Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/119/2025.19330

Research on the Design and Application of 6G Communication Network Architecture Based on Quantum Key Encryption

Yuan Wang[1,a,*]

[1]*School of Physics and Information Engineering, Fuzhou University, Wulongjiang North Avenue, Fujian, China*
a. 3314073411@qq.com
**corresponding author*

Abstract: With the rapid development of 6G technology, people's lives are becoming increasingly convenient. Simultaneously, great emphasis must be placed on the security demands of this communication technology. We propose two encryption methods for 6G communication security based on different encryption scenarios: a Quantum Key Distribution (QKD)-Secured 6G fronthaul communication architecture for high-security scenarios and a QKD-Secured 6G fronthaul communication architecture for low-security scenarios. For high-security scenarios, the QKD-Secured 6G fronthaul communication architecture utilizes multiple quantum transmitters and corresponding quantum receivers to generate multiple quantum keys simultaneously, significantly enhancing security requirements for high communication rates. However, due to its high cost, this setup is not always practical. In most applications, we adopt a QKD-Secured 6G fronthaul communication architecture for low-security scenarios. In this approach, a single quantum transmitter corresponds to multiple quantum receivers, which, while potentially reducing the quantum key generation speed, significantly lowers costs. We address the reduced key rate by adjusting the information load on each key pair. The proposed architecture largely satisfies the security requirements of 6G, broadening its application scenarios. As a crucial technology for communication security, QKD offers high security, strong resistance to attacks, and flexibility. With its continued development and adoption, QKD is expected to play an increasingly significant role in future communication networks.

Keywords: 6G, QKD, secure key rate, noise analysis.

1. Introduction

5G, the fifth-generation mobile communication technology, integrates high speed, low latency, massive connectivity, and other advantages, making it widely used in daily life [1]. In an ideal online environment, users can achieve a minimum transmission speed of 1 Gbps, experience only 1 ms latency in receiving data, and support up to 1 million connections per square kilometer [1-4]. How does 5G achieve such powerful capabilities? There are several key technologies that enable this performance. First, 5G utilizes high-frequency waves as information carriers, allowing for increased bandwidth and improved transmission speeds. Common frequency bands include the millimeter wave

DOI: 10.54254/2755-2721/119/2025.19330

and Sub-6 GHz bands, which enable 5G to transmit data at significantly faster rates compared to previous generations [1-4]. Second, beamforming technology enhances signal transmission efficiency and directionality. This technology reduces interference during transmission to ensure complete and accurate information delivery. By precisely directing signals, beamforming optimizes network performance and enhances the overall user experience [1,2]. Third, 5G incorporates Multiple-Input Multiple-Output (MIMO) technology on both the transmission and reception ends, which, without increasing bandwidth or transmission power, significantly boosts network capacity. This allows more devices to connect simultaneously to the network [2,3]. With these features, 5G not only addresses individual communication needs and enables experiences like augmented reality, virtual reality, and 3D applications but also meets a wide range of Internet of Things (IoT) requirements, driving innovations in smart homes, cities, and industries [1-4].

Compared to 5G, 6G promises even higher speeds, lower latency, and greater connectivity overall. Transmission speeds in 6G can reach up to 1 Tbps, with latency potentially dropping to milliseconds or even lower [5],[6],[7]. Beyond these advantages, 6G emphasizes sustainable and optimized energy use, aligning with green development goals [5],[6],[8]. While 6G performance may surpass 5G by a factor of ten, research on 6G is still in the early exploratory stages, and there is no global consensus on its technical standards. In other words, 6G is largely conceptual, and its development will be a long and challenging task [5-7],[9]. Security in 6G is also of paramount importance. For instance, 6G could be applied to autonomous driving systems, which rely heavily on continuous communication and real-time data processing. These systems face significant security threats, as interference or tampering with communication signals and control instructions could lead to traffic accidents. As the saying goes, “with great power comes great responsibility.” It is essential to enhance security systems from multiple angles, including technical, application-specific, and preventive measures [7,10].

The sixth-generation (6G) mobile communication system will be built on a software-defined slicing platform, emphasizing edge computing and leveraging artificial intelligence and big data mining to support diverse application scenarios and performance objectives. Traditional add-on network security mechanisms are inadequate to meet the inherent security embedding requirements of 6G [7]. Researchers have proposed an endogenous security mechanism for 6G, elaborating on the architecture and key technologies of 6G’s built-in security and analyzing the security threats posed by new technologies adopted within 6G [8].

The 6G secure network architecture we propose largely addresses security issues in the communication process. By establishing quantum transmitters and receivers on base stations and transmitting quantum signals alongside data, the key sequences generated by these quantum signals can be used to encrypt information, effectively addressing potential security risks in 6G communications. Implementing this architecture requires resolving key challenges: matching key rates with bit rates, mitigating interference between 6G and quantum signals, and ensuring that the key rates generated by quantum signals align with the bit rates of transmitted data. This necessitates advanced quantum key distribution (QKD) techniques that can generate and distribute keys efficiently at rates compatible with high-speed 6G data transmission. As 6G signals operate within high-frequency bands, they may interfere with the delicate quantum states used in quantum communication. To mitigate this interference, careful design and engineering of both the 6G and quantum communication systems are essential.

Once these issues are addressed, the 6G security architecture will bring revolutionary changes to the field of communication. This architecture, leveraging advanced encryption technologies and security protocols combined with QKD-generated keys, can establish a robust network defense system, effectively countering cybersecurity risks such as network attacks, data theft, and identity spoofing, thereby protecting user privacy and data security. Integrating the 6G security architecture with QKD provides powerful technical support for applications such as smart cities and intelligent

DOI: 10.54254/2755-2721/119/2025.19330

transportation systems. Through 6G's high-speed data transmission capabilities and QKD's secure encryption, real-time monitoring, data analysis, and intelligent decision-making can be achieved within intelligent transportation systems, enhancing urban traffic efficiency and safety. By continuously strengthening communication security, advancing new technologies, and promoting cross-domain integration, the combination of 6G and QKD will offer substantial technical support for future intelligent applications.

2. QKD

The BB84 protocol is one of the most important QKD protocols. Proposed by Bennett and Brassard in 1984, its theoretical foundation and security have been well-established [11]. In this protocol, photons are used as information carriers, dividing the four polarization states of light into two sets of conjugate bases. In this scenario, we assume there is a sender, Alice, and a receiver, Bob. First, they agree in advance on an information encoding method and generate a random sequence, establishing a correspondence between photon polarization states and binary values. Then, Alice randomly selects one of the two conjugate bases and uses the photon's polarization to encode information onto the corresponding quantum state based on the random sequence. Bob then randomly chooses a basis to receive the photons. If Bob's chosen basis matches Alice's, he successfully receives the photons and, according to the established correlation, they generate secret keys. If the bases do not match, no keys are generated, giving Bob a 50% chance of receiving the information. Why does this protocol protect the information? If an eavesdropper, Eve, attempts to intercept the communication, she must measure the photons just like Bob. However, Eve only has a 50% chance of choosing the correct basis, and thus, she can only accurately eavesdrop on 50% of the bits Bob receives, resulting in an effective interception probability of only 25%. This process introduces errors that Alice and Bob can detect when they compare a subset of their keys, thereby revealing the presence of any eavesdropping attempts.

Table 1: BB84 protocol procedure

Random sequences Alice generates	0	0	1	1	1	0	1	0	1
Bases Alice chooses	+	x	+	+	x	x	x	+	x
photon's polarization states	→	↗	↑	↑	↖	↗	↖	→	↑
Random bases Bob chooses	+	+	x	+	+	x	+	+	x
Bob's measurement results	→	→	↗	↑	↑	↗	→	→	↑
base-pair comparison results	√			√		√		√	√
Generated key sequences	0			1		0		0	1

3. QKD-Secured 6G Fronthaul Communication Architecture

In the 6G fronthaul optical network, the Active Antenna Unit (AAU) and Distributed Unit (DU) are two essential components of the 6G network architecture [12]. The AAU is responsible for the lower layers of the radio frequency and physical layers, including signal reception, amplification, processing, and transmission. The DU primarily handles physical layer protocols and real-time services [13]. Common data transmission methods between the AAU and DU include direct fiber connection, passive Wavelength Division Multiplexing (WDM), active WDM, and Slice Packet Network (SPN) [14], among others. Since the AAU transmits information to the DU, which is vulnerable to eavesdropping, this process can potentially integrate with QKD. Thus, we propose a QKD-secured 6G fronthaul communication architecture, where a QKD transmitter in the AAU (corresponding to

DOI: 10.54254/2755-2721/119/2025.19330

the sender, Alice) and a QKD receiver in the DU (corresponding to the receiver, Bob) facilitate secure communication.

In the QKD-secured 6G fronthaul communication architecture, there are two crucial types of signals: quantum signals and data signals. Quantum signals utilize the unique properties of quantum states, as described in the BB84 protocol, to securely facilitate the transmission process through QKD. Data signals, which represent concrete information during transmission, can be divided into uplink and downlink data signals. Uplink data signals transmit information from customer devices, such as computers and mobile phones, to servers and networks, enabling functions like uploading files or sending emails. Downlink data signals transfer information from servers or networks to customer devices, enabling functions such as downloading files or browsing the web.

Theoretically, there is a one-to-one correspondence between transmitter and receiver, which we term the QKD-Secured 6G fronthaul communication architecture for high-encryption scenarios. However, in practice, the cost of constructing multiple receivers is relatively high, so it is more common to have multiple transmitters correspond to a single receiver, termed the QKD-Secured 6G fronthaul communication architecture for low-encryption scenarios. In Figure 1, where key generation is one-to-one, we can simultaneously transmit multiple types of data, achieving high key rates. In Figure 2, to ensure accurate and orderly transmission, information must be time-separated due to the limited number of receivers. Each approach has its own advantages and disadvantages: the former offers higher key generation rates but is costly, while the latter is more economical and practical but has lower key generation capabilities.

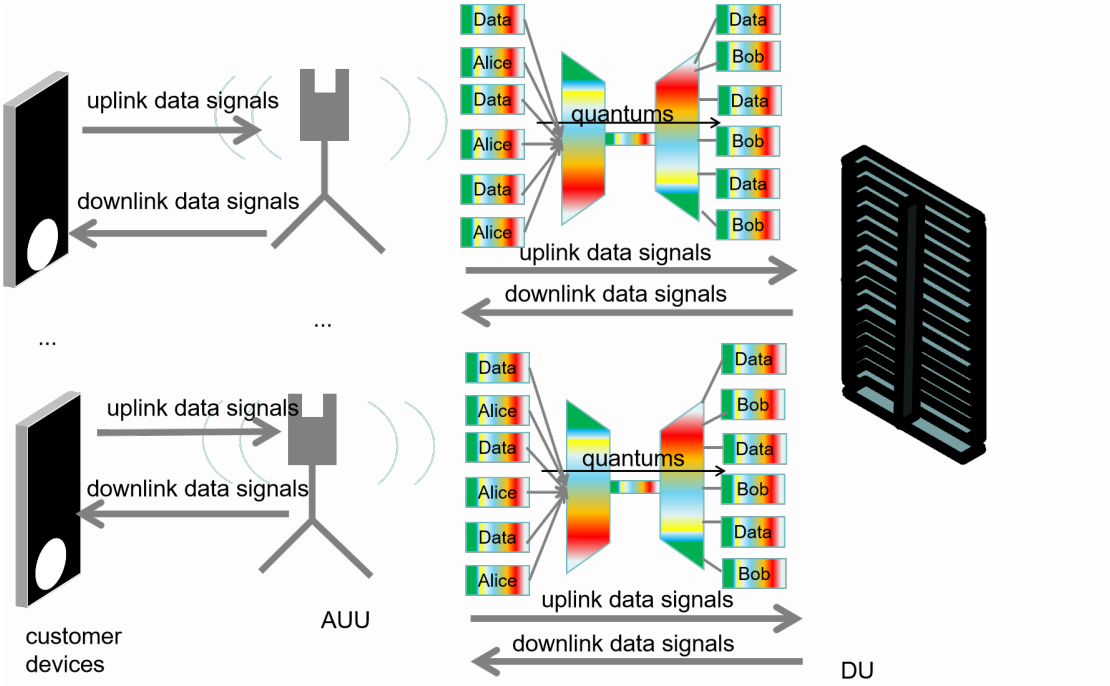

Figure 1: QKD-Secured 6G fronthaul communication architecture for high-encryption scenarios

DOI: 10.54254/2755-2721/119/2025.19330

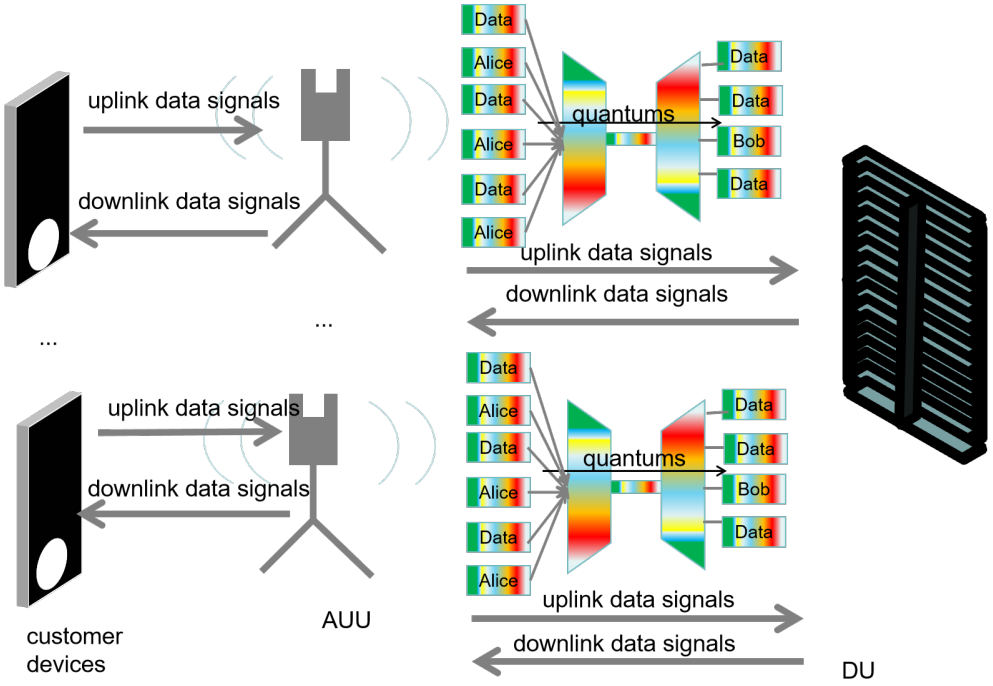

Figure 2: QKD-Secured 6G fronthaul communication architecture for low-encryption scenarios

QKD is a transmission mode focused on key security, while 6G is a new communication technology. The integration we propose can significantly enhance security in high-speed communication, effectively preventing information theft or tampering and providing strong resilience against attacks. This integration also promotes the development of quantum communication technology and offers practical value across a wide range of applications. For example, by deploying QKD terminals at both primary and backup sites of data centers, a secure key distribution link can be established. Shared security keys are then used to encrypt data transmissions between these sites, tailored to specific confidentiality levels and security requirements. For communication nodes that are difficult to reach by optical fiber and are located over long distances—such as island or intercontinental connections—QKD terminals can be deployed at each node. Using satellites, key distribution channels are established with each node to generate shared security keys, enabling secure data interactions.

4. Performance Analysis

4.1. Secure Key Rate Calculation

Is it feasible to integrate QKD with 6G architecture? This can be assessed from the perspectives of key generation rate, the impact of noise on key generation, and the attenuation of quantum signal intensity.

We use the GLLP formula to calculate the key generation rate [12]. The premise of the formula is that for a light source with multiple photons, only the single-photon pulses among them can generate secure keys. Based on this, the lower limit of the secure key rate using a given protocol is as follows:

$$S \geq Q_{\mu}\left\{-H_{2(e_{\mu})} + \Omega\left[1 - H_{2(e_1)}\right]\right\} \quad (1)$$

In the formula, Q_{μ} and e_{μ} represent the gain and quantum bit error rate (QBER) of the signal state, respectively. Here, the meaning of gain refers to the ratio of the signals detected by Bob after basis

DOI: 10.54254/2755-2721/119/2025.19330

reconciliation to the signals sent by Alice. $\Omega=Q_1/Q_\mu$ refers to the percentage of single-photon signals detected by Bob among the total signals sent by Alice. e_1 represents the QBER caused by single-photon signals, and $H_{2(x)} = -x\log_2(x) - (1-x)\log_2(1-x)$is the binary entropy associated with this QBER. Q_μ, e_μ, Q_1, e_1 are variables in it, and Q_μ and e_μ can be directly obtained through measurement. Therefore, the key to determining the lower limit of the key amount lies in accurately determining Q_1 and e_1 .By counting the signal states and Decoy states [13], and statistically analyzing the bit error rate, we can accurately estimate the lower bound of Ω as well as the upper bound of e_1 . This, in turn, significantly enhances the key generation rate and extends the secure communication distance of the quantum key distribution (QKD) system[15-19].

When Alice sends out an n-photon state, the errors arise from background noise and incorrect measurement results of the signal light:

$$e_n = \frac{e_0 Y_0 + e_{Det}\eta_n}{Y_n} \tag{2}$$

Where e_{Det} is the probability of incorrect detection results caused by the signal light.This parameter is typically determined by the interference performance and stability of the optical system. The general formula for describing the gain is as follows:

$$Q_\mu = \sum_{n=0}^{\infty} Y_n P_\mu(n) = \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu} = Y_0 + 1 - e^{-n\mu} \tag{3}$$

Therefore, the total bit error rate (BER) is given by:

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} e_n Y_n P_\mu(n) = \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n}{n!} e^{-\mu} = e_0 X_0 + e_{Det}(1 - e^{-n\mu}) \tag{4}$$

By increasing the key generation rate and reducing the impact of noise, we can make this integration feasible.

4.2. noise analysis

In a QKD-secured 5G fronthaul communication architecture, the quantum signals can experience noise interference from 6G signals, such as spontaneous Raman scattering noise. Assuming that the generation power of spontaneous Raman scattering is proportional to the intensity of the quantum signal. Over a short segment of optical fiber, the generation power of spontaneous Raman scattering is proportional to both the pump power and the length of that segment, with the proportionality constant denoted as the Raman efficiency η. Next, we provide the formula for the pump power as it varies with position z along the optical fiber, namely $P_P(z)=P_P(0)\exp(-\alpha_p*z)$, where $P_P(0)$ is the input pump power and α_p is the loss coefficient of the pump light. By substituting the pump power formula into the formula for the generation power of spontaneous Raman scattering, we obtain $dP(z)=\eta P_P(0)\exp(-\alpha_p z)dz$.

However, spontaneous Raman scattered light experiences loss in optical fibers, and both forward-scattered power and backward-scattered power are calculated separately. The forward-scattered power is the spontaneous Raman scattered power measured at the output end of the optical fiber, while the backward-scattered power is the spontaneous Raman scattered power measured at the input end of the optical fiber. For the forward-scattered power, we obtain the total forward-scattered power $raman_f^P$ by multiplying $dP(z)$ by $\exp(-\alpha_r(L-z))$ (where α_r is the loss coefficient of the spontaneous Raman scattered light) and integrating along the length of the optical fiber. Under the condition that $\alpha_p \approx \alpha_r$, we derive an approximate formula for the forward-scattered power. For the backward-scattered power, we obtain the total backward-scattered power $raman_b^P$ by multiplying

DOI: 10.54254/2755-2721/119/2025.19330

$dP(z)$ by $\exp(-\alpha_r * z)$ and integrating along the length of the optical fiber. Similarly, under the condition that $\alpha_p \approx \alpha_r$, we derive an approximate formula for the backward-scattered power. The specific formulas are:

$$raman_f^P = \int_0^L \eta P_P(0)\exp(-\alpha_p z) \times \exp[-\alpha_r(L-z)]dz = \frac{\eta P_P(0)}{\alpha_r - \alpha_p}\{\exp[-\alpha_p L] - \exp[-\alpha_r L]\} \quad (5)$$

If $\alpha_p \approx \alpha_r$, the forward scattering power is approximated as

$$raman_f^P \approx \eta P_P(0)\exp(-\alpha_p L)L \quad (6)$$

$$raman_f^P = \int_0^L \eta P_P(0)\exp(-\alpha_p z) \times \exp[-\alpha_p z]dz = \frac{\eta P_P(0)}{\alpha_r + \alpha_p}\{\exp[\alpha_p L] - \exp[-\alpha_r L]\}\exp[-\alpha_p L] \quad (7)$$

If $\alpha_p \approx \alpha_r$, the backward scattering power is approximated as

$$raman_b^P \approx \frac{\eta P_P(0)}{2\alpha_p}\{1 - \exp(-2\alpha_p L)\} \quad (8)$$

If we can solve the issue of power degradation, then this combination could be possible.

5. Results discussion

Current research is mainly focused on the 6G architecture itself, or on the quantum key distribution protocol and rate. This study focuses on applying quantum communication technology to the 6G fronthaul optical architecture, which has the advantages of high security and low cost, and can be well compatible with the 5G architecture.

QKD-Secured 6G fronthaul communication architecture leverages the principles of quantum mechanics to ensure the security of information transmission. Due to the non-clonability of quantum states, any attempt to eavesdrop on the key exchange will be immediately detected, thereby guaranteeing the absolute security of key distribution. It boasts ultra-low latency characteristics, which enhance the efficiency of QKD. In a high-speed, low-latency network environment, QKD can generate and distribute keys more rapidly, fulfilling the requirements of real-time communication and encryption. Beyond traditional wired and wireless network environments, it can also be integrated with new-generation communication methods such as satellite communications and drone communications, enabling secure communication globally.

It offers extremely high security, ultra-low latency, and broad applicability. Quantum communication technology has made remarkable advancements, leveraging the principles of quantum mechanics, particularly the non-clonability of quantum states and quantum entanglement, to ensure the security of information transmission. 6G's high data rates support the rapid transfer of large volumes of data, low latency ensures real-time key distribution, and high reliability guarantees the stability and security of communication. These factors provide strong support for the implementation of quantum communication solutions.

6. Conclusion

By establishing quantum transmitters and receivers at the AUU and DU sites and encrypting transmitted information using quantum keys, our proposed QKD-Secured 6G fronthaul communication architecture addresses the security requirements of the 6G communication process. This architecture not only enhances communication security but also enables innovative applications. The feasibility of this architecture is demonstrated through solutions for noise analysis and secure key rate optimization. Specific scenarios for the combined application of 6G and QKD include: High-Security Industries: In sectors such as government, military, and finance, data security is paramount.

DOI: 10.54254/2755-2721/119/2025.19330

The integration of 6G and QKD offers end-to-end secure communication solutions, ensuring data confidentiality and integrity during transmission. Connected Vehicles and Autonomous Driving: In autonomous driving and connected vehicle applications, real-time data transmission and security are equally critical. The combination of 6G and QKD can provide ultra-secure communication links, ensuring that data transmitted between vehicles and central control systems is protected from hacking or malicious tampering. These specific scenarios highlight the potential and versatility of combining 6G and QKD technologies to enhance security across various industries and applications. As technology continues to advance, we anticipate more innovative and secure solutions emerging from this powerful combination.

References

[1] *Andrews, Jeffrey G. , et al. "What Will 5G Be?." IEEE Journal on Selected Areas in Communications 32.6(2014):1065-1082.*

[2] *Bogale, Tadilo , and L. Le . "Massive MIMO and mmWave for 5G Wireless HetNet: Potential Benefits and Challenges." IEEE Vehicular Technology Magazine 11.1(2016):64-75.*

[3] *Zhou, Zhou , et al. "Deep Reservoir Computing Meets 5G MIMO-OFDM Systems in Symbol Detection." Proceedings of the AAAI Conference on Artificial Intelligence (2020).*

[4] *Bojkovic, Zoran , and D. Milovanovic . "A Technology Vision of the Fifth Generation (5G) Wireless Mobile Networks." Springer, Cham (2016).*

[5] *Bourbah, Ayoub , et al. "The Next-Generation 6G: Trends, Applications, Technologies, Challenges, and Use Cases." (2023).*

[6] *Tonkikh, E. V. , K. D. Burobina , and A. A. Shurakhov . "Possible Applications of Sixth Generation Communication Networks." Systems of Signals Generating and Processing in the Field of on Board Communications 2020.*

[7] *Liang, Chen , and Y. U. Shao-Hua . "Preliminary Study on the Key Technologies of 6G Mobile Communication." Study on Optical Communications (2019).*

[8] *Eldrandaly, Khalid , et al. "Green Communication for Sixth-Generation Intent-Based Networks: An Architecture Based on Hybrid Computational Intelligence Algorithm." Hindawi Limited (2021).*

[9] *Bourbah, Ayoub , et al. "The Next-Generation 6G: Trends, Applications, Technologies, Challenges, and Use Cases." (2023).*

[10] *Gundu, Srinivasa Rao , et al. "Sixth-Generation (6G) Mobile Cloud Security and Privacy Risks for AI System Using High-Performance Computing Implementation." Wireless Communications and Mobile Computing (2022).*

[11] *C.H Bennett,and G.B Brassard,"Quantum cryptography:Public-key distribution and coin tossing",Proceedings of IEEE International Conference on Computers,Systems and Signal Processing,Bangalore,India,December 1984.*

[12] *Lim, Kyongchun , C. Suh , and J. K. K. Rhee . "Longer distance continuous variable quantum key distribution protocol with photon subtraction at receiver." Quantum Information Processing 18.3(2018).*

[13] *Wong, E. , K. L. Lee , and T. Anderson . "Low-cost WDM passive optical network with directly-modulated self-seeding reflective SOA." Electronics Letters 42.5(2006):299-301.*

[14] *Azmi, F. H. , N. F. Naim , and Ya'acob N.Sarnin S.S.Supian L.S. "Design of time division multiplexing/wavelength division multiplexing passive optical network system for high-capacity network." international journal of electrical and computer engineering 13.4(2023):4152-4158.*

[15] *Wang, Xiang Bin . "Decoy-state protocol for quantum cryptography with four different intensities of coherent light." Physical Review A 72.1(2005):12322-012322.*

[16] *Máttar, Alejandro, et al. "Device-independent quantum key distribution with single-photon sources." (2018).*

[17] *Zhao, Y. . "Experimental Quantum Key Distribution with Decoy States." Physical review letters 96.7(2006):070502.*

[18] *Zaitcev, A. I. , et al. "Quantum Key Distribution Through a Multi-Core Optical Fiber." 2023 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) (2023):1-4.*

[19] *Yi Zhao,Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber,IEEE International Symposium on Information Theory(2006) 2094-2098.*