 22 Aug. 2022,https://doi.org/10.1145/3544216.3544225.*

*[6] Rajmohan, Tanusan, et al. "A Decade of Research on Patterns and Architectures for IoT Security." Cybersecurity, vol. 5, no. 1, 5 Jan. 2022, https://doi.org/10.1186/s42400-021-00104-7.*

*[7] Vatsal Vasani, et al. "Embracing the Quantum Frontier: Investigating Quantum Communication, Cryptography, Applications and Future Directions." Journal of Industrial Information Integration (Online), vol. 39, 1 May 2024, pp. 100594–100594, https://doi.org/10.1016/j.jii.2024.100594.*

*[8] Kazmi, Syed Hussain Ali, et al. "Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions." Symmetry, vol. 15, no. 6, 1 June 2023, https://doi.org/10.3390/sym15061147.*

*[9] Marcello Caleffi, et al. "Distributed Quantum Computing: A Survey." Computer Networks, no. 254, 1 Aug. 2024, pp. 110672–110672, https://doi.org/10.1016/j.comnet.2024.110672.*

*[10] Yang, Mengmeng, et al. "From 5G to 6G: A Survey on Security, Privacy, and Standardization Pathways." ArXiv.org, 2024, arxiv.org/abs/2410.21986.*

*[11] Marcello Caleffi, et al. "Distributed Quantum Computing: A Survey." Computer Networks, no. 254, 1 Aug. 2024, pp. 110672–110672, https://doi.org/10.1016/j.comnet.2024.110672.*

*[12] Dutta, A., and E. Hammad. "5G Security Challenges and Opportunities: A System Approach." IEEE Xplore, 1 Sept. 2020, ieeexplore.ieee.org/document/9221122.*

*[13] Gracia, M. B., Malele, V., et al. "6G Security Challenges and Opportunities." Presented at the 2022 IEEE 13th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT), Cape Town, South Africa, 2022. IEEE, pp. 339-343. https://ieeexplore.ieee.org/document/9845296.*