

International Journal of Data Engineering and Intelligent Computing

Vol. 4, No. 1, 2021

Doi: [10.67228/30715717/IJDEIC-2021PI2L4T](https://doi.org/10.67228/30715717/IJDEIC-2021PI2L4T)

PP. 01-13

Original Article

Quantum Communication and Its Impact on Future Data Transmission Systems

Zara Ahmed

Business Development Manager, Engro Corporation, Pakistan.

Received: 01-04-2021

Revised: 01-14-2021

Accepted: 01-28-2021

Published: 02-09-2021

ABSTRACT

Quantum communication is an emerging field that promises to revolutionize data transmission by leveraging the principles of quantum mechanics. This paper explores the fundamental concepts, underlying principles, and potential impact of quantum communication on future data transmission systems. The study delves into quantum key distribution (QKD), quantum teleportation, and quantum networks, highlighting their advantages over classical communication systems. A comparative analysis of classical cryptographic methods and quantum-enhanced security mechanisms is provided. Furthermore, the paper discusses the challenges associated with implementing quantum communication, such as decoherence, quantum error correction, and scalability. The methodology section outlines experimental setups, simulations, and practical implementations of quantum communication networks. The results emphasize the benefits of quantum encryption and the potential of quantum internet. The discussion explores real-world applications in banking, defense, and cloud computing. Finally, the paper concludes with future perspectives, emphasizing the necessity for ongoing research and technological advancements to achieve a fully functional quantum communication infrastructure.

KEYWORDS

Quantum communication, Quantum Key Distribution, Quantum Internet, Quantum Cryptography, Quantum Networks, Data Transmission, Secure Communication.

1. INTRODUCTION

1.1. Background of Data Transmission Systems

Data transmission has undergone significant transformations over the past centuries, evolving from rudimentary signal-based communication systems to highly advanced digital and wireless networks. The earliest known systems, such as the telegraph and Morse code, relied on basic electrical signals to transfer information over long distances. The introduction of telephone networks in the late 19th century enhanced communication capabilities, enabling real-time voice transmission. As technology progressed, the emergence of radio waves and satellite communication in the 20th century further expanded the reach and efficiency of data transmission.

The advent of the internet and fiber-optic technology marked a revolutionary shift in data transmission. Fiber-optic cables, which use light pulses to transmit information, provided unparalleled speed and bandwidth compared to traditional copper wires. Wireless communication technologies, including Wi-Fi, 4G, and 5G, have further improved mobility and accessibility, making data transmission faster and more reliable.

Despite these advancements, classical communication systems rely on electromagnetic waves and binary encoding methods, making them vulnerable to security threats such as hacking, eavesdropping, and data breaches. Encryption techniques like RSA and AES have been employed to secure data; however, the increasing computational power of adversaries, including the potential rise of quantum computers, poses a serious threat to classical encryption. This necessitates the exploration of more secure alternatives, such as quantum communication, which leverages the fundamental principles of quantum mechanics to achieve secure and efficient data transmission.

1.2. Emergence of Quantum Communication

Quantum communication represents a transformative approach to data transmission that surpasses the limitations of classical systems. Rooted in quantum mechanics, it utilizes the principles of superposition, entanglement, and Heisenberg's uncertainty principle to ensure secure information exchange. The idea of quantum communication emerged in the late 20th century as scientists sought to develop foolproof cryptographic systems.

Superposition, a fundamental concept in quantum mechanics, allows quantum bits (qubits) to exist in multiple states simultaneously. Unlike classical bits, which are either 0 or 1, qubits can represent both states at once, enabling faster and more complex computations. Entanglement, another key principle, refers to the phenomenon where two or more particles become interconnected, such that the state of one instantly influences the state of the other, regardless of distance. This property is exploited in quantum networks to enable ultra-secure data exchange.

One of the most significant applications of quantum communication is Quantum Key Distribution (QKD), particularly the BB84 protocol developed by Bennett and Brassard in 1984. QKD enables two parties to securely exchange cryptographic keys, detecting any eavesdropping attempts by exploiting the no-cloning theorem, which prohibits the copying of an unknown quantum state.

Unlike classical cryptographic systems, which rely on computational complexity, QKD derives its security from the fundamental laws of physics.

As quantum technologies continue to advance, research is expanding toward building quantum networks and the quantum internet, which will enable secure global communication. Governments and private sectors worldwide are investing in quantum research to develop commercial quantum communication infrastructures, paving the way for a new era of ultra-secure data transmission.

1.3. Importance of Secure Communication

In today's digital age, secure communication is a fundamental necessity across various sectors, including finance, healthcare, defense, and corporate enterprises. With the exponential increase in data exchange through online transactions, cloud computing, and IoT devices, ensuring the confidentiality, integrity, and authenticity of transmitted data has become a priority.

Traditional encryption methods, such as RSA and AES, have served as standard security measures for digital communication. These encryption techniques rely on mathematical complexity to prevent unauthorized decryption. However, with the rapid advancement of computing power, particularly the anticipated development of quantum computers, classical encryption methods face a significant threat. Quantum computers have the potential to break current encryption algorithms through Shor's algorithm, which can efficiently factor large prime numbers, undermining the security of RSA-based cryptographic systems.

Quantum communication addresses this vulnerability by offering an inherently secure method of data transmission. Quantum cryptographic protocols, such as QKD, leverage the principles of quantum mechanics to create encryption keys that are immune to interception. Any attempt to eavesdrop on a quantum-encrypted transmission disturbs the quantum state of the system, immediately alerting the communicating parties.

Beyond cryptography, secure communication is crucial in national security and defense applications. Governments are investing in quantum communication technologies to safeguard classified information, ensuring that sensitive military and diplomatic data remains protected from cyber threats. Similarly, the financial sector can benefit from quantum encryption to secure banking transactions and prevent cyber fraud. The increasing reliance on digital infrastructure underscores the urgency for more secure communication systems. Quantum communication not only provides a robust defense against cyber threats but also sets the foundation for future-proof data security in an era of rapid technological advancements.

1.4. Objectives of the Study

The primary objective of this study is to analyze the transformative potential of quantum communication in revolutionizing data transmission systems. The research aims to bridge the gap

between theoretical quantum principles and their practical implementation in modern communication networks. Specifically, this study seeks to:

- Explore the fundamental principles of quantum communication: A detailed examination of quantum mechanics concepts such as superposition, entanglement, and quantum cryptographic protocols will provide a comprehensive understanding of how quantum communication operates.
- Analyze the impact of quantum technologies on data transmission systems: By comparing quantum communication with classical methods, the study evaluates how quantum advancements enhance security, efficiency, and scalability.
- Identify challenges and potential solutions in implementing quantum communication: Practical barriers, including decoherence, quantum error correction, and technological limitations, will be examined alongside emerging solutions to address these challenges.
- Provide insights into the future development of quantum networks: The study will explore the ongoing progress in quantum internet research, government initiatives, and potential commercial applications, outlining the roadmap for a fully operational quantum communication infrastructure.

Through an in-depth analysis, this research aims to contribute valuable insights into the evolution of quantum communication, highlighting its significance in shaping the future of secure and efficient data transmission.

2. LITERATURE SURVEY

2.1. Quantum Communication Fundamentals

Quantum communication is built on the principles of quantum mechanics, which govern the behavior of particles at microscopic scales. Unlike classical communication systems that rely on electronic signals and binary encoding, quantum communication exploits unique quantum properties such as superposition, entanglement, and wavefunction collapse to enhance security and efficiency.

The foundational research in quantum communication can be traced back to the groundbreaking work of Bennett and Brassard (1984), who introduced the BB84 protocol. This protocol was the first practical implementation of Quantum Key Distribution (QKD), a method that ensures secure key exchange by detecting eavesdropping attempts. The security of QKD is rooted in the no-cloning theorem, which states that it is impossible to create an exact copy of an unknown quantum state. This fundamental principle makes quantum communication inherently more secure than classical encryption methods.

Further developments in quantum communication have explored quantum teleportation, a process that allows quantum states to be transmitted between distant locations using entangled particles. Experiments conducted by researchers such as Zeilinger et al. have demonstrated the feasibility of quantum teleportation in laboratory settings, paving the way for the development of quantum networks.

Quantum communication has also found applications in satellite-based quantum encryption. China's Micius satellite experiment successfully demonstrated intercontinental QKD, marking a significant milestone in the field. These advancements indicate that quantum communication has the potential to reshape secure communication infrastructures worldwide.

2.2. Quantum Key Distribution (Qkd) Studies

Quantum Key Distribution (QKD) is one of the most well-studied applications of quantum communication, as it provides a method for two parties to securely exchange cryptographic keys. Traditional encryption relies on computational complexity to protect data, making it vulnerable to attacks by powerful quantum computers. In contrast, QKD ensures security through the fundamental principles of quantum mechanics.

The BB84 protocol, developed by Bennett and Brassard, remains the most widely implemented QKD protocol. It uses the polarization of photons to encode information and enables the detection of eavesdropping by measuring the disturbance in the quantum states. Any attempt to intercept the transmission results in detectable anomalies, alerting the communicating parties to potential security breaches.

Another key development in QKD was the E91 protocol, introduced by Ekert in 1991. This protocol is based on quantum entanglement, where two entangled particles share a correlated state regardless of distance. The security of the E91 protocol is guaranteed by Bell's theorem, which confirms the non-local correlations of entangled particles. Experimental implementations of E91 QKD have demonstrated its robustness against various forms of cyber threats.

Recent advancements in QKD have focused on improving key transmission distances and efficiency. The deployment of fiber-optic QKD networks in countries like China, Japan, and the United States has showcased the potential of QKD in real-world communication infrastructures. Additionally, research is ongoing to develop satellite-based QKD systems, which aim to extend secure communication capabilities on a global scale.

2.3. Quantum Networks and Quantum Internet

Quantum networks extend the principles of quantum communication beyond two-party interactions to create interconnected systems capable of transmitting quantum information over long distances. Unlike classical networks that rely on electronic signals, quantum networks use entangled particles to enable ultra-secure communication.

The concept of a quantum internet, proposed by researchers such as Kimble (2008) and Wehner et al. (2018), envisions a global-scale network where quantum information can be transmitted across different nodes securely. The key components of quantum networks include quantum repeaters, quantum routers, and quantum memory, all of which are necessary to maintain the integrity of transmitted quantum states over long distances.

Quantum repeaters play a crucial role in mitigating signal degradation caused by quantum decoherence. By leveraging entanglement swapping and quantum error correction techniques, quantum repeaters enable entangled states to be extended across large distances without loss of information. Experimental progress has been made in demonstrating small-scale quantum networks, such as the quantum backbone networks in China and Europe.

One of the biggest challenges in realizing a functional quantum internet is the need for high-fidelity quantum memory. Unlike classical memory storage, quantum memory must preserve the coherence of quantum states for extended periods. Research efforts are currently focused on developing efficient quantum memory systems using atomic ensembles and solid-state materials.

Once fully developed, quantum networks and the quantum internet will revolutionize fields such as secure communication, distributed quantum computing, and advanced cryptographic protocols. They hold the potential to create an ultra-secure digital ecosystem immune to cyber threats posed by future quantum computers.

2.4. Challenges in Quantum Communication

Despite its promising advantages, the practical implementation of quantum communication faces several significant challenges. One of the primary hurdles is quantum decoherence, a phenomenon where quantum states lose their coherence due to interactions with the environment. Decoherence severely limits the transmission distance of quantum signals, making long-range quantum communication difficult without additional technological innovations.

Another critical challenge is quantum error correction. Unlike classical error correction techniques that use redundant bits to detect and correct errors, quantum error correction requires specialized codes such as the Shor code and surface codes to protect quantum information from noise and interference. These techniques are still under development and require complex hardware for implementation.

Scalability is another major concern. Current quantum communication systems operate on small scales, but expanding them to large-scale networks requires overcoming technological and infrastructural limitations. The development of quantum repeaters and efficient quantum memory systems is essential for achieving large-scale quantum communication networks.

Furthermore, hardware limitations pose a significant barrier to widespread adoption. Quantum communication relies on delicate quantum devices such as single-photon sources, quantum detectors, and superconducting circuits, all of which require extreme conditions (such as ultra-low temperatures) for optimal operation. The cost and complexity of maintaining these systems hinder their large-scale deployment.

Addressing these challenges requires continued research and investment in quantum technologies. Governments and private organizations are funding initiatives to develop practical

quantum communication infrastructures, and collaborative research efforts are essential for overcoming the barriers to large-scale implementation.

3. METHODOLOGY

3.1. Experimental Setup for Quantum Communication

The experimental setup for quantum communication involves the deployment of Quantum Key Distribution (QKD) protocols using photonic systems. These experiments require specialized optical components such as laser sources, beam splitters, polarizers, and single-photon detectors. The BB84 and E91 protocols are commonly tested in laboratory settings to establish secure quantum channels between communicating parties.

In a typical experimental setup, a laser source generates single photons, which are encoded with quantum information through polarization or phase modulation techniques. The photons travel through a quantum channel, such as optical fiber or free space, to reach the receiving station. Beam splitters and polarizers at the receiving end analyze the quantum states, ensuring that any eavesdropping attempts result in detectable disturbances due to the fundamental principles of quantum mechanics.

Various research institutions have developed advanced quantum communication testbeds to evaluate the feasibility of real-world implementation. These setups include fiber-optic networks, free-space optical links, and even satellite-based quantum communication. The development of highly efficient single-photon detectors has further improved the accuracy and reliability of these experiments.

To ensure accurate experimental results, researchers also employ quantum state tomography, which reconstructs the quantum state of transmitted photons to verify the integrity of the communication. Additionally, error correction techniques, such as quantum error correction codes, are implemented to mitigate the effects of noise and decoherence in quantum channels.

3.2. Simulations Of Quantum Networks

Simulations play a crucial role in understanding the behavior of quantum networks and optimizing their performance before real-world implementation. Quantum network simulators model various aspects of quantum communication, including entanglement distribution, quantum routing algorithms, and error mitigation techniques.

Quantum simulators, such as QuNetSim and SimulaQron, provide a virtual environment to test different network configurations and protocols. These simulations help researchers analyze how entanglement can be distributed efficiently across multiple nodes, ensuring reliable quantum communication over large distances. By modeling the behavior of quantum repeaters and quantum memory systems, simulations contribute to designing scalable quantum networks.

One of the key objectives of quantum network simulations is to optimize the trade-off between transmission fidelity and communication speed. Since quantum signals are highly susceptible to noise and decoherence, researchers use machine learning and optimization algorithms to enhance the performance of quantum networks. By testing various network topologies and quantum error correction methods, simulations provide insights into the most effective approaches for large-scale quantum communication deployment.

Additionally, simulations are used to study the impact of external factors such as atmospheric conditions and fiber-optic losses on quantum communication. By incorporating realistic environmental parameters, researchers can develop robust quantum communication strategies that can withstand real-world challenges.

3.3. Practical Implementations and Testing

Real-world implementations of quantum communication have progressed significantly in recent years, with various pilot projects demonstrating the feasibility of large-scale quantum networks. One of the most notable practical implementations is China's Micius satellite experiment, which successfully established a quantum-secure communication link between distant locations.

The Micius experiment demonstrated intercontinental QKD by transmitting entangled photons between ground stations located thousands of kilometers apart. This breakthrough proved that quantum communication could be extended beyond terrestrial fiber-optic networks, opening new possibilities for global secure communication. Similar initiatives are being undertaken by the European Union, the United States, and Japan, with ongoing efforts to develop satellite-based quantum networks.

In addition to satellite-based projects, several research institutions are implementing terrestrial quantum communication systems. The development of quantum backbone networks, such as China's 2000-kilometer fiber-optic QKD network and Europe's SECOQC project, highlights the growing interest in integrating quantum communication into existing infrastructure.

Furthermore, companies like IBM, Google, and Toshiba are actively investing in quantum communication technologies to enhance cybersecurity and develop commercial quantum networking solutions. Ongoing research in quantum repeaters and quantum teleportation techniques aims to address the current limitations of quantum communication and expand its applicability in real-world scenarios.

3.4. Security Analysis and Performance Metrics

To evaluate the effectiveness of quantum communication systems, security analysis and performance metrics are essential. These assessments ensure that quantum protocols provide a higher level of security compared to classical cryptographic methods.

One of the key performance metrics in quantum communication is the key generation rate, which measures the speed at which cryptographic keys can be securely exchanged using QKD. Higher key generation rates improve the efficiency of quantum-secure networks, making them more viable for real-time applications.

Another important parameter is the bit error rate (BER), which quantifies the errors introduced during quantum transmission. Lower BER values indicate higher reliability and integrity of transmitted quantum states. Error correction techniques, such as quantum error correction codes and entanglement purification, are employed to minimize errors and improve overall communication performance.

Security analysis of quantum communication involves testing the resistance of QKD protocols against various attack strategies. One of the most well-known attacks is the photon number splitting (PNS) attack, which targets weak laser pulses used in QKD. Countermeasures such as decoy state protocols have been developed to mitigate the risks associated with PNS attacks.

Additionally, security proofs based on quantum information theory confirm the unconditional security of QKD against computational attacks. Unlike classical encryption, which relies on the difficulty of mathematical problems, quantum encryption derives its security from the laws of physics. This makes it immune to brute-force attacks and quantum computing threats.

By continuously refining security measures and optimizing performance metrics, researchers aim to establish quantum communication as the future standard for secure data transmission. Future advancements in quantum cryptography, network scalability, and device miniaturization will further enhance the feasibility of widespread quantum communication deployment.

4. RESULTS AND DISCUSSION

4.1. Enhanced Security of Quantum Communication

One of the most significant findings in quantum communication research is its superior security compared to classical cryptographic methods. Unlike conventional encryption techniques, which rely on computational complexity, quantum encryption derives its security from the fundamental laws of physics. Quantum Key Distribution (QKD) protocols such as BB84 and E91 ensure secure key exchange by leveraging quantum mechanics, making them resistant to brute-force attacks and decryption by quantum computers.

Experimental results demonstrate that QKD is inherently immune to eavesdropping attempts. Any interception of quantum states results in measurable disturbances due to the no-cloning theorem and Heisenberg's uncertainty principle. This unique property ensures that any unauthorized access can be detected immediately, reinforcing the security of communication networks.

In addition, research has shown that integrating QKD into existing fiber-optic networks significantly enhances their security by enabling end-to-end encryption with provable security

guarantees. Various pilot projects have demonstrated the successful deployment of quantum-secure communication channels in banking, government institutions, and defense applications.

While quantum encryption offers unparalleled security advantages, there are still challenges in practical implementation, such as the need for highly efficient single-photon sources and low-noise detection systems. Nevertheless, ongoing advancements in quantum hardware and algorithms continue to improve the feasibility of large-scale quantum-secure communication networks.

4.2. Performance Comparison with Classical Communication

A key aspect of evaluating quantum communication is comparing its performance against classical communication methods. Experimental studies indicate that quantum networks generally exhibit lower latency in cryptographic key distribution and are highly resistant to hacking attempts. However, some challenges remain, such as transmission distance limitations and infrastructure costs.

One of the main performance metrics used in comparison studies is the key generation rate in QKD systems. While early QKD implementations suffered from low key generation rates, recent advances in high-speed single-photon detectors and decoy-state protocols have significantly improved performance, making QKD viable for practical applications.

Another advantage of quantum communication is its resilience to cyber threats. Unlike traditional encryption, which can be broken with sufficient computational power, quantum encryption remains secure regardless of technological advancements. This makes it particularly valuable for applications requiring long-term data protection, such as military communications and financial transactions.

However, a major limitation is the transmission distance in fiber-optic quantum networks. Photonic losses in optical fibers lead to signal degradation, restricting the range of QKD to approximately 100-200 kilometers. To address this issue, researchers are developing quantum repeaters that extend entanglement distribution over long distances, potentially enabling global-scale quantum communication.

Despite these challenges, the increasing integration of quantum technology into commercial telecommunication networks suggests that quantum communication will soon surpass classical systems in security and efficiency.

4.3. Challenges in Large-Scale Implementation

Despite its advantages, large-scale implementation of quantum communication systems presents several technical and logistical challenges. One of the most pressing issues is scalability. Current quantum networks operate on relatively small scales, primarily due to technological constraints such as quantum decoherence and photon loss.

Quantum decoherence refers to the loss of quantum state integrity over time, which affects the reliability of quantum communication. This issue is particularly problematic for long-distance communication, where signal degradation reduces the efficiency of QKD protocols. To mitigate decoherence effects, researchers are working on developing fault-tolerant quantum communication systems that incorporate quantum error correction techniques.

Another significant challenge is the development of quantum repeaters. Unlike classical repeaters, which amplify signals, quantum repeaters use entanglement swapping to extend the range of quantum communication. While experimental progress has been made in entanglement-based quantum networks, practical quantum repeaters capable of supporting global-scale communication are still in the early stages of development.

Additionally, there are infrastructure and cost constraints. Implementing quantum-secure communication requires specialized equipment, such as single-photon sources and superconducting detectors, which are expensive and require precise environmental conditions. The integration of quantum networks with existing telecommunication infrastructure also poses compatibility challenges.

Despite these obstacles, governments and private companies are investing heavily in quantum communication research, with several pilot projects already demonstrating the feasibility of large-scale quantum networks. Future advancements in quantum hardware and network optimization are expected to address scalability challenges and enable widespread adoption of quantum communication.

4.4. Future Applications and Industrial Adoption

Quantum communication has the potential to revolutionize multiple industries by providing unprecedented levels of security and efficiency in data transmission. Several sectors, including banking, cybersecurity, healthcare, and national defense, are expected to benefit significantly from quantum-secure communication infrastructures. One of the most promising applications is financial transactions and secure banking. Financial institutions handle vast amounts of sensitive data daily, making them prime targets for cyberattacks. The adoption of QKD in banking networks can ensure secure data transmission, preventing financial fraud and identity theft.

The cybersecurity industry is also expected to undergo a transformation with the integration of quantum cryptography. Traditional encryption methods face increasing threats from quantum computing advancements, but QKD provides a long-term solution for securing communication networks. Governments worldwide are investing in quantum-secure encryption to protect critical infrastructure, including power grids and communication networks. Another major application is in national defense and intelligence communications. Military organizations require highly secure channels to transmit classified information. Quantum communication can ensure that defense networks remain impervious to cyber espionage and hacking attempts. Several countries are actively developing quantum-secure military communication systems.

Additionally, healthcare and medical data security can benefit from quantum communication. Patient records and medical research data require high levels of security to prevent unauthorized access and data breaches. Quantum encryption can provide a reliable solution for protecting sensitive medical information. With increasing investments from governments and technology companies, quantum communication is poised to become an integral part of future secure communication infrastructures. As research progresses and technological challenges are addressed, quantum communication is expected to be widely adopted across industries, revolutionizing data security on a global scale.

5. CONCLUSION

Quantum communication offers a transformative approach to secure data transmission, providing unparalleled advantages over classical cryptographic methods through innovations such as Quantum Key Distribution (QKD), quantum networks, and quantum cryptography. The findings of this study underscore the potential of quantum communication to enhance security and efficiency in future communication systems by mitigating the vulnerabilities associated with classical encryption techniques. The integration of quantum technologies into existing telecommunication frameworks will significantly improve data security, ensuring robust protection against cyber threats and quantum-computing attacks. However, the transition from classical to quantum communication necessitates substantial research, infrastructure investment, and technological advancements to address critical challenges, including quantum repeater development, scalability, and quantum error correction. Future research should prioritize optimizing quantum repeater technologies to extend communication distances, developing hybrid quantum-classical networks to facilitate seamless integration, and improving quantum error correction methods to enhance reliability. Despite existing challenges, continuous advancements in quantum hardware, network protocols, and computational models will drive the commercialization and widespread adoption of quantum communication, positioning it as the future of secure data transmission across industries such as finance, cybersecurity, healthcare, and defense. As governments and private enterprises increasingly invest in quantum technologies, the realization of a global-scale quantum internet is becoming more tangible, promising unprecedented levels of security and efficiency in data exchange. The evolution of quantum communication marks a pivotal shift in the landscape of information security, laying the groundwork for next-generation secure communication infrastructures.

REFERENCE

- [1] Bennett, C. H., & Brassard, G., "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.
- [2] Ekert, A. K., "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.
- [3] Shor, P. W., & Preskill, J., "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, vol. 85, no. 2, pp. 441–444, 2000.
- [4] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H., "Quantum Cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.
- [5] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M., "The Security of Practical Quantum Key Distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

- [6] Pirandola, S., Braunstein, S. L., & Lloyd, S., "Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography," *Physical Review Letters*, vol. 101, no. 20, 2008.
- [7] Van Meter, R., "Quantum Networking," Wiley-ISTE, 2014.
- [8] Lo, H.-K., Curty, M., & Tamaki, K., "Secure Quantum Key Distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014.
- [9] Kimble, H. J., "The Quantum Internet," *Nature*, vol. 453, pp. 1023–1030, 2008.
- [10] Elliott, C., "Building the Quantum Network," *New Journal of Physics*, vol. 4, 2002.
- [11] Sasaki, M., et al., "Field Test of Quantum Key Distribution in the Tokyo QKD Network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.
- [12] Ursin, R., et al., "Entanglement-Based Quantum Communication over 144 km," *Nature Physics*, vol. 3, pp. 481–486, 2007.
- [13] Duan, L.-M., Lukin, M. D., Cirac, J. I., & Zoller, P., "Long-Distance Quantum Communication with Atomic Ensembles and Linear Optics," *Nature*, vol. 414, pp. 413–418, 2001.
- [14] Peev, M., et al., "The SECOQC Quantum Key Distribution Network in Vienna," *New Journal of Physics*, vol. 11, 2009.
- [15] Shah, S., Shah, M., Shah, A., & Shah, R., "Quantum Key Distribution," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 10, 2015.