Proceedings of the 5th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/100/20251738

A Sturdy Shield: Enhancing 6G Fronthaul with Quantum-Security

Mingxuan Yang[1,a,*]

[1]Xiamen University, No. 422, Siming South Road, Xiamen, Fujian, China
a. 2949706280@qq.com
**corresponding author*

Abstract: With the emergence of smart devices and the Internet of Things (IoT), 5G has been developed to meet the growing demand for transmission speeds and bandwidth. 5G overcomes the limitations of previous generations of technology, offering significant improvements in speed, latency, and stability. However, with the advancement of computational capabilities and the advent of quantum computers, security issues have become a pressing concern. Current technologies in 5G fronthaul rely on intrinsic security technologies, which are difficult to defend against quantum computer-based attacks. Consequently, this paper proposes a future mobile fronthaul architecture, such as 6G, which builds upon the 5G fronthaul network architecture while introducing quantum communication based on the BB84 protocol. This architecture enhances privacy protection and improves resistance to eavesdropping while maintaining the original performance. Additionally, the paper models the architecture to explore its noise resistance, using forward and backward spontaneous Raman scattering power as indicators, and demonstrates the system's feasibility under the influence of high-power 6G signals. The potential applications of this architecture are also examined. The results indicate that the quantum-secure 6G fronthaul network represents a significant breakthrough. It not only meets the stringent security requirements of modern communication but also enables a wide range of applications, paving the way for a safer and more interconnected digital future.

Keywords: Quantum Communication, 6G communication, Architecture design, Noise analysis.

1. Introduction

As smartphones, video streaming services, and Internet of Things (IoT) devices become more widespread, the global demand for data transmission speed and bandwidth has surged, with 4G technology struggling to keep up with this growth. This surge necessitated the development of new technology to address these challenges. At the same time, the widespread use of IoT devices requires networks to have higher connection density and lower latency to ensure efficient and reliable communication between devices [1]. In response to this, 5G technology emerged. 5G, short for the fifth generation of mobile communication technology, follows the progression of 1G, 2G, 3G, and 4G. Compared to previous generations, 5G offers notable improvements in transmission speed and latency, as well as breakthroughs in network security, coverage, and connection performance. The proliferation of 5G has driven the development of innovative applications like smart cities, autonomous driving, and remote healthcare, significantly enhancing information transmission efficiency, improving user experience, and bringing transformative changes to industries such as manufacturing, healthcare, and transportation [2].

Although 5G has made significant advancements in data transmission speed, low latency, and device connection density, it still faces several pressing issues, including network security and privacy concerns, spectrum limitations, integrated applications, and high construction costs. These shortcomings highlight the challenges and limitations of 5G technology in practical applications and offer insights into areas for improvement in the future development of 6G technology [3]. Compared to 5G, 6G promises substantial improvements in peak data rates, user experience data rates, spectrum efficiency, regional traffic density, connection density, mobility, latency, reliability, security, privacy, and resilience. It also introduces breakthroughs in positioning accuracy, interoperability, sustainability, artificial intelligence (AI) capabilities, sensing capabilities, and coverage range. Unlike previous mobile communication systems, security in the 6G era has garnered unprecedented attention [4]. In this era, we are not only dealing with a society of interconnected devices but a rich and diverse intelligent world, where the security requirements for networks are more stringent. Those who can master security capabilities in this era will avoid being undermined.

6G places greater emphasis on network security and user privacy by introducing more advanced encryption algorithms and technologies, alongside adopting more sophisticated identity verification mechanisms to protect privacy and security during data transmission. This includes cutting-edge technologies such as quantum encryption to prevent unauthorized access or decryption of data. 6G networks aim to be trustworthy, secure, and resilient, with self-immunity, security autonomy, proactive defense, and dynamic evolution capabilities, meeting the differentiated security needs of various application scenarios [5].

2. Literature Review

Currently, significant progress has been made in 6G research. Ref [6] highlights the architectural concepts, security-enabling factors, and mobile communication networks for 6G technology. It also explores the broad applications of 6G and conducts a comparative analysis, revealing the key differences and potential advancements of 6G technology compared to its predecessor, 5G. Ref [7] discusses the opportunities and various methods for achieving the goals of sixth-generation internet networks. It addresses the major and critical functions and technologies that can be used for 6G communication, outlining the challenges and research directions that may arise in its successful implementation. In addition to outlining 6G internet communication goals, it examines and explains different technologies that can be implemented following the comprehensive deployment of 6G communication. By implementing solution providers and adding more tower stations, 6G can be made a practical reality. Ref [8] emphasizes that communication security between individuals, industries, and multiple smart objects in 6G wireless communication technology requires significant attention. It outlines the need for new paradigms that will redefine security in next-generation wireless communication technologies, warning that ignoring these needs could lead to serious security risks that may hinder 6G's potential.

This paper innovatively explores the potential of a quantum-secure 6G fronthaul architecture, which integrates Quantum Key Distribution (QKD) with traditional fronthaul technologies to address significant security vulnerabilities in existing methods posed by quantum computing threats. Key innovations include the dual design of both active and passive fronthaul networks, enabling efficient bidirectional data signal transmission alongside unidirectional quantum signal transmission within the same optical fiber. Utilizing photonic states to carry quantum information in different polarization states forms a robust system capable of supporting diverse applications. This architecture effectively leverages wavelength division multiplexing to optimize fiber resources, significantly enhancing the efficiency of quantum communication. Additionally, our work emphasizes the importance of conducting noise analysis within the system. By investigating spontaneous Raman scattering, we establish the power dynamics affecting both forward and backward scattering in the quantum-secure 6G fronthaul. This analysis not only validates the feasibility of the proposed design but also lays the groundwork for further research to optimize performance under varying conditions. The results indicate that the quantum-secure 6G fronthaul architecture represents a significant advancement in meeting the challenges of combining data speed, bandwidth, and security while ensuring enhanced safety through quantum mechanics principles, such as the no-cloning theorem. The proposed architecture demonstrates exceptional adaptability, thriving in various scenarios—from resource-limited areas requiring cost-effective solutions to urban networks demanding high signal integrity.

3. Quantum Key Distribution

With the rapid development of information technology, network security issues have become increasingly severe. Traditional encryption methods, such as Rivest Shamir Adleman (RSA) and Advanced Encryption Standard (AES), face security risks in the face of enhanced computational capabilities and the advent of quantum computers. Therefore, there is an urgent need for new encryption methods to ensure the secure transmission of data. QKD utilizes fundamental principles of quantum mechanics, such as quantum superposition and entanglement, to ensure the security of keys. Various protocols and implementation methods have been continuously proposed and optimized, with the BB84 protocol being a typical and widely recognized process of QKD.

In the BB84 protocol, the sender (commonly referred to as Alice) and the receiver (commonly referred to as Bob) agree on the method of encoding information, including the orthogonal complementary bases used and the correspondence between the quantum states and binary information. Alice uses photons as the physical quantity to encode information, modulating a randomly generated bit sequence into quantum states, and sends them using two different orthogonal bases. Typically, the polarization states of the photons are set at 0°, 45°, 90°, and 135°. The two orthogonal bases are the horizontal-vertical basis and the diagonal basis. The horizontal-vertical basis allows 0° and 90° polarized light to pass, while the diagonal basis allows 45° and 135° polarized light to pass. Upon arrival, Bob randomly selects either the horizontal-vertical or diagonal basis to measure the incoming photons. For each quantum state, Bob records the measurement results and the basis used. Once all quantum states have been measured, Alice and Bob publicly disclose the bases they used for measurement, but not the measurement results themselves. They compare the bases and retain only the results measured with the same basis. Although the basis comparison process is conducted over a classical channel and could potentially be eavesdropped upon, any eavesdropper can only randomly select measurement bases like Bob, and cannot obtain precise information about the quantum states [9].

To detect potential eavesdropping during the communication process, Alice and Bob can randomly select a portion of the key and publicly compare it to check for discrepancies. According to the no-cloning theorem, quantum states cannot be copied, meaning that any attempt to eavesdrop during key distribution would result in detectable disturbances in the quantum states. By leveraging the properties of quantum mechanics, QKD provides a theoretically unconditionally secure method for key distribution, offering wide-ranging applications [10].

4. Quantum-Secure 6G Fronthaul Architecture Design

5G fronthaul is a critical component of the 5G network architecture. An efficient fronthaul network design not only enables more effective data transmission but also improves cost efficiency while ensuring network reliability and stability. 5G fronthaul technology uses fiber optic communications to transmit multiple signals simultaneously over a single optical fiber. At the transmitting end, different wavelengths of light are multiplexed, and at the receiving end, they are demultiplexed, maximizing the fiber optic cable's capacity [11]. However, ensuring security remains a challenge, as the inherent security technologies in 5G fronthaul are vulnerable to attacks from quantum computers.

Quantum communication, by contrast, is a method that utilizes principles of quantum mechanics to provide secure communication through the generation and distribution of encryption keys. Thanks to the no-cloning theorem and the disturbance of quantum information during measurement, any eavesdropping attempts can be detected by the communicating parties, granting it theoretical absolute security. Consequently, integrating Quantum Key Distribution (QKD) with mobile fronthaul technology is a promising direction, and we believe this could be realized in 6G networks.

By combining 5G fronthaul technology with quantum communication, we propose a quantum-secure 6G passive fronthaul architecture (shown in Figure 1) and an active fronthaul architecture (shown in Figure 2). In both architectures, the Distributed Unit (DU) and Active Antenna Unit (AAU) sites are capable of receiving and transmitting data, enabling bidirectional data transmission in the 6G fronthaul network. In the downlink, data is transmitted from the DU to the AAU site, while transmission from the AAU site to the DU constitutes the uplink. In contrast, quantum information is transmitted unidirectionally, meaning that quantum information can only flow from the DU to the AAU site.

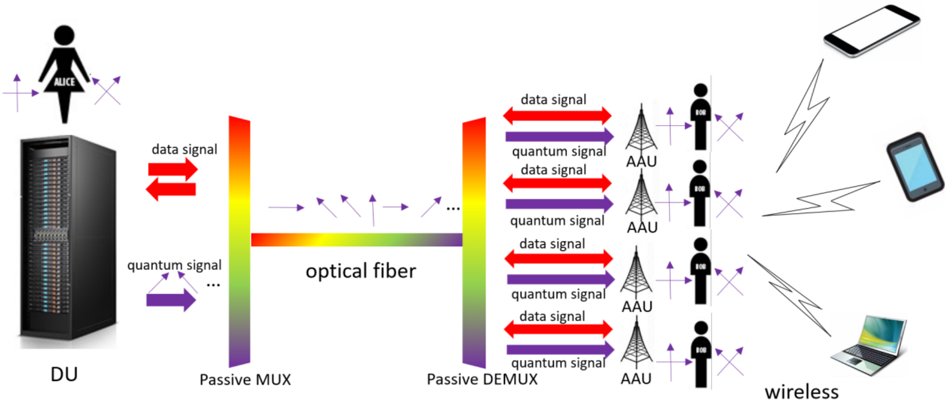

Figure 1: Quantum-Secure 6G Passive Fronthaul Architecture. DU: Distributed Unit. AAU: Active Antenna Unit. MUX: Multiplexer. DEMUX: Demultiplexer.

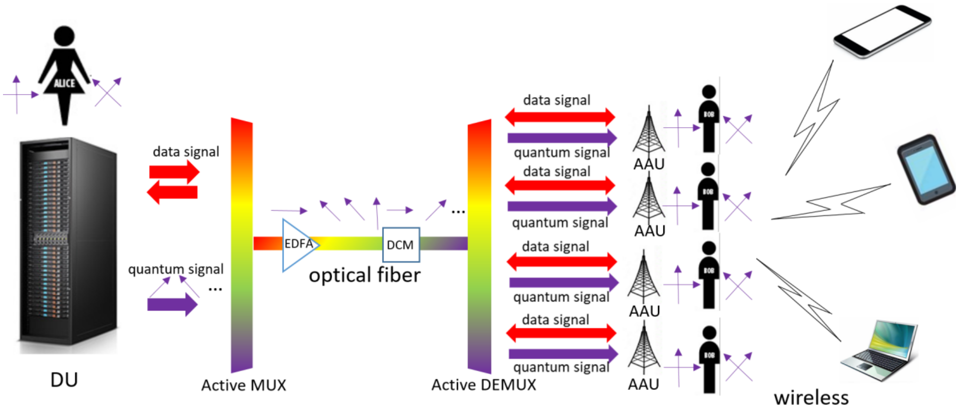

Figure 2: Quantum-Secure 6G Active Fronthaul Architecture. DU: Distributed Unit. AAU: Active Antenna Unit. MUX: Multiplexer. DEMUX: Demultiplexer. EDFA: Erbium Doped Fiber Amplifier. DCM: Dispersion Compensation Module.

In this architecture, quantum states are transmitted from the DU and received at various AAU sites. We can denote the transmitting and receiving ends as Alice and Bob, respectively. After agreeing on the quantum states and their corresponding binary relationships with Bob, Alice randomly chooses to use either the horizontal-vertical or diagonal basis. She then prepares photons with polarization states at 0° (→), 45° (↗), 90° (↑), and 135° (↖) to carry the quantum information. These photons are loaded into different wavelengths of lasers, each assigned to specific AAU sites. The optical carrier signals of various wavelengths are combined through a multiplexer (MUX) and coupled into a single optical fiber, which contains all the quantum information needed for the various AAU sites.

At the receiving end, a demultiplexer (DEMUX) separates the optical carriers of different wavelengths and transmits them to their respective AAU sites. Each Bob, like Alice, randomly chooses either the horizontal-vertical or diagonal basis to receive the photons of different polarization states. By doing so, they obtain a series of polarization state information. After performing basis reconciliation, Alice and Bob generate their respective key sequences based on the retained polarization states and the pre-agreed correspondence between polarization states and binary representations.

The quantum-secure 6G fronthaul architecture can be categorized into passive and active fronthaul designs. The passive fronthaul employs passive components to multiplex and demultiplex different wavelength optical signals. It does not require electrical power to operate; instead, it relies purely on the physical properties of light for signal processing, which typically limits transmission distances. In contrast, the active fronthaul employs active devices such as Erbium-Doped Fiber Amplifiers (EDFAs) and Dispersion Compensation Modules (DCMs) to process and manage signals. These devices require electrical power but allow for longer transmission distances. Since each DU is connected to multiple AAU sites, this significantly enhances the utilization efficiency of quantum communication. Moreover, compared to backhaul and midhaul, the fronthaul has the shortest transmission distance, which results in minimal quantum attenuation.

The 6G fronthaul architecture with quantum security contributes significantly to the future of communication. Combining 6G with quantum communication is a relatively novel approach that retains the efficient transmission capabilities of traditional data while simultaneously enhancing the security and reliability of traditional architectures through quantum communication. In contrast to 5G, future 6G networks will focus not only on data transmission speed but also on privacy. Therefore, this architecture serves as a technical reference for the future of 6G. Moreover, considering that quantum communication is currently in the development stage, integrating 6G with Quantum Key Distribution (QKD) will aid in the practical implementation of quantum communication.

5. Noise Analysis in the Quantum-Safe 6G Fronthaul Architecture

Compared to the traditional 5G architecture, the quantum-secure 6G fronthaul architecture supports bidirectional transmission of data signals and unidirectional transmission of quantum signals over the same optical fiber. By leveraging wavelength multiplexing, it optimizes the use of fiber resources, enhancing practical application scenarios. However, in such wavelength multiplexing systems, the power of the 6G optical signals is relatively high, while quantum signals are typically transmitted at low power to maintain the fidelity and security of quantum states. This makes quantum signals more susceptible to interference from high-power transmissions. Specifically, high-power 6G signals can lead to spontaneous Raman scattering, which introduces noise and interferes with the integrity of the quantum communication in the fronthaul network.

To assess this, we will analyze the impact of spontaneous Raman scattering in the quantum-secure 6G fronthaul architecture. Spontaneous Raman forward scattering refers to the scattering of light that propagates in the same direction as the quantum signal. This phenomenon degrades signal quality and transmission efficiency. In contrast, spontaneous Raman backward scattering refers to the scattering of light that propagates in the opposite direction, potentially causing interference as the scattered light returns to the source, thus affecting signal transmission. By evaluating the power of spontaneous Raman forward and backward scattering in the 6G architecture, we can determine the feasibility and stability of the quantum-secure system. The next step involves modeling the power generated by Raman scattering in the 6G network. Since 6G signals are transmitted bidirectionally, different types of noise interference arise depending on the direction of signal propagation within the optical fiber. For instance, when 6G signals are transmitted in the downlink direction, spontaneous Raman scattering generates forward noise, which aligns with the quantum signal. On the other hand, in the uplink direction, spontaneous Raman scattering generates backward noise, which opposes the quantum signal's propagation. By analyzing and quantifying these scattering effects, we can validate the robustness and practicality of the proposed quantum-secure 6G fronthaul architecture under real-world transmission conditions, ensuring that the quantum signals remain protected even in high-power environments typical of 6G communication. The power generated by spontaneous Raman scattering in a small segment of that fiber is written as [12]

$$\mathrm{dP(z)} = \eta \mathrm{P_p(0)} \exp\left[-\alpha_\mathrm{p} \mathrm{z}\right] \mathrm{dz} \tag{1}$$

where n is a proportional constant, Pp(0) is the input power of 6G optical signals, and ɑp is the loss coefficient of the fiber. Next, we will derive the expressions for the forward reflection power and backward reflection power in a small segment of that fiber as follows:[13]

$$\begin{aligned}\mathrm{dP(z \to L)} &= \mathrm{dP(z)} \exp[-\alpha_\mathrm{r}(\mathrm{L-z})] \\ &= \eta \mathrm{P_p(0)} \exp\left[-\alpha_\mathrm{p} \mathrm{z}\right] \times \exp[-\alpha_\mathrm{r}(\mathrm{L-z})]\, \mathrm{dz}\end{aligned} \tag{2}$$

$$\begin{aligned}\mathrm{dP(z \to 0)} &= \mathrm{dP(z)} \exp[-\alpha_\mathrm{r} \mathrm{z}] \\ &= \eta \mathrm{P_p(0)} \exp\left[-\alpha_\mathrm{p} \mathrm{z}\right] \times \exp[-\alpha_\mathrm{r} \mathrm{z}]\, \mathrm{dz}\end{aligned} \tag{3}$$

where ɑr is the loss coefficient of the SpRS light. The total spontaneous Raman forward scattering power and spontaneous Raman backward scattering power are obtained by integrating the previous two expressions, respectively:[14]

$$\begin{aligned}P_{raman}^{f} &= \int_{0}^{L} \eta P_p(0) \exp\,[-\,\alpha_r(L-z)]dz \\ &= \frac{\eta P_p(0)}{\alpha_r-\alpha_p}\left\{\exp\left[-\alpha_p L\right] - \exp[-\alpha_r z]\right\}\end{aligned} \tag{4}$$

$$\begin{aligned}P_{raman}^{f} &= \int_{0}^{L} \eta P_p(0) \exp\,[-\,\alpha_p z] \times \exp\,[-\alpha_p z]dz \\ &= \frac{\eta P_p(0)}{\alpha_r+\alpha_p}\left\{\exp\left[\alpha_p L\right] - \exp[-\alpha_r z]\right\}\exp\,[-\alpha_p L]\end{aligned} \tag{5}$$

It is evident that the Raman scattering power generated in a quantum-secure 6G fronthaul network is influenced by several factors, including fiber length, the 6G optical signal loss coefficient, and the spontaneous Raman scattering (SpRS) loss coefficient, among others. If the calculated results from the noise analysis of a quantum-secure fronthaul network show no significant discrepancies compared to those of a fronthaul network without quantum communication, this would confirm the feasibility of the quantum-secure 6G fronthaul network in terms of resistance to noise interference.

6. Application Mode Analysis

The 6G passive fronthaul network leverages passive optical devices, eliminating the need for additional power supplies. It typically connects various components directly through optical fibers. Since it doesn't require extra power equipment or complex network management, passive fronthaul networks are more cost-effective in terms of construction and maintenance. This makes them particularly suited for deployment in edge areas or resource-limited environments. Passive fronthaul networks are ideal for simple, short-distance connections, such as network deployments for small businesses or residential communities [15]. Additionally, passive devices generally offer enhanced stability and reliability, making them well-suited for regions with unstable electricity or harsh environmental conditions, such as mountainous or plateau regions.

In contrast, the 6G active fronthaul network typically includes active devices that support dynamic bandwidth allocation and resource scheduling, making it suitable for long-distance transmission and more complex topologies, such as larger metropolitan access networks [16]. Active fronthaul networks excel in scenarios that require high signal quality, making them suitable for applications in virtual reality (VR), augmented reality (AR), and high-frequency trading.

7. Conclusion

In conclusion, the proposed quantum-secure 6G fronthaul architecture represents a significant advancement in addressing the security challenges faced by traditional communication methods, particularly in light of emerging quantum computing capabilities. By seamlessly integrating QKD with both passive and active fronthaul technologies, this architecture not only enhances security but also optimizes data transmission efficiency. The innovative dual design of the fronthaul network achieves efficient bidirectional data signal transmission and unidirectional quantum signal transmission, thereby maximizing the utilization of existing optical fiber infrastructure. The effective use of wavelength division multiplexing not only fully exploits the capacity of optical fibers but also significantly enhances the overall efficiency of quantum communication protocols. A key outcome of this research is the validation of the architecture's resilience against noise interference, particularly through a comprehensive analysis of spontaneous Raman scattering. This analysis demonstrates the architecture's ability to maintain high-quality signal transmission in a combined optical environment, highlighting its feasibility for real-world applications. The applications of the quantum-secure 6G fronthaul architecture span multiple domains, making it suitable for deployment in both urban and remote areas. The passive fronthaul model is particularly well-suited for resource-limited environments, providing reliable and stable network connections for small businesses and residential communities without the need for complex power management systems. Overall, the quantum-secure 6G fronthaul architecture not only signifies a leap in optical communication technology but also paves the way for a new era of secure wireless communication that supports smart cities, the Internet of Things (IoT), and critical real-time services. By leveraging the principles of quantum mechanics, we envision a future where secure, efficient, and reliable communication becomes the standard, catering to current and emerging needs in the telecommunications field.

References

[1] *M. Vaezi et al., "Cellular, Wide-Area, and Non-Terrestrial IoT: A Survey on 5G Advances and the Road Toward 6G," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 1117-1174, Secondquarter 2022, doi: 10.1109/COMST.2022.3151028.*

[2] *M. A. Ali Al-Samawi and M. Singh, "Effect Of 5G On IOT And Daily Life Application," 2022 3rd Inter national Conference for Emerging Technology (INCET), Belgaum, India, 2022, pp. 1-5, doi: 10.1109/INCET54531.2022.9823983.*

[3] *M. Taheribakhsh, A. Jafari, M. M. Peiro and N. Kazemifard, "5G Implementation: Major Issues and Challenges," 2020 25th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran, 2020, pp. 1-5, doi: 10.1109/CSICC49403.2020.9050110.*

[4] *H. Du, S. He, L. Su, J. Bai and R. Yan, "Requirements and Potential Key Technologies of Security for 6G Mobile Network," 2023 International Conference on Networking and Network Applications (NaNA), Qingdao, China, 2023, pp. 1-6, doi: 10.1109/NaNA60121.2023.00008.*

[5] G. M. Karam, M. Gruber, I. Adam, F. Boutigny, Y. Miche and S. Mukherjee, "The Evolution of Networks and Management in a 6G World: An Inventor's View," in IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 5395-5407, Dec. 2022, doi: 10.1109/TNSM.2022.3188200.

[6] J. Singh, G. Singh and N. Vashisht, "Evaluating 6G Network Technology Principles and Applications: A Review," 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/SMARTGENCON60755.2023.10442029.

[7] G. Singh, I. Verma, S. Bhardwaj, R. Sharma and W. Ahmed, "Requirements, Technologies, Applications and Challenges of 6G Communication: A Review," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 1608-1612, doi: 10.1109/IC2PCT60090.2024.10486362.

[8] M. B. Gracia, V. Malele, S. P. Ndlovu, T. E. Mathonsi, L. Maaka and T. Muchenje, "6G Security Challenges and Opportunities," 2022 IEEE 13th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT), Cape Town, South Africa, 2022, pp. 339-343, doi: 10.1109/ICMIMT55556.2022.9845296.

[9] H. -F. Li, L. -X. Zhu, K. Wang and K. -B. Wang, "The Improvement of QKD Scheme Based on BB84 Protocol," 2016 International Conference on Information System and Artificial Intelligence (ISAI), Hong Kong, China, 2016, pp. 314-317, doi: 10.1109/ISAI.2016.0073.

[10] I. Giroti and M. Malhotra, "Quantum Cryptography: A Pathway to Secure Communication," 2022 6th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2022, pp. 1-6, doi: 10.1109/CSITSS57437.2022.10026388.

[11] J. Han, P. Han and Y. Liu, "Survivable Wavelength-Division-Multiplexed Passive Optical Network for Fronthaul in 5G and Beyond," 2021 9th International Conference on Intelligent Computing and Wireless Optical Communications (ICWOC), Chongqing, China, 2021, pp. 5-10, doi: 10.1109/ICWOC52624.2021.9530212.

[12] R. Ranjan, G. Costa, M. A. Ferrara, M. Sansone and L. Sirleto, "Noise Investigation in Femtosecond Stimulated Raman Scattering Microscopy," 2023 23rd International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 2023, pp. 1-4, doi: 10.1109/ICTON59386.2023.10207520.

[13] M. Krause, J. Müller and E. Brinkmeyer, "Measurement of nonreciprocal stimulated Raman scattering in silicon photonic wires," The 9th International Conference on Group IV Photonics (GFP), San Diego, CA, USA, 2012, pp. 6-8, doi: 10.1109/GROUP4.2012.6324068.

[14] D. Semrau, "Modeling of Fiber Nonlinearity in Wideband Transmission," 2022 Optical Fiber Communications Conference and Exhibition (OFC), San Diego, CA, USA, 2022, pp. 1-3.

[15] K. Honda, T. Kobayashi, T. Shimada, J. Terada and A. Otaka, "WDM passive optical network managed with embedded pilot tone for mobile fronthaul," 2015 European Conference on Optical Communication (ECOC), Valencia, Spain, 2015, pp. 1-3, doi: 10.1109/ECOC.2015.7341999.

[16] A. Kawakita et al., "Design for Long-Reach Coexisting PON in Consideration of Area Characteristics with Wavelength Selective Asymmetrical Splitters," 2019 24th OptoElectronics and Communications Conference (OECC) and 2019 International Conference on Photonics in Switching and Computing (PSC), Fukuoka, Japan, 2019, pp. 1-3, doi: 10.23919/PS.2019.8817849.