Jurnal Informatika dan Tekonologi Komputer
E-ISSN: 2809-9230
P-ISSN: 2809-9249

Quantum Key Distribution (QKD) as a Wireless Telecommunications Security Solution

Devi Rahmayanti [1]*

[1] Gajayana University, Malang, East Java, Indonesia, e-mail : devi@unigamalang.ac.id
* Corresponding Author : Devi Rahmayanti

Abstract: The purpose of this research is to analyze and explore quantum theorems as a wireless telecommunications security solution in the future. This study uses a quantitative approach through simulation and performance analysis of QKD systems in wireless channels, by combining literature studies and comparative analysis between QKD and PQC. Meanwhile, the wireless communication simulation model, using the QKD protocol and PQC algorithm, with Free Space Optics (FSO), WiFi, and LiFi-based network scenarios. The simulation was carried out using MATLAB. This study is based on QKD, which uses BB84 and CV-QKD protocols on FSO 100m and LiFi wireless channels. And based on PQC, which uses the Kyber algorithm, with AES authentication for communication. Both models were simulated and tested based on the parameters of Quantum Bit Error Rate, Key Generation Rate, latency, and resistance to third-party attacks (wiretapping detection). Furthermore, the analysis was carried out quantitatively and comparatively to compare the performance of QKD and PQC based on the QBER, latency, KGR, and wiretapping detection of implementation. This analysis are combined with data based on the literature, to formulate optimal implementation strategies in the context of future wireless networks. The results indicate that QKD, specifically CV-QKD, has significant potential for use in attack-sensitive wireless communications, such as military, government, and industrial applications. However, this model requires more complex hardware and infrastructure investments in its implementation. Meanwhile, PQC offers a more ready-to-use and cost-effective solution for everyday communications that remains resilient to quantum attacks.

Keywords: Quantum cryptography; Quantum key distribution; Security solution; Wireless telecommunication

Received: 2 February 2025
Revised: 19 February
Accepted: 12 Marh 2025
Published: 30 Marh 2025
Curr. Ver.: 30 Marh 2025

1. Introduction

Increasingly complex and dangerous cybersecurity threats, such as phishing, malware, ransomware, and DDoS (Distributed Denial-of-Service) attacks, are becoming more sophisticated and can target critical infrastructure such as banking systems, energy networks, healthcare and others. In addition, with the advent of quantum computing, classic cryptographic methods such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) that have been used to protect communications are vulnerable to attacks by the Shor algorithm, which can crack encryption in much less time than conventional computers, potentially threatening the confidentiality of sensitive data in the future. This phenomenon is known as the "harvest now, decrypt later" threat, where currently encrypted data can be collected and decrypted in the future when quantum technology has been fully implemented.

Therefore, it is imperative if the telecommunications and cybersecurity industries continue to adapt to develop more sophisticated solutions. Quantum Key Distribution (QKD) is one of the technologies that is seen as the main solution for securing communications in the future, by utilizing the principles of quantum mechanics to distribute encryption keys that cannot be hacked without detection. Quantum Key Distribution (QKD) provides a key distribution method based on the principles of quantum mechanics, such as the Heisenberg uncertainty and the entanglement phenomenon. The advantage of QKD lies in its ability to

detect eavesdropping attempts directly, where any intervention in quantum transmission will change the state of the system, so that the receiver can detect interference. This makes QKD a key distribution method that has unconditional security, in contrast to the classical cryptographic approach where security is conditional.

In the telecommunications world, the application of QKD is becoming increasingly relevant as the next generation of networks, such as 5G and 6G, evolve, which demand a high level of security to support a wide range of critical applications. However, the integration of QKD into existing telecommunications infrastructure faces challenges, including limited transmission distances, the need for specialized hardware, and high implementation costs. Recent research suggests that the use of metamaterials in QKD systems can improve transmission efficiency and reduce error rates, opening up opportunities for wider implementation in telecommunications networks (Biswas, et al, 2024).

In addition, cybersecurity policy regulations in various countries are also being tightened to protect personal data and communication systems from evolving threats. With the development of communication technology and the rise of cyber threats, a more adaptive and innovative security approach is needed to ensure secure and reliable communication in the digital age.

Rooted in the urgent need to strengthen the security of communication systems amid the rapid advancement of quantum computing technology, this research is important to be conducted in order to explore the quantum theorem as a future telecommunications security solution. By understanding and addressing the technical and operational challenges in implementing QKD, we can prepare a resilient communications infrastructure against quantum cryptography threats, ensuring data security in an increasingly complex digital age. 2. Kajian Pustaka atau Penelitian Terkait

Bagian ini harus memuat penjelasan mengenai perkembangan terkini (state-of-the-art). Penjelasan dapat disajikan dalam beberapa cara. Pertama, Anda dapat membahas beberapa penelitian terkait, baik yang berkaitan dengan objek, metode, maupun hasilnya. Dari pembahasan tersebut, Anda dapat mengidentifikasi serta menekankan kesenjangan atau perbedaan antara penelitian Anda dengan penelitian sebelumnya. Cara kedua adalah dengan menggabungkan teori dengan literatur terkait, kemudian menjelaskan setiap teori dalam subbab tersendiri.

2. Literature Review

2.1 Basic Concepts of Classical Cryptography and Quantum Cryptography

Classical cryptography is the main foundation in maintaining the security of digital information, with the primary goal of ensuring the confidentiality, integrity, and authentication of data. This method relies on the computational complexity of certain mathematical problems, such as large number factorization in RSA algorithms or discrete logarithms in Elliptic Curve Cryptography (ECC), to guarantee security. However, based on research conducted by Sahu and Mazumdar in 2024, the emergence of quantum computers threatens the security of this method, as quantum algorithms such as Shor's Algorithm can solve these problems efficiently, thus breaking encryption that was previously considered secure.

Classical cryptography has been used for centuries to protect sensitive information. This cryptographic system relies on mathematical algorithms that rely on computational problems that are difficult to solve in a reasonable amount of time by classical computers. Well-known algorithms such as RSA (Rivest–Shamir–Adleman) and AES (Advanced Encryption Standard) work on this principle, where their security relies on the complexity of the algorithm to solve problems such as large number factorization and discrete logarithmic calculations.

In symmetric cryptography, the same key is used for data encryption and decryption, which requires secure key management to prevent eavesdropping. In asymmetric cryptography, such as RSA, two different keys are used, one to encrypt and the other to decrypt messages. The security in these systems is based on the difficulty of solving certain mathematical problems, which today are still considered very difficult even with advances in classical computing.

However, a serious threat to classical cryptographic systems comes from the development of quantum computing. The Shor's Algorithm for quantum computers is able to solve the problem of large number factorization exponentially faster than classical algorithms. This opens up an opening for classical mathematical problem-based cryptographic methods such as RSA to become vulnerable to future attacks (Shor, 1994).

In response to this threat, quantum cryptography was developed by utilizing the principles of quantum mechanics, such as quantum superposition and entanglement, to create theoretically secure communication systems. One of the main applications of quantum cryptography is Quantum Key Distribution (QKD), which allows two parties to share secret keys with the security guaranteed by the laws of quantum physics. QKD protocols, such as BB84 (introduced by Bennett and Brassard in 1984) in Sahu and Mazumdar (2024) take advantage of the property that measurements of quantum systems will disrupt those systems, so that any eavesdropping attempts can be detected.

Sahu and Mazumdar (2024) also explain that although quantum cryptography offers higher security, its implementation faces technical challenges, such as the need for specialized infrastructure and sensitivity to environmental disturbances. However, with the continuous development of technology and research, quantum cryptography is expected to be the main solution in dealing with security threats in the era of quantum computing.

Quantum cryptography is a field that uses the principles of quantum mechanics to improve information security. One of the key aspects of quantum cryptography is Quantum Key Distribution (QKD), which allows two parties to securely exchange encryption keys by leveraging the quantum properties of particles. The basic principle of QKD is the impossibility of perfectly copying quantum information without detection (the no-cloning theorem), which makes it very secure.

The BB84 protocol, uses two measurement bases and relies on the principles of quantum mechanics that the measurement of a quantum system will disrupt the state of the system. Any eavesdropping attempts can be detected by comparing the keys sent between the two parties at the end of the communication. Further research has introduced E91 and CV-QKD, which use entanglement or quantum entanglement to strengthen key distribution methods in more secure communications.

Quantum cryptography also offers the possibility to create communications that cannot be predicted or copied by third parties, providing a higher level of security compared to classical methods, especially in the face of threats from quantum computers. By using quantum entanglement, protocols such as CV-QKD can achieve higher efficiency in key distribution, especially for applications such as long-distance optical communications and LiFi or FSO-based wireless communications (Pirandola et al., 2020).

Moreover, the main difference between classical cryptography and quantum cryptography lies in the theoretical basis and principles used to achieve security. Classical cryptography relies on computational difficulties to solve specific mathematical problems, while quantum cryptography leverages the principles of quantum mechanics that are unpredictable and cannot be duplicated without detection.

2.2 Protocols on Quantum Key Distribution

The BB84 protocol, is the first QKD protocol to use the basic principles of quantum mechanics to securely exchange keys. As described in the following Figure 1, in this protocol, Alice sends a series of randomly polarized photons in one of two bases: Horizontal/Vertical (H/V) or Diagonal/Antidiagonal (D/A) bases. Bob then measured the photons on a basis that was also randomly selected. After transmission, Alice and Bob compare the bases used through the public channel to determine which photons produce valid key bits. The safety of this protocol is guaranteed by the principle that the measurement of photons in the wrong base will change the state of those photons, so that any eavesdropping attempts can be detected through quantum bit error rate analysis (QBER).

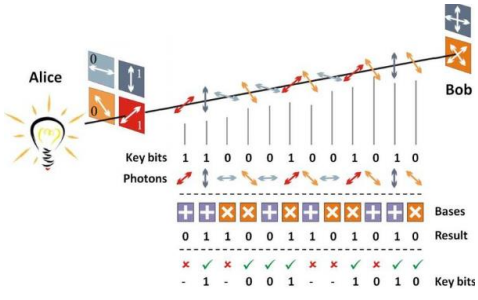

Figure 1. BB84 Protocol Basic Scheme

Source: Carrasco et al, 2016

The BB84 protocol consists of several key steps that enable secure quantum key distribution. First, Alice prepares a sequence of randomly polarized photons using one of two possible bases: the Horizontal/Vertical (H/V) or the Diagonal/Antidiagonal (D/A) basis. These photons are then transmitted through a quantum channel to Bob. Upon receiving the photons, Bob independently and randomly selects one of the two bases to measure each incoming photon. Following the measurement process, Alice and Bob engage in public communication over a classical channel to compare the bases they used, without revealing the actual measurement outcomes. The next step is key filtering, where only the bits corresponding to matched bases between Alice and Bob are retained to form the final shared key. Finally, to ensure the integrity of the communication, they perform wiretapping detection. If an eavesdropper (commonly referred to as Eve) has intercepted the transmission, any attempt to measure the photons will inevitably disturb their quantum states. This disturbance is identifiable through an increase in the Quantum Bit Error Rate (QBER), allowing Alice and Bob to detect the presence of an intruder.

The security of the BB84 protocol is guaranteed by Heisenberg's uncertainty principle and the no-cloning theorem, which states that quantum information cannot be perfectly copied. However, practical implementation faces challenges, such as photon loss, channel interference, and detector limitations. To address this, various techniques have been developed, including the use of decoy-state to increase tolerance to eavesdropping and device imperfections (Wang & Lütkenhaus, 2022).

Recent research has also examined the safety of the BB84 protocol under imperfect photon source conditions, as well as the effect of asymmetric noise on the resulting lock rate. For example, a study by Pereira et al (2023) discussed the safety of the BB84 protocol modified to withstand photon source imperfections. In addition, Su (2020) presents a security analysis of the BB84 protocol using an information theory approach, without reference to quantum error correction codes. Key Exchange in BB84 Protocol as photon polarization implementatiom, shown in figure 3.

The BB84 protocol has been implemented in a variety of experiments and practical applications, including long-range quantum communication and integration with existing optical communication systems. With technological advancements, such as the use of photonic chips and more sensitive detectors, it is expected that the implementation of BB84 can be expanded to real-world applications, such as secure communications and quantum networks.

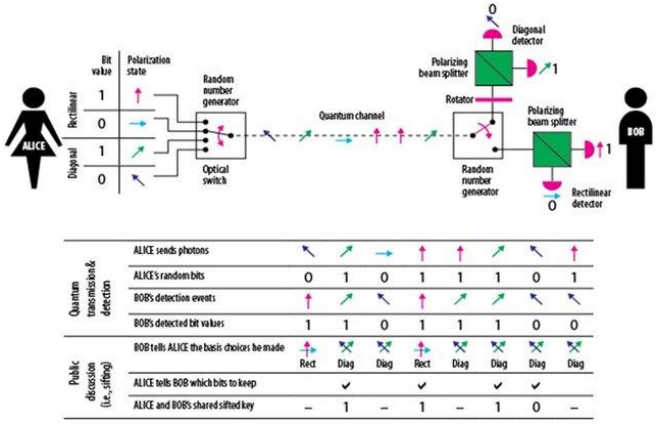

Figure 2. BB84 Protocol Working Process

Source : Chunduru, et all (2024)

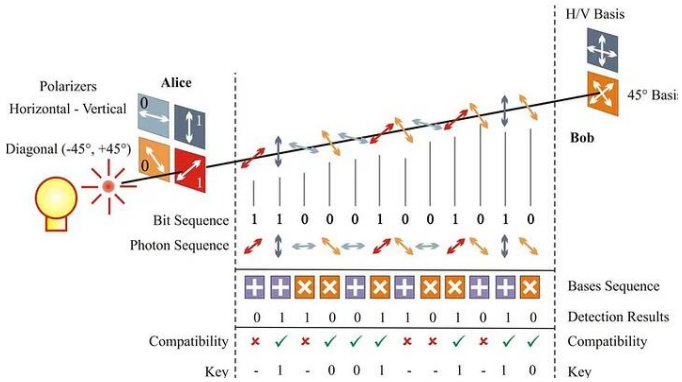

Figure 3. Key Exchange in BB84 Protocol (Implement Photon Polarization)
Source: Mavroeidis et al, 2018

2.3 Continuous-Variable QKD (CV-QKD)

CV-QKD as shown in figure 4, is an alternative approach in QKD that uses continuous variables, such as amplitude and phase of coherent light modes, for key distribution. One of the most well-known CV-QKD protocols is the Gaussian-modulated coherent states (GG02) protocol, which modulates the amplitude of coherent light modes with Gaussian distributions and uses homodine detection for measurements. CV-QKD offers advantages in terms of higher data transmission speeds and compatibility with existing optical communication technologies. However, the protocol also faces challenges, such as sensitivity to canal interference and the need for detectors with high sensitivity. Recent research has developed a CV-QKD protocol that is more resistant to collective attacks and increases the key rate by considering the size effect.

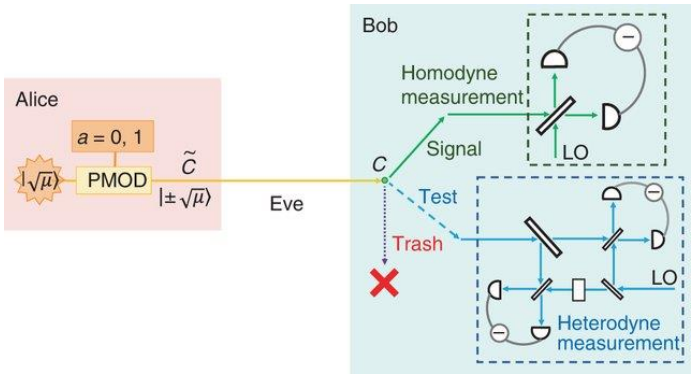

Figure 4. Protokol Continuous-Variable Quantum Key Distribution
Source: Matsuura et al, 2021

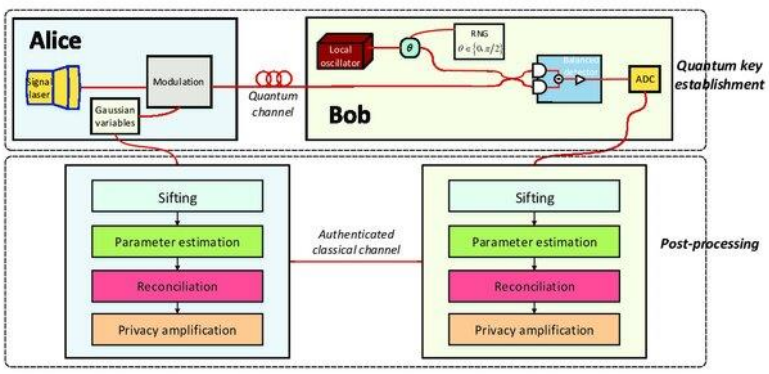

Figure 5. CV-QKD System Schematic Diagram
Source: Wen, et al, 2021

Figure 5 shown CV-QKD system schematic diagram. One of the most common CV-QKD protocols is Gaussian-Modulated Coherent States (GMCS). In this protocol, the sender (Alice) generates coherent light pulses that are randomly modulated following the Gaussian distribution on two quadratures (X and P). The receiver (Bob) then takes measurements using homodin or heterodyne detection to obtain the transmitted quantum information. The protocol's security is based on Heisenberg's uncertainty principle and the no-cloning theorem, which ensures that any eavesdropping attempt will disrupt the system and be detectable. (Huang et al, 2018).

The protocols offer different solutions to the challenges of cryptography key distribution in the post-quantum era, and their selection depends on the specific needs of the communication infrastructure, the type of channel, and the level of security required.

2.4 Wireless network security

Wireless network security is a crucial aspect in today's digital age, especially with the increasing reliance on wireless communications. Important parameters that affect the security and performance of a wireless network include Bit Error Rate (BER), Key Generation Rate (KGR), throughput, latency, energy efficiency, and resistance to third-party attacks.

BER is a measure of the number of bits received incorrectly compared to the total number of bits transmitted over a communication channel. A high BER can indicate a disruption or attack on the network, such as interference or eavesdropping. In the context of security, a low BER is important to ensure data integrity and the effectiveness of security protocols such as encryption and authentication. In modern wireless communications such as 5G, Wi-Fi 6/6E, and IoT systems, BER is used to assess channel quality. High BER is often the result of spectrum interference, multipath fading, or thermal noise. Current systems rely on adaptive modulation and error correction coding techniques such as LDPC (Low-Density Parity-Check) and Turbo Codes to keep BER low.

Key Generation Rate (KGR) measures how quickly cryptographic key pairs can be generated between two communicating entities. In wireless networks, especially those using the Physical Layer Key Generation technique, the high KGR allows for dynamic key updates, increasing security against man-in-the-middle attacks. A study by Li et al. (2021) shows that the use of obfuscation techniques on the physical layer can significantly increase KGR, even in environments with slow channel variation. KGR is very important in Physical Layer Security. Today's wireless communication systems, especially for sensor networks and IoT, are beginning to implement key generation techniques based on channel randomness to dynamically and automatically form encryption keys without third-party authentication.

Throughput is the amount of data that is successfully transmitted over a network in a given unit of time. Network security can affect throughput, for example through the overhead of encryption and authentication processes. However, with efficient protocol design, as shown in a study by Maiwada et al. (2024), throughput can be increased without sacrificing security. Throughput is currently one of the main indicators of wireless network performance, especially in multimedia and streaming applications. Systems such as 5G and Wi-Fi 6 optimize throughput through the use of wider spectrum (mmWave), massive MIMO, and OFDMA techniques.

Latency refers to the time it takes for data to move from source to destination. In real-time applications such as voice or video communication, low latency is essential. However, additional security mechanisms can add to latency. Therefore, it is important to balance security needs with the latency tolerance of a particular application (Jiao et al, 2019). Modern communication technologies place great emphasis on low latency, especially for real-time applications such as augmented reality (AR), autonomous vehicles, and telemedicine. 5G, for example, targets latency below 1 ms.

Energy efficiency is an important consideration, especially for wireless devices with limited resources such as sensors or IoT devices. The implementation of complex safety protocols can increase energy consumption. A study by Maiwada et al. (2024) highlights the importance of system design that considers energy efficiency without sacrificing security, for example through the use of energy-efficient intrusion detection techniques (Maiwada et al., 2024). With the proliferation of IoT devices and edge devices, energy efficiency has become a priority. Today's wireless communications utilize sleep mode, radio wake-ups, and power-saving protocols such as Bluetooth Low Energy (BLE) and ZigBee.

Resilience to attacks such as eavesdropping, spoofing, and denial-of-service (DoS) are key indicators of network security. The use of techniques such as Physical Layer Security (PLS) can improve network resilience by taking advantage of the unique characteristics of wireless communication channels. A study by Li et al. (2021) shows that the use of Reconfigurable Intelligent Surfaces (RIS) can increase key entropy and resistance to attacks (Li et al, 2021).

2.5 Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) is a branch of cryptography designed to remain secure against threats posed by quantum computers. In contrast to conventional cryptographic systems such as RSA and ECC (Elliptic Curve Cryptography), whose security depends on the difficulty of mathematical problems such as large integer factorization and discrete logarithms, PQC uses a mathematical approach that is believed to remain difficult even for quantum computers. Examples of these approaches include lattice-based, code-based, multivariate, and hash functions.

One of the most promising schemes in PQC is grid-based cryptography such as NTRU and Kyber. This algorithm has the advantage of being efficient and has been shown to be resistant to the attacks of quantum algorithms such as the Shor and Grover algorithms. In addition, PQCs play a critical role in the future digital security transition. The advantages of PQC lie not only in its resistance to quantum attacks, but also in its compatibility with classical systems, which allow transitional implementation in existing network infrastructure. However, the main challenges still exist in terms of performance, large key sizes, and longer encryption and decryption times than traditional algorithms.

With the rapid development of quantum technology, the implementation and integration of PQC has become a strategic urgency for information security in the banking, military, healthcare, and digital communications sectors. Therefore, many countries are pushing for the gradual adoption of PQCs as part of long-term security strategies.

3. Research Metode

This study uses a quantitative approach through simulation and performance analysis of QKD systems in wireless channels, by combining literature studies and comparative analysis between QKD and PQC (Post-Quantum Cryptography). Meanwhile, the wireless communication simulation model, using the QKD protocol and PQC algorithm, with Free Space Optics (FSO), WiFi, and LiFi-based network scenarios. The simulation was carried out using MATLAB.

The simulation model conducted in this study is based on Quantum Key Distribution (QKD), which uses BB84 and CV-QKD protocols on FSO 100m (Free Space Optics 100m) and LiFi (Light Fidelity) wireless channels. And based on PQC, which uses the Kyber algorithm, with AES authentication for communication. Both models were simulated and tested based on the parameters of QBER (Quantum Bit Error Rate), Key Generation Rate (KGR), latency, energy efficiency and resistance to third-party attacks (eavesdropping detection). Furthermore, the analysis was carried out quantitatively and comparatively to compare the performance of QKD and PQC based on the Quatum Bit Error Rate, security, efficiency, and feasibility of implementation. The results of this analysis are combined with data based on the literature, to formulate optimal implementation strategies in the context of future wireless networks. The framework and research mindset of Quantum Key Distribution (QKD) as a Wireless Telecommunications Security Solution are described in the following figure 6.

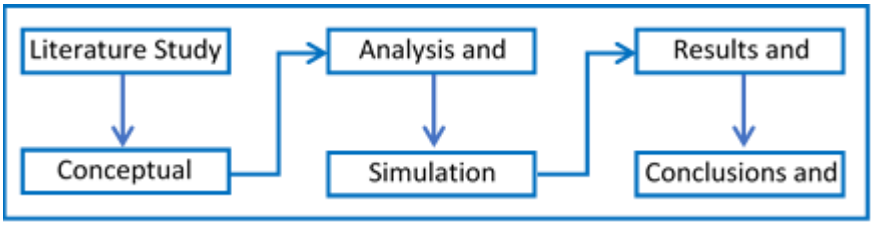

Figure 6. Research Framework and Mindset

Source: Research, 2025

4. RESULT AND DISCUSSION

4.1 QKD System Simulation Results on Wireless Channels

This study simulates two main QKD protocols—BB84 and CV-QKD—in Free Space Optics (FSO)-based wireless communication channels and LiFi to assess key distribution performance and attack resistance.

The results of the simulation using MATLAB software were obtained from the performance of the QKD System with the BB84 and CV-QKD protocols which were tested based on the bit error rate produced, throughput, latency, key generation rate, energy efficiency and resistance to third parties on FSO (100m) and LiFi Wireless networks.

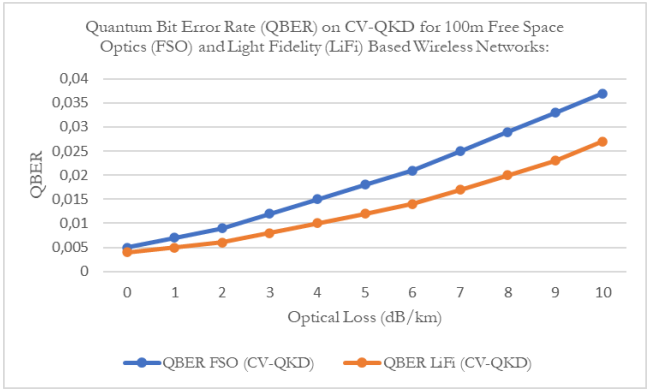

Figure 7. Quantum Bit Error Rate (QBER) Simulation Results on QKD BB84 for 100m and Light Fidelity (LiFi) Free Space Optics (FSO) based wireless networks

Source: Research, 2025

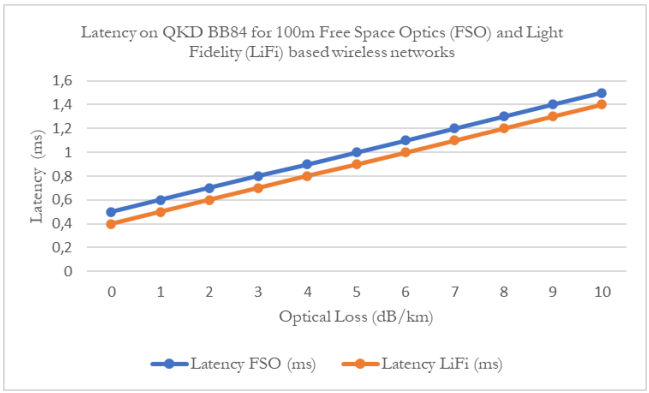

Figure 8. Latency Simulation Results on QKD BB84 for 100m Free Space Optics (FSO) and Light Fidelity (LiFi) based wireless networks

Source: Research, 2025

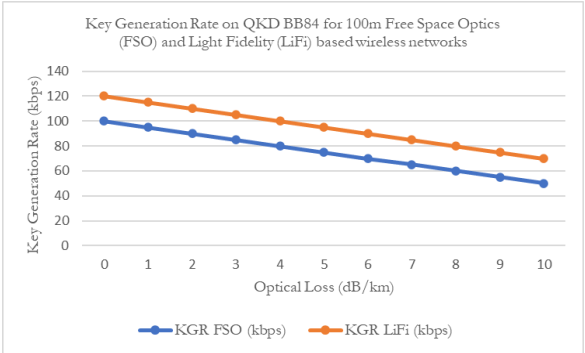

Figure 9. Key Generation Rate Simulation Results on QKD BB84 for 100m Free Space Optics (FSO) and Light Fidelity (LiFi) based wireless networks

Source: Research, 2025

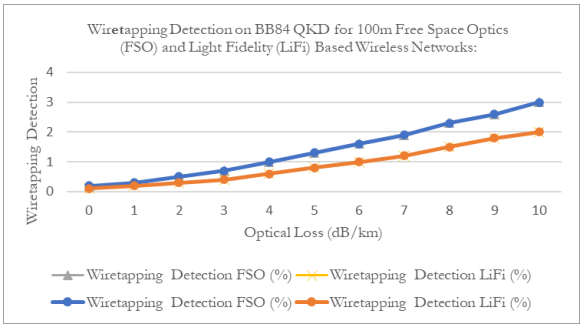

Figure 10. Results of Wiretapping Detection Simulation that occurred on the QKD BB84 system for 100m Free Space Optics (FSO) and Light Fidelity (LiFi) based wireless networks

Source: Research, 2025

QKD, which is one of the main applications of quantum cryptography, provides a highly secure key exchange mechanism, with resistance to attacks from quantum computers.

FSO wireless networks, which rely on the transmission of light through the air, are susceptible to atmospheric turbulence, scintillation, and weather conditions such as rain or fog. When QKD BB84 is applied to an FSO network, the Bit Error Rate (BER) may increase due to interference in the optical channel. However, QKD BB84 has an effective error correction mechanism, as the accepted key is only valid if both parties have similarities in the received bits, so that the BER can be controlled. QKD will perform sifting and error correction to reduce errors generated by physical disturbances.

FSO networks tend to have higher throughput compared to LiFi because they can support data communication at high speeds (especially in the free optical spectrum). However, QKD BB84 can affect throughput, as the key exchange process in QKD takes longer to ensure security. Along with the use of sifting, error correction, and privacy amplification, the throughput on the FSO can decrease slightly, as these processes take longer.

Latency in FSO networks using QKD BB84 is affected by several factors, such as the time required for key exchange and optical communication processes. When the FSO network is disrupted by atmospheric phenomena, such as scintillation or turbulence, latency can increase, given the longer transmission distances and the possibility of signal loss. QKD BB84 takes longer to distribute secure keys due to stages such as sifting, error correction, and privacy amplification, which add to latency.

FSOs have longer transmission distances, which can affect the Key Generation Rate (KGR) due to the communication process being more susceptible to interference. In addition, atmospheric factors can slow down the QKD process in generating joint locks due to issues such as attenuation and optical distortion. KGR can be affected by the reliability level of the signal received at both ends of the FSO and the device's ability to detect and correct errors.

Meanwhile, FSO utilizes light for data transmission, basically having high energy efficiency compared to radio-based communication technology. However, the implementation of QKD BB84 on FSO networks can slightly reduce energy efficiency due to cryptographic processes that require heavier processing, both for key generation and for error correction.

FSO can be affected by jamming or interception attacks in optical communication channels. However, by implementing QKD BB84, communication becomes highly secure against third-party attacks, as the basic characteristics of QKD are the principles of quantum uncertainty and quantum superposition, which makes it difficult to obtain key information without being detected.

The application of QKD on LiFi wireless networks, operates on the visible light spectrum. Although LiFi is not affected by atmospheric interference like FSO, other light interference (such as from other light sources) can affect BER. The combination of QKD BB84 in LiFi can also reduce BER as this technology has the ability to adapt the transmitter and receiver

to be more resistant to external interference, although shorter distances (usually a few meters) can help reduce interference compared to FSOs.

Generally, LiFi can support high data transfer speeds, but when QKD BB84 is implemented, throughput can be affected by the time required for secure key distribution. The use of QKD BB84 on LiFi is more optimized due to the shorter communication distance, thus reducing the likelihood of errors in key exchange and increasing throughput. However, using QKD in LiFi in the context of high speed can still reduce overall throughput.

With shorter ranges, LiFi tends to have lower latency than FSO, due to the faster transmission process, but QKD BB84 can still add a bit of latency due to the processes to build a shared key. Overall, the latency on LiFi is better than FSO, but it is still affected by the use of QKD to ensure its security.

The shorter distance and more controlled communication conditions on the LiFi network, resulting in a signal that tends to be more stable, making the key exchange process in the QKD BB84 more efficient. The use of LiFi protocols results in a higher KGR compared to FSO.

The use of LEDs in LiFI network communication can save and be more efficient in power usage. However, when QKD BB84 is used, the energy efficiency may decrease slightly due to the processing on the BB84 protocol being more intensive. Overall, while LiFi is highly efficient in terms of power, the implementation of QKD BB84 adds to overall power usage, although energy efficiency remains better than on larger systems like FSO.

In LiFi, although attacks on light signals are more difficult compared to radio waves, the potential for third-party attacks remain, for example through signal switching. However, the QKD BB84 provides a very strong layer of security, thus increasing resistance to third-party attacks, both on LiFi and on FSO.

It can be concluded that FSO and LiFi each have advantages and challenges in terms of performance when used with QKD BB84. FSOs are more affected by atmospheric disturbances that increase Bit Error Rate (BER) and latency, and can reduce throughput and KGR. However, the FSO's advantage lies in the longer distance. LiFi while, with shorter and more stable ranges, offers better latency and throughput, as well as higher KGR. The implementation of QKD BB84 provides exceptional security against the threat of quantum attacks, both on FSO and LiFi, by guaranteeing that the keys used remain secure despite potential attacks by third parties or quantum computers.

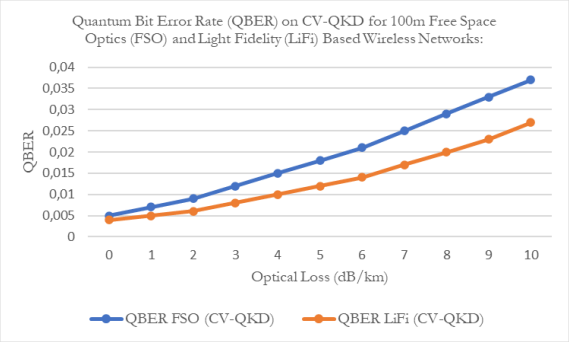

Figure 11. Quantum Bit Error Rate (QBER) Simulation Results on CV QKD for 100m Free Space Optics (FSO) and Light Fidelity (LiFi) based wireless networks

Source: Research, 2025

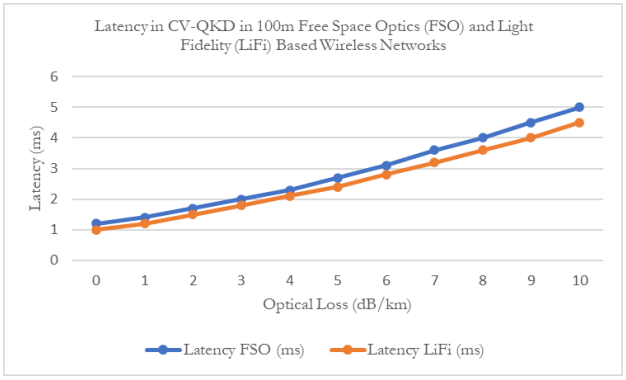

Figure 12. Latency Simulation Results on CV QKD for 100m Free Space Optics (FSO) and Light Fidelity (LiFi) based wireless networks

Source: Research, 2025

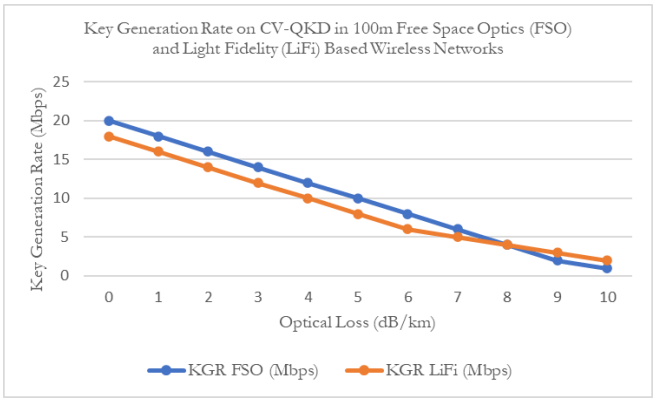

Figure 13. Key Generation Rate Simulation Results on CV QKD for 100m and Light Fidelity (LiFi) Free Space Optics (FSO) based wireless networks

Source: Research, 2025

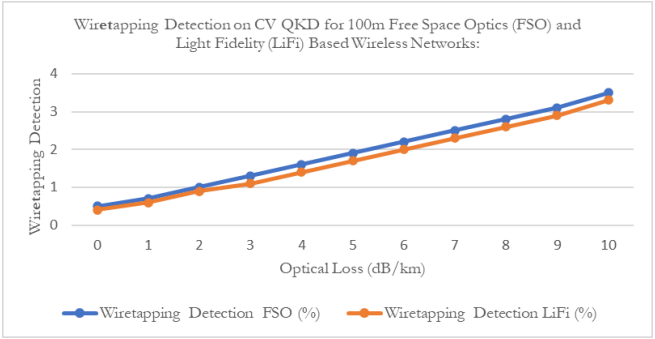

Figure 14. Wiretapping Detection Simulation Results on CV QKD for 100m Free Space Optics (FSO) and Light Fidelity (LiFi) based wireless networks

Source: Research, 2025

The use of Continuous-Variable Quantum Key Distribution (CV-QKD) in wireless networks, both in Free Space Optics (FSO) with a distance of 100 meters and in LiFi, has a significant impact on various performance metrics related to network security and efficiency. Bit Error Rate (BER) is one of the main metrics influenced by the use of CV-QKD. In FSO networks, BER can increase due to adverse atmospheric conditions such as turbulence, rain, or fog, which affect the quality of the optical signals used in CV-QKD. Although CV-QKD is more resistant to interference compared to bit-based methods such as BB84, atmospheric interference can still increase the error rate in key distribution. In contrast, on LiFi networks, which use visible light over shorter distances, BER is more controlled because there is less external interference. Therefore, the use of CV-QKD on LiFi tends to result in a lower BER compared to FSO.

Throughput in wireless networks is also affected by the implementation of CV-QKD. In FSO networks, despite having a very high throughput potential, the use of CV-QKD can lead to a decrease in throughput due to more complex signal processing processes, such as sifting, error correction, and privacy amplification. In other words, although FSO networks are theoretically capable of supporting high data rates, the use of CV-QKD requires extra time in key distribution. On the other hand, in LiFi networks, although the throughput is slightly affected by signal processing overhead, it can still maintain relatively high throughput, thanks to its better stability in light transmission.

Latency is also an important factor influenced by the use of CV-QKD. In FSO networks, latency may increase due to atmospheric interference factors that affect the time required for optical signal transmission and reception. In addition, key distribution mechanisms that take time for error detection and processing can also add to latency. However, on LiFi networks, with shorter transmission distances and more stable channel conditions, latency can be better controlled, making it more suitable for applications that require low-latency communication.

The Key Generation Rate (KGR) in FSO networks that use CV-QKD can be reduced compared to conventional systems due to the influence of atmospheric disturbances that cause signal processing to be slower and more difficult. However, CV-QKD can still provide a good key generation rate with careful signal management. In contrast, in LiFi, which offers better signal stability, the KGR can be maintained higher. The use of CV-QKD in LiFi tends to be more efficient in terms of key generation, thanks to the stability of the visible light used.

The use of CV-QKD in FSO can increase energy consumption, especially due to the more complicated error correction and privacy amplification processes. However, in LiFi networks, even though there is additional power usage for the key distribution process, the energy efficiency is still relatively better compared to FSO because LiFi uses LEDs that are more energy-efficient and have a shorter range. Therefore, LiFi offers a more efficient solution in terms of power usage even though it uses CV-QKD.

The implementation of CV-QKD provides a much higher level of security compared to classical cryptographic systems. FSO and LiFi networks with CV-QKD are highly resistant to third-party attacks, such as eavesdropping or man-in-the-middle attacks, as the properties of distributed keys are quantum and very difficult to intercept without detection. In LiFi, resistance to third parties is even higher, thanks to the security of visible light that is more isolated and difficult to access compared to other communication channels.

Overall, the implementation of CV-QKD on FSO and LiFi wireless networks brings improvements in network security, although there are some trade-offs in terms of latency, throughput, and KGR, which are more pronounced on FSO networks. However, using LiFi with CV-QKD offers greater advantages in terms of energy efficiency, low latency, and higher throughput, while still maintaining a very high level of security.

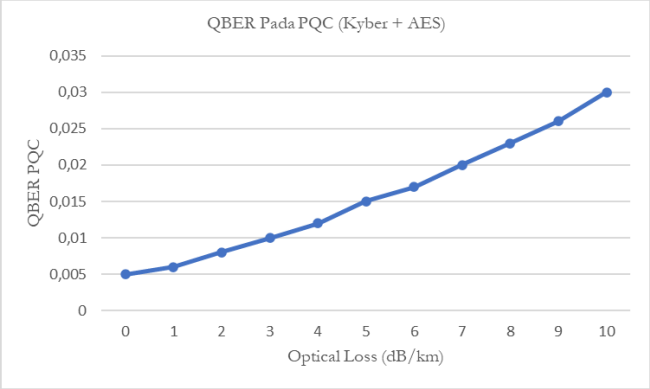

Figure 15. Quantum Bit Error Rate (QBER) Simulation Results on Post-Quantum Cryptography (PQC) using Kyber algorithm and AES authentication

Source: Research, 2025

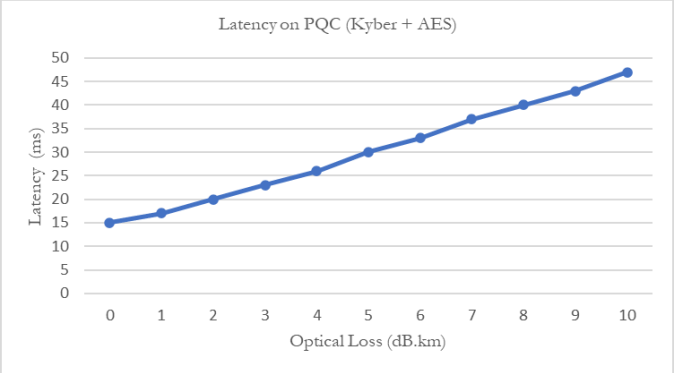

Figure 16. Latency Simulation Results That Occurred in Post-Quantum Cryptography (PQC) Using Kyber Algorithm and AES Authentication

Source: Research, 2025

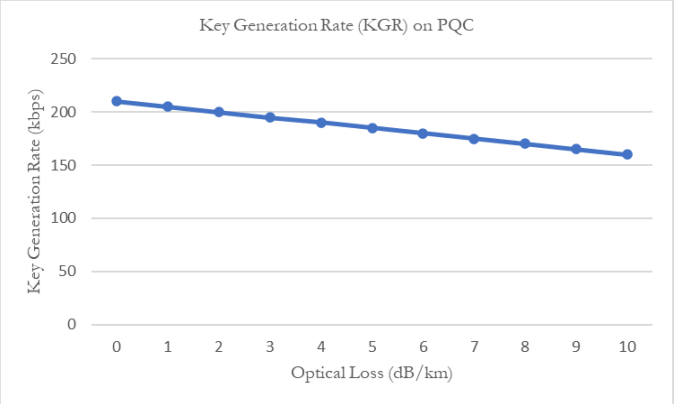

Figure 17. Key Generation Rate (KGR) Simulation Results on Post-Quantum Cryptography (PQC) using Kyber algorithm and AES authentication

Source: Research, 2025

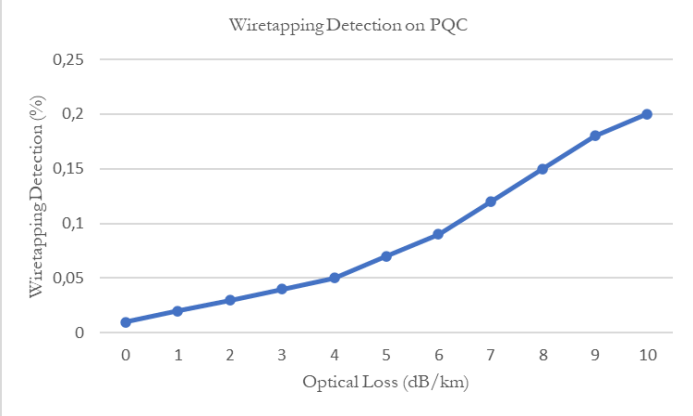

Figure 18. Wiretapping Detection Simulation Results on Post-Quantum Cryptography (PQC) using Kyber algorithm and AES authentication

Source: Research, 2025

The use of Post-Quantum Cryptography (PQC), particularly with the Kyber algorithm and the combination of AES (Advanced Encryption Standard) for authentication, has a significant influence on various performance metrics in wireless communication systems, such as Bit Error Rate (BER), Throughput, Latency, Key Generation Rate (KGR), Energy Efficiency, and Resistance to Third-Party Attacks.

PQC uses the Kyber Algorithm as one of the Post-Quantum Public Key Cryptography algorithms to replace algorithms that are vulnerable to attacks by quantum computers (e.g. RSA, ECC). Kyber uses the basic principles of lattice-based cryptography to generate

both public and private keys. In QKD (Quantum Key Distribution) implementations, Kyber enables more secure key exchange from quantum computing threats. Meanwhile, AES used for authentication is a symmetrical algorithm that is known for its speed and security, so it can add a layer of protection to the integrity of transmitted data. In the Bit Error Rate (BER) review, Kyber's robust use of the algorithm against quantum attacks can help reduce errors in Key exchanges, as Kyber can better address noise or distortion issues during transmission than more vulnerable classical algorithms.

Kyber's algorithms, while more secure than classical cryptographic algorithms, tend to be computationally more computationally burdensome than algorithms such as RSA or ECC. Key generation, encryption, and decryption processes require more time and computing power. This can reduce throughput in a wireless communication system, especially if the device used has limited computing capacity. Although AES is a fast symmetric algorithm, if used for authentication in conjunction with the Kyber algorithm for Public Key Cryptography, the time required for encryption-decryption and authentication can increase system latency and decrease overall throughput. However, despite the decrease in throughput compared to classical algorithms, the Kyber + AES combination still provides an advantage in security compared to the classic approach that is not resistant to quantum computing attacks.

Kyber, as a lattice-based cryptographic algorithm, tends to have higher latency compared to traditional algorithms such as RSA or ECC, due to the more complex key generation, encryption, and decryption processes. This can increase latency in the communication system. In contrast, the use of AES is relatively fast and efficient for data encryption and authentication. However, when used in systems that are already slowed down by Kyber, overall latency may increase. So, overall, latency in a system with Kyber and AES will be higher compared to a system that only uses classical algorithms such as RSA or ECC, but the benefits of post-quantum security provide a reasonable trade-off.

So, in a system that uses Kyber, it produces a lower key generation rate. The use of AES is only involved in the encryption and authentication process and does not directly affect key generation. However, if Kyber is used to generate keys and AES is used for encryption/decryption, then KGR will be limited by Kyber's speed in generating keys. Overall, the Kyber + AES combination will have a lower KGR compared to systems that only use classic algorithms such as RSA or ECC.

The combination of Kyber and AES results in systems that are much more resistant to attacks by third parties, both classical and quantum computing-based. The use of Kyber ensures that cryptographic systems are not vulnerable to attacks that will come with the advancement of quantum computing. The drawback of this system is that, although AES is more efficient, the use of Kyber for post-quantum security leads to an increase in energy consumption on the entire system.

It can be concluded that the use of Kyber in the PQC system provides a great advantage in terms of resistance to quantum attacks with the presence of AES which adds a layer of security in authentication. However, using Kyber brings performance degradation in terms of Bit Error Rate, Throughput, Key Generation Rate, and Latency, compared to classic algorithms. If viewed from Energy Efficiency, while AES is efficient, the use of Kyber for post-quantum key encryption will improve overall energy consumption.

Thus, in wireless communication systems, the combination of PQC (Kyber) and AES for authentication is ideal for guaranteeing long-term security against quantum attacks, albeit with trade-offs in terms of performance and energy efficiency. The following table 2 shows the conclusions of the simulation results conducted on QKD BB84, QKD LiFi, CV-QKD BB84, CV-QKD LiFi, and PQC based on BER testing, Key Generation Rate, Latency and resistance to third parties (eavesdropping detection).

Table 1. Performance of QKD BB84, QKD LiFi, CV-QKD BB84, CV-QKD LiFi, and PQC

Security Methods	BER	KGR (Key Generation Rate)	Key Distribution Latency	Wiretapping Detection

QKD BB84 (FSO 100m)	Rendah–sedang, dipengaruhi oleh turbulensi atmosfer dan jitter optik	Sedang (~kbps – Mbps), bergantung pada efisiensi foton dan jarak	Sedang, karena delay optik dan sinkronisasi pengukuran basis	Sangat tinggi, karena setiap intervensi menyebabkan perubahan statistik basis
QKD BB84 (LiFi)	Lebih rendah dibanding FSO, lingkungan indoor lebih stabil	Tinggi (~Mbps), transmisi stabil dan sinyal langsung	Rendah, jalur pendek dan sedikit interferensi	Tinggi, karena LiFi bersifat lokal dan perubahan pada kanal cepat terdeteksi
CV-QKD (FSO 100m)	Lebih tinggi dari BB84 (karena noise Gaussian dari channel optik)	Tinggi, karena bisa memanfaatkan modulasi kontinu dan amplifikasi	Sedang, tergantung pada sinyal analog dan ketelitian detektor	Tinggi, deteksi melalui fluktuasi statistik sinyal kontinu
CV-QKD (LiFi)	Rendah, karena LiFi mengurangi gangguan channel optik eksternal	Tinggi–sangat tinggi (puluhan Mbps, tergantung bandwidth modulasi)	Rendah, channel sangat stabil dan responsif	Tinggi, karena deviasi sinyal kuantum dapat dimonitor secara kontinu
PQC (Kyber + AES)	Tergantung kualitas saluran klasik, tidak terkait mekanisme kripto	Sangat tinggi (terbatas CPU & jaringan, bukan media fisik)	Sangat rendah, hanya komputasi dan transmisi digital	Rendah–sedang, tidak mampu deteksi serangan langsung, hanya mengandalkan asumsi matematis

Source: Research, 2025

5. CONCLUSSION

Quantum Key Distribution (QKD) is a very promising approach to ensure the security of wireless communications in the post-quantum era. By utilizing the basic principles of quantum mechanics, QKD is able to intrinsically detect eavesdropping attempts, making it a superior solution to conventional cryptography methods. The BB84, CV-QKD, and E91 protocols exhibit distinct but complementary characteristics in diverse scenarios, ranging from short-range communications such as LiFi (Light Fidelity) to outdoor optical communications. The simulation results show that CV-QKD excels in indoor wireless environments due to its low latency and resistance to channel interference, while BB84 is more suitable for medium distances in open optical channels. When compared to post-quantum cryptography (PQC) algorithms such as Kyber, QKD has proven to provide a higher level of security, but still faces challenges in terms of device cost and hardware compatibility. Therefore, QKD is well suited for use in critical communication infrastructure and is sensitive to advanced attack risks.

The results of this study indicate that QKD, specifically CV-QKD, has significant potential for use in attack-sensitive wireless communication scenarios, such as military, government, and industrial applications. Nonetheless, the implementation of QKD requires the investment of specialized hardware and precise optical infrastructure. PQC offers a more ready-to-use and cost-effective solution for everyday communication that remains resistant to quantum attacks.

It is necessary to develop a hybrid security system that combines the advantages of QKD and PQC to overcome the limitations of each approach. QKD can be used to distribute keys at the backbone level or between data centers, while PQC is used to protect communications at the end-user level. Governments, strategic industries, and the research community are also advised to start developing QKD supporting infrastructure, especially in the context of light-based communications (such as LiFi), which is suitable for use in high-security indoor environments. In addition, further efforts are needed in research and standardization so that

the application of QKD can be more widespread and interoperable in modern communication systems, including 5G, 6G, and IoT ecosystems. With this step, the transition to a communications security system that is resistant to quantum computer attacks can be realized gradually and sustainably.

REFERENCE

[1] Ahilan, A., & Jeyam, A. (2023). Breaking barriers in conventional cryptography by integrating with quantum key distribution. *Wireless Personal Communications, 129*, 549–567. https://doi.org/10.1007/s11277-022-10110-8

[2] Alghamdi, M. I. (2025). A review on quantum key distribution for wireless networks: Current status and future prospects. *Communications on Applied Nonlinear Analysis, 32*(2s). https://doi.org/10.52783/cana.v32.2516

[3] Alshaer, N., Moawad, A., & Ismail, T. (2021). Reliability and security analysis of an entanglement-based QKD protocol in a dynamic ground-to-UAV FSO communications system. *IEEE Access*, 1–1. https://doi.org/10.1109/ACCESS.2021.3137357

[4] Aquina, N., Cimoli, B., Das, S., Hövelmanns, K., Weber, F. J., Okonkwo, C., ... & Verschoor, S. (2025). A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography. *Cryptology ePrint Archive*.

[5] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

[6] Basset, F. B., Valeri, M., Roccia, E., Poderini, D., Neuwirth, J., Spagnolo, N., ... & Trotta, R. (2021). Quantum key distribution with entangled photons generated on demand by a quantum dot. *Science Advances, 7*(12). https://doi.org/10.1126/sciadv.abe6379

[7] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science, 560*, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

[8] Biswas, S., Goswami, R. S., Reddy, K. H. K., Mohanty, S. N., & Ahmed, M. A. (2024). Advancing quantum communication security: Metamaterial-based quantum key distribution with enhanced protocols. *IET Quantum Communication, 5*(4), 399–416. https://doi.org/10.1049/qtc2.12116

[9] Carrasco-Casado, A., Fernández, V., & Denisenko, N. (2016). Free-space quantum key distribution. In M. Uysal, C. Capsoni, Z. Ghassemlooy, A. Boucouvalas, & E. Udvary (Eds.), *Optical wireless communications* (pp. 499–523). Springer. https://doi.org/10.1007/978-3-319-30201-0_27

[10] Chunduru, A., Lenka, S., Neelima, N., & Easwaramoorthy, S. (2024). A secure method of communication through BB84 protocol in quantum key distribution. *Scalable Computing: Practice and Experience, 25*, 21–33. https://doi.org/10.12694/scpe.v25i1.2152

[11] Haiyu Yang, G. L., Zhang, J., Liu, H., & Hu, A. (2021). Fast and secure key generation with channel obfuscation in slowly varying environments. https://doi.org/10.48550/arXiv.2112.02273

[12] Huang, P., Huang, J., Zhang, Z., & Zeng, G. (2018). Quantum key distribution using basis encoding of Gaussian-modulated coherent states. *Physical Review A, 97*(4). https://doi.org/10.1103/PhysRevA.97.042311

[13] Jiao, L., Wang, N., Wang, P., Fanid, A. A., Tang, J., & Zeng, K. (2019). Physical layer key generation in 5G wireless networks. *Electrical Engineering and Systems Science*. https://doi.org/10.48550/arXiv.1908.10362

[14] Kundu, N. K., McKay, M. R., & Mallik, R. K. (2024). Wireless quantum key distribution at terahertz frequencies: Opportunities and challenges. *IET Quantum Communication, 5*(4), 450–461. https://doi.org/10.1049/qtc2.12085

[15] Lim, C. C., Xu, F., Pan, J. W., & Ekert, A. (2021). Security analysis of quantum key distribution with small block length and its application to quantum space communications. *Physical Review Letters, 126*(10). https://doi.org/10.1103/PhysRevLett.126.100501

[16] Maiwada, U. D., Danyaro, K. U., Sarlan, A., Liew, M. S., Taiwo, A., & Audi, U. I. (2024). Energy efficiency in 5G systems: A systematic literature review. *International Journal of Knowledge-Based and Intelligent Engineering Systems, 28*(1), 93–132. https://doi.org/10.3233/KES-230061

[17] Matsuura, T., Maeda, K., Sasaki, T., & Koashi, M. (2021). Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nature Communications, 12*, 1–11. https://doi.org/10.1038/s41467-020-19916-1

[18] Mavroeidis, V., Vishi, K., Zych, M., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications, 9*(3). https://doi.org/10.14569/IJACSA.2018.090354

[19] Pereira, M., Lorenzo, G. C., Navarrete, A., Mizutani, A., Kato, G., Curty, M., & Tamaki, K. (2023). Modified BB84 quantum key distribution protocol robust to source imperfections. *Physical Review Research, 5*. https://doi.org/10.1103/PhysRevResearch.5.023065

[20] Pirandola, S. (2021). Composable security for continuous-variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Physical Review Research, 3*(4). https://doi.org/10.1103/PhysRevResearch.3.043014

[21] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics, 12*(4), 1012–1236.

[22] Primaatmaja, I. W., Goh, K. T., Tan, E. Y. Z., Khoo, J. T. F., Ghorai, S., & Lim, C. C. W. (2023). Security of device-independent quantum key distribution protocols: A review. *Quantum, 7*, 932. https://doi.org/10.22331/q-2023-03-02-932

[23] Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. *Frontiers in Physics, 12*. https://doi.org/10.3389/fphy.2024.1456491

[24] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

[25] Stanley, M., Gui, Y., Unnikrishnan, D., Hall, S. R. G., & Fatadin, I. (2022). Recent progress in quantum key distribution network deployments and standards. *Journal of Physics: Conference Series, 2416*(1). https://doi.org/10.1088/1742-6596/2416/1/012001

[26] Su, H. Y. (2020). Simple analysis of security of the BB84 quantum key distribution protocol. *Quantum Information Processing, 19*, 169. https://doi.org/10.1007/s11128-020-02663-z

[27] Sun, S., & Huang, A. (2022). A review of security evaluation of practical quantum key distribution system. *Entropy, 24*(2), 260. https://doi.org/10.3390/e24020260

[28] Tan, X. (2013). *Introduction to quantum cryptography*. In *Theory and Practice of Cryptography and Network Security Protocols and Technologies*.

[29] Wang, W., & Lütkenhaus, N. (2022). Numerical security proof for the decoy-state BB84 protocol and measurement-device-independent quantum key distribution resistant against large basis misalignment. *Physical Review Research, 4*. https://doi.org/10.1103/PhysRevResearch.4.043097

[30] Wen, X., Li, Q., Mao, H., Wen, X., & Chen, N. (2021). Rotation-based slice error correction protocol for continuous-variable quantum key distribution and its implementation with polar codes. https://doi.org/10.48550/arXiv.2106.06206

[31] Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics, 92*(2), 025002. https://doi.org/10.1103/RevModPhys.92.025002