SSRG International Journal of Recent Engineering Science
ISSN: 2349–7157 / https://doi.org/10.14445/23497157/IJRES-V11I3P105

Volume 11 Issue 3, 48-55, May-Jun 2024
© 2024 Seventh Sense Research Group®

Original Article

Quantum Key Distribution Protocol for Secure Fiber Optic Communication

Ezeilo Ifeoma Kelechukwu[1], Asianuba Ifeoma[2]

[1]*Department of Electrical/electronics department, Nnanmdi Azikiwe University Awka, Anambra State, Nigeria.*
[2]*Department of Electrical/electronic, University of Port Harcourt, RiversState, Nigeria.*

[1]*Corresponding Author : Ik.ezeilo@unizik.edu.ng*

Received: 06 April 2024 Revised: 10 May 2024 Accepted: 23 May 2024 Published: 13 June 2024

Abstract - *Currently, secure communication is crucial in the digital era since sensitive information is always in transit and data moves freely. Despite their effectiveness, traditional encryption techniques are not impervious to the changing threat environment*. *Clearly, one surefire method of ensuring security for upcoming fiber communication networks is through quantum key distribution. The Quantum Key Distribution (QKD) cryptographic protocol secures communication channels by utilizing concepts from quantum mechanics. Key distribution security is the goal of the Quantum Key Distribution Protocol for Secure Fiber Communication, quantum key generation, detection of eavesdropping, perfect secrecy, information-theoretic security, security against quantum computers, integration with classical cryptography and compatibility with fiber optic communication. Key Distribution Security's main goal of QKD is to transfer cryptographic keys between two parties in a secure manner. The application and advantages of Quantum Key Distribution (QKD) techniques for improving fiber optic communication security are examined in this paper. QKD exploits principles of quantum physics to establish secure keys between participants, minimizing cyber dangers in fiber optic networks. In order to secure data transfer, the paper examines the theoretical foundation, real-world use, and difficulties associated with QKD techniques. It ends with some thoughts on how QKD can develop secure communication technology in the future*.

Keywords - *Fiber optic communication, Key distribution, Security, Qubits, Quantum.*

1. Introduction

The confidentiality of private information sent over fiber networks is seriously threatened by eavesdropping or the unlawful interception of communications. Although fiber communication is more secure by nature, it is nevertheless vulnerable to eavesdropping, much like traditional copper-based communication routes. Fiber optic transmissions are made up of light pulses, and since they can be intercepted by specialized equipment, there is a risk that private information could be compromised.

The most important factor in preventing eavesdropping efforts is communication security by using encryption protocols like advanced classical encryption algorithms or Quantum Key Distribution (QKD). Quantum physics concepts are used by a cryptography system known as Quantum Key Distribution (QKD) to establish secure communication channels. One may make sure that the intercepted data cannot be decrypted without the right cryptographic keys, even in the event that an unauthorized person manages to obtain access to the fiber channel. The threat of cybercrimes targeting fiber communication networks is growing along with the digital landscape. Cybercriminals use a variety of strategies to take advantage of weaknesses, endangering the readiness and integrity of data that is transferred. Data breaches and unauthorized access are just a few of the numerous cyber threats that have the ability to obstruct communication and jeopardize important data.

The development of quantum communication and quantum mechanics are intimately related. Scientists like Max Planck and Albert Einstein questioned conventional physics in the early 1900s, laying the foundation for quantum mechanics. The idea of quantum communication originated with the proposal of quantum key distribution (QKD) in the 1980s by Charles Bennett, Stephen Wiesner, and other individuals. The field has advanced quickly from the 1990s to the present, including new research directions. (Athanassias S., 2023).

2. Quantum Bits

The fundamental units of quantum information are called qubits. Qubits are different from classical bits in that They are able to coexist in a condition of simultaneous superposition of 0 and 1.

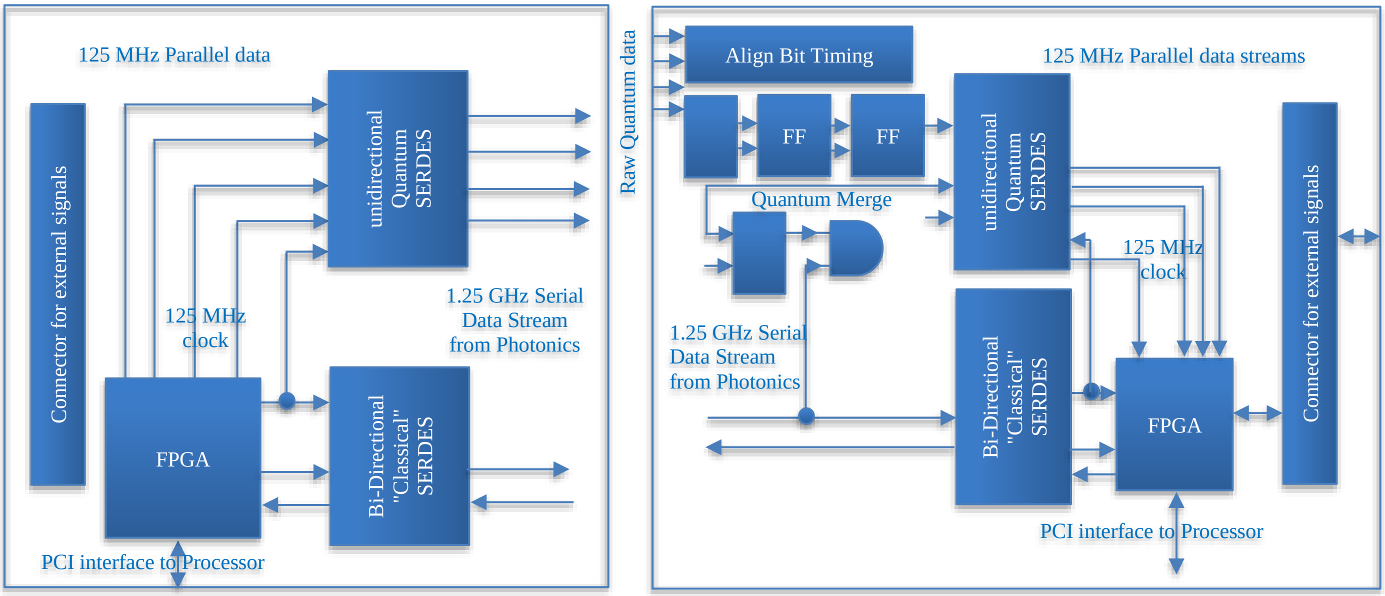
125 MHz Parallel data
Connector for external signals
unidirectional Quantum SERDES
125 MHz clock
1.25 GHz Serial Data Stream from Photonics
FPGA
Bi-Directional "Classical" SERDES
PCI interface to Processor
Raw Quantum data
Align Bit Timing
FF
FF
125 MHz Parallel data streams
Quantum Merge
unidirectional Quantum SERDES
125 MHz clock
1.25 GHz Serial Data Stream from Photonics
Bi-Directional "Classical" SERDES
FPGA
Connector for external signals
PCI interface to Processor

Fig. 1 Functional block diagrams of alice and Bob

2.1. *Distribution of Quantum Key Protocol*

Distribution of Quantum key (QKD) techniques, including Bennett-Brassard (1992) and Ekert (1991), utilize quantum principles to facilitate safe key exchange. In these protocols, Alice and Bob, the sender and recipient, exchange qubits, and the conveyed particles' quantum characteristics ensure the key's security.

2.1.1 Application of Quantum Key Distribution in Communication

Secure Banking: Though theoretically unbreakable, quantum communication offers an alternative to traditional encryption, which can be subject to attacks.

Health care: quantum provides robust security for hospital patients' data, which is very important.

2.1.2. Military Communication

To safeguard sensitive data, governments and defense agencies are investing in quantum communication.

2.1.3. Scientific Research

Quantum communication facilitates secure and efficient data dissemination among research institutions.

2.2. Advantages of Quantum Key Distribution

2.2.1. Quantum Immunity to Shor's Algorithm

A countermeasure to the threats posed by quantum computers is provided by quantum cryptography, specifically by Quantum Key Distribution (QKD).

The intrinsic features of quantum mechanics, such as entanglement and superposition, add an element of uncertainty that makes classical attacks, like Shor's technique, useless.

2.2.2. Unconditional Security

QKD offers unrestricted security, in contrast to traditional key exchange techniques. Due to its intrinsic connection to the laws of quantum physics, the key's security is unaffected by assaults that take advantage of flaws in traditional algorithms.

2.2.3. DDetection of Eavesdropping

Mechanisms in QKD are designed to identify any effort at listening in. Measuring quantum states always perturbs the system, enabling the parties involved in communication to detect the intrusion.

2.2.4. Quantum Immunity

Interestingly, quantum computers—which represent a danger to traditional cryptography techniques, are defenseless against QKD. Since certain pairings of attributes cannot be precisely measured simultaneously, the uncertainty principle protects quantum keys.

2.2.5. Information and Communication Capacity

The enhanced information capacity per quantum system is the first and most obvious benefit provided by qudits as well as the connection with log2d, which yields the quantity of qubits bits required for encoding the exact same quantity of data, provides a quantifiable measure of the greater information capacity. Moreover, higher channel capacities, that is, the quantity of data that can be securely transferred over a communication channel, are produced by high-dimensional entangled states. Einstein et al. anticipated entanglement, which results in quantum non-local correlations that no local theory can produce.

Higher Noise Resistance

High-dimensional quantum states have an additional crucial property for quantum communication in addition to their enhanced information capacity: they are more resilient to noise, whether from outside sources or from eavesdropping attempts. In fact, the foundation not only for general quantum communication protocols but also for the sharing of random keys that are encrypted quantum key distribution is the safety of the quantum conduit, which is enabled by utilizing quantum physical rules With the (QBER)-quantum bit error rate available, or the proportion of an erroneous rate relative to the total rate of reception, below a given cutoff, ensures the security of a settled quantum connection. It is shown that when Using two impartial grounds that are mutually for restitution, that is one-way. (Daniele Cozzolino et.al., 2019).

Qudits' greater resistance to noise sources has been demonstrated in references when Eve, a possible eavesdropper, provided information. Using 2 and MUBs is taken into account when calculating cohesive attacks. It has thus been shown that the resilience of qudits to noise grows with their dimension d, i.e., the threshold values of QBERs, which guarantees safe communication, shoot up. For example, by employing two MUBs, the thresholds for =4 and =8 are 18.93% and 24.70%, respectively. The ultimate secret key rate is likewise affected by this increased noise tolerance. In fact, The private key rate grows with Hilbert space dimensionality at a fixed noise level. The maximum allowable mistakes for producing an effective private key rates as an expression of the range and for different qudit sizes are displayed in Figure 1.2.

The curves are obtained and correspond to an ideal system executing a d-dimensional single-photon BB84 protocol, assuming coherent attacks and employing ideal detectors impacted exclusively by the dark count probability (). A zone where a positive secret key rate may be recovered is found for each dimension. Additionally, as dimensions increase, the attainable transmission distances decrease, suggesting qubit techniques to achieve the largest distance. However, in a real-world setting, the true benefits of extremely dimensional states beyond qubits are highly dependent on the exact execution that changes the necessary operational limitations. Therefore, there may be situations in which high-dimensional states outperform qubits in terms of transmission distance as well.

The figure above shows The highest possible tolerance in terms of distance and various dimensions for a positive secret key rate. The curves were calculated using perfect detectors impacted just by the dark count probability, taking into account a single-photon d-dimensional BB84 protocol.

(=10−8 per detector) and when coordinated attacks occur. We analyse the usual single-mode fiber variable for attenuation, dbkm−1, and presume d detectors measuring d signals concurrently. Every arc represents a location from which an optimistic encryption rate can be retrieved. The greatest achievable distance for transmission is reduced by raising the state's dimension d; actually, the higher d is, the greater the degree to which the states react to the gloomy tracks of the detectors.

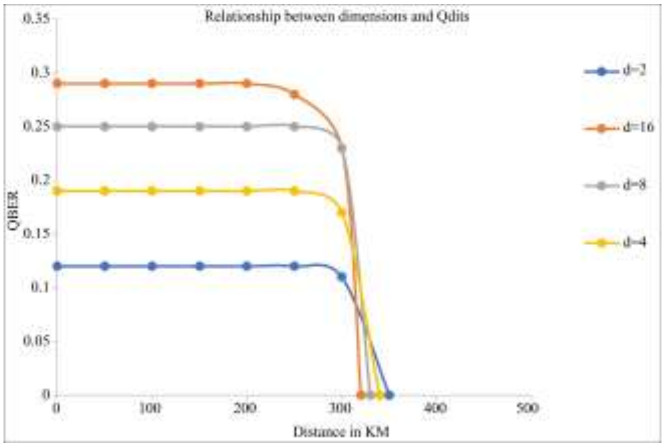

Fig 1.2. Relationship between dimension and qudits

3. Quantum Mechanics Principles Underpinning Quantum Key Distribution

Quantum Key Distribution (QKD), a unique approach to secure communication, leverages the fundamental concepts of quantum physics. Understanding the complexities of QKD requires an exploration of the fundamental quantum ideas that form the basis of this state-of-the-art technology. This in-depth investigation will clarify the concepts of superposition, entanglement, and quantum measurement and show how they work together to prove the safety and effectiveness of QKD.

The basic concepts of quantum key distribution are derived from quantum mechanics, a branch of study that studies how particles behave. The ideas of quantum cryptography were first presented in quantum physics, which contrasts with classical mechanics and includes superposition, entanglement, and uncertainty.

Within QKD, the safe key exchange process is derived from the utilization of the quantum features of particles, commonly photons. Any attempt to eavesdrop on or intercept communication can be detected thanks to the special properties of quantum particles. Quantum states are inherently unstable; thus, measuring them gives the communication parties a way to recognize and neutralize possible threats.

3.1. Quantum Superposition QKD

Quantum bits, or qubits, are used in QKD and are capable of existing in several states at once. This enables simultaneous representation of 0 and 1 in qubit transmission. The act of measuring would disrupt the superposition if an eavesdropper tried to intercept the qubit, revealing the existence of an incursion.

Superposition is a rudimentary proportion principle. A qubit in superposition is represented mathematically as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Where, α and β are intricate numbers, and the odds for determining the qubit's position 0 or 1 are given by $|\alpha| \wedge 2and|\beta| \wedge 2, respectively.$

3.1.1. Entanglement

Famously described by Einstein as "spooky action at a distance," A significant quantum phenomenon known as entanglement occurs when two or more particles become so coupled that their states are intimately related to one another even though they are physically separated. Entanglement, which Einstein famously referred to as "spooky action at a distance," is a deep quantum phenomenon wherein two or more particles combine to form so correlated that their states are directly coupled to each other even if they are physically separated.

Even at great distances, entangled particles—also known as entangled qubits in the quantum context—display an amazing association. Two qubits in an entangled state are commonly depicted as:

$$|\psi\rangle = 1/2(19)A \otimes |1\rangle\beta - |1\rangle A \otimes |0\rangle\beta)$$

In such cases, Alice's and Bob's particles are indicated by the subscripts A and B, respectively. The phrase "entangled state" describes a situation in which the single qubit's measurement instantly ascertains the other qubit condition.

3.2. Quantum Measurement in QKD

In quantum mechanics, measuring is a crucial and frequently mysterious process. Quantum measurement is intrinsically probabilistic, in contrast to conventional systems where measurement produces a predictable result. The last stage of QKD is measuring qubits in order to derive a shared secret key. To guarantee security, the probabilistic aspect of quantum measurement is utilized. The disruption produced by an eavesdropper trying to intercept or measure the qubits exchanged between Alice and Bob would probably cause mistakes in the measured states.

The quantum measurement process can be expressed mathematically as:

$$|\psi\rangle == 1/2(10)A \otimes |1\rangle B - |1\rangle A \otimes |0\rangle B)$$
$$MB(1/2|0\rangle A \otimes |1\rangle B - 1/21/2|1\rangle A \otimes |0\rangle B)$$
$$= |1\rangle BMB(1/2|0\rangle A \otimes |1\rangle B$$
$$- 1/21/2|1\rangle A \otimes |0\rangle B) = |1\rangle B$$

3.3. Basic Steps in Quantum Distribution Protocol

3.3.1. Quantum Key Generation

This step involves generating a quantum key using a Quantum Key Distribution (QKD) protocol, such as BB84 or E91. This key is used for encrypting and decrypting data in a secure manner.

3.3.2. Key Distribution

The quantum key is then distributed between the sender and the receiver using quantum communication channels, typically using photons as quantum carriers.

3.3.3. Key Reconciliation

In this step, the sender and receiver compare parts of their key to detect and correct errors introduced during transmission. This ensures that both parties share the same key.

3.3.4. Privacy Amplification

To further boost the key's security, privacy amplification techniques are applied. This involves processing the key to remove any remaining correlations that an eavesdropper might exploit.

3.3.5. Data Encryption

Once the secure key is established, it is used to encrypt the information that has to be sent back and forth between the sender and the recipient.

3.3.6. Data Transmission

The recipient receives the secure information via a traditional communication route.

3.3.7. Data Decryption

The original message can be retrieved by the recipient by using the shared key to decode the data that was received.

4. Decoherence and Attenuation in Fiber Optic Quantum Communication

The loss of quantum state coherence due to various fiber optic medium characteristics is known as discoherence in fiber optic quantum communication. One important characteristic of quantum systems is coherence, which describes the phase connection between various quantum states. Because of its high receiver sensitivity, coherent detection was the subject of extensive research in the 1980s. Early in the 1990s, research on coherent optical communication came to an end with the creation of WDM systems and the discovery of EDFA due to the complexity and difficulty of implementing new systems. Particularly the intricate implementation of the optical phase-locked loop. It was found that phase and polarization management were the biggest challenges to the actual application of conventional coherent receivers. Thankfully, DSP allows for the realization of phase and polarization control in the field of electricity. Coherent optical communication has garnered significant interest once more in recent times due to the growing demand for transmission capacity. It has emerged as a novel and auspicious method for achieving high-capacity, long-haul optical communication systems (Jian Zhao et al., 2019). Discoherence in fiber optic transmission can happen for a number of reasons:

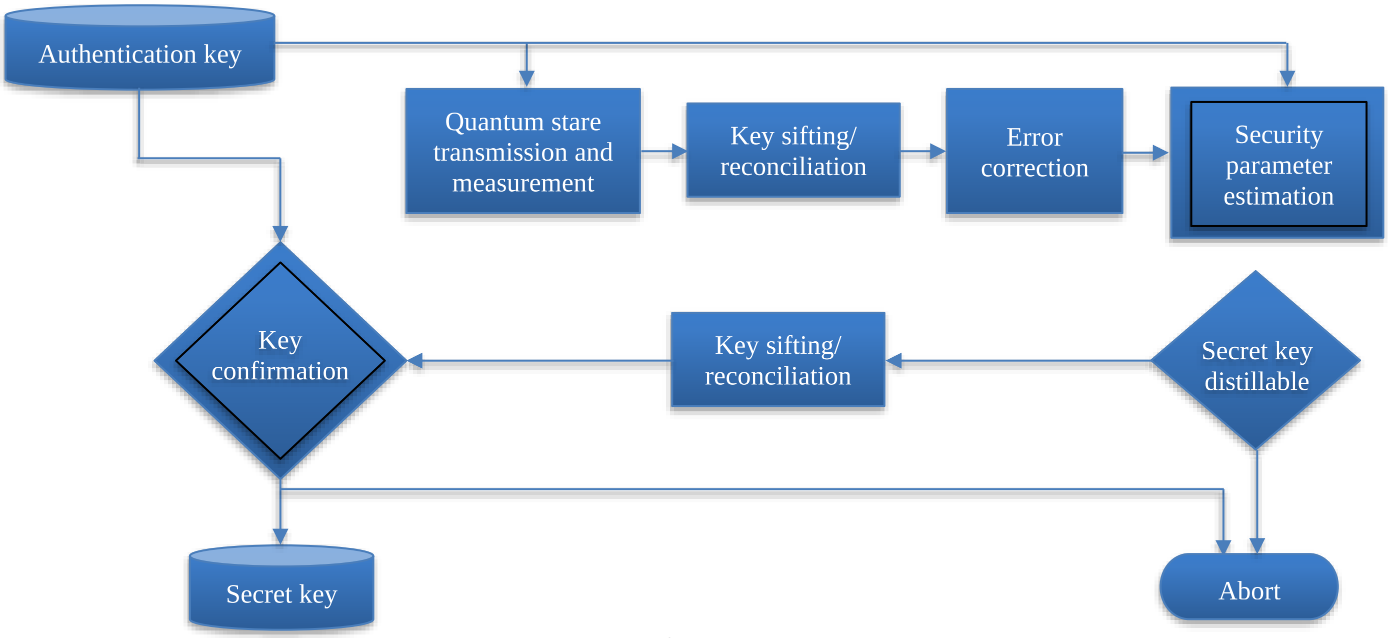
Authentication key
Quantum stare transmission and measurement
Key sifting/ reconciliation
Error correction
Security parameter estimation
Key confirmation
Key sifting/ reconciliation
Secret key distillable
Secret key
Abort

Fig 1.2 Diagram of the basic step in QDK

4.1. Photon Loss

The coherence of the quantum state can be reduced when photons carrying quantum information are lost through scattering, absorption, or leakage in the fiber.

4.2. Phase Noise

Phase noise is introduced into the fiber by external sources like temperature variations, mechanical vibrations, or electromagnetic interference, which can result in the loss of coherence of the quantum state.

4.3. Fiber Birefringence

When light is polarized in two separate directions, it can travel at two different speeds in fiber optic cables. This may result in quantum states that are polarization-sensitive losing their coherence. Fiber dispersion is the result of different light wavelengths moving through the fiber at various rates. This may result in quantum states with frequency-domain encoding losing coherence. A major obstacle in fiber optic quantum communication is discoherence, which can reduce the dependable transmission distance of quantum information. To lessen the impacts of discoherence in fiber optic quantum communication systems, a number of strategies are being explored, including error correction codes and active stabilization of the quantum states, as explained below: Purification and Filtering: Decoherence can be decreased by filtering out undesired environmental noise and using high-purity materials for fiber optics.

4.4. Active Stabilization

Decoherence effects like phase noise or polarization shifts can be countered by actively stabilizing the quantum states through feedback methods.

4.5. Cryogenic Temperatures

Decoherence processes can be slowed down, and thermal noise can be minimized by cooling fiber optic cables to cryogenic temperature.

4.6. Photon-Photon Entanglement

Compared to using traditional light sources, utilizing entangled photon pairs for communication can increase resistance to decoherence.

4.7. Quantum Repeater Protocols

By reducing decoherence across extended distances, the use of quantum repeater protocols can effectively increase the range of quantum communication.

4.8. Optimized Fiber Design

Loss and other decoherence issues can be decreased by creating fiber optic cables with optimal materials and structures.

These techniques can help researchers greatly minimize decoherence in fiber optic quantum communication systems, which will improve the efficiency and dependability of quantum communication across extended distances.

An equation for the overall decoherence in fiber optic quantum communication could be expressed as:

$$reff = \alpha + r + renv$$

5. Attenuation

The major challenges of traditional fiber optic communication are dispersion and attenuation (fiber bend, scattering, absorption); they both result in degradation of signal /loss in signal strength as it travels through the fiber cable. This loss can occur due to various factors such as scattering (propagation mode change), absorption, and imperfections in the fiber optic material. There are two types of absorption that occur in fiber communication: extrinsic and intrinsic absorption. Intrinsic absorption occurs as a result of interaction between the fiber optic cable materials and the light, while extrinsic absorption is as occurs due to impurities molded into the fiber during manufacturing. Scattering is also of two major types: linear (Rayleigh and Mie scattering) and nonlinear scattering (stimulated brillouin scattering and Raman scattering).

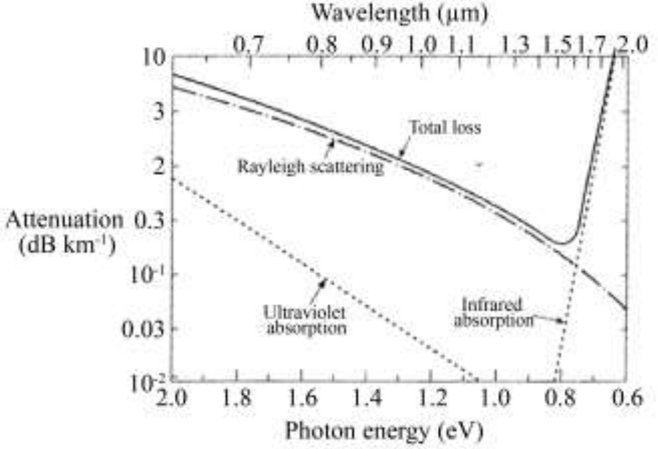

Figure 5.2 The attenuation spectra for the intrinsic loss mechanisms in pure GeO2–SiO2 glass (Ifeoma B. Asianuba, 2024)

The term "attenuation" in fiber optic quantum communication describes the quantum information that is lost during transmission across the fiber optic cable. A number of things, including scattering, absorption, and flaws in the fiber optic material, can cause this loss, which makes it very similar to the traditional losses in fiber optic communication. However, the nature of the signal is different in quantum communication. Photons' polarization or phase, for example, are examples of quantum states that store quantum information. Compared to classical signals, these states are usually more susceptible to noise and loss.

A number of strategies including the use of error correction codes, high-quality fiber optic cables, and quantum repeaters to periodically amplify the signal along the fiber, can be used to reduce attenuation in fiber optic quantum communication. By using these methods, attenuation effects are mitigated, and quantum communication systems operate better overall.

4.1. Present Real-world Application of Quantum Key Distribution in Secure Fiber Optic Communication Secure Communication

Among the most exciting purposes for quantum communication is secure communication. Quantum communication makes it possible to transfer information in an entirely secure way, which is essential for sectors like finance, government, and the military. Given that quantum communication is based on quantum mechanical concepts, any attempt to overhear the conversation will be quickly discovered. An eavesdropper cannot obtain the information being conveyed as a result. Quantum mechanics is one use of this (Hossani. M.etal, 2011).

4.2. Telecommunication

Quantum communication has applications in traditional telecommunications as well. One potential application of quantum communication is enhancing the security of well-established communication networks, such as the internet. By encrypting communications via quantum communication, a secure communication channel that is resistant to hacking and other forms of cyberattacks can be built.

4.3. Quantum Computing

Another crucial element of quantum computing is quantum communication. Quantum bits, or qubits, are extremely sensitive to environmental disturbance and are used in quantum computing. This implies that a safe and dependable method of information transfer between qubits is necessary for quantum computers. This is possible with quantum communication, which makes it a crucial part of quantum computing.

4.4. Quantum Sensing

Sensing is another area where quantum communication shows promise. Due to their extreme sensitivity, quantum sensors are able to pick up on even the smallest environmental changes. This makes them perfect for a variety of uses, such as environmental monitoring and medical diagnostics. Quantum sensors, for instance, could be utilized to identify magnetic field variations, which is useful for diagnosing diseases like cancer. They can also be used to track pollution levels by detecting changes in the quality of the air.

4.5. Transportation

The field of transportation is another possible use for quantum communication. The usage of quantum communication can raise the dependability and safety of transportation systems, including self-driving automobiles. One way to make the system more dependable and safe is to use quantum communication to facilitate communication between its many parts.

5. Conclusion

Quantum communication has enormous potential for safe data transfer in the future. Utilizing quantum repeaters, which, by amplifying and repeating the signal, may expand the potential range of quantum communication, is one possible way to get around the range restriction. Furthermore, developments in science and technology might result in more practical and affordable ways to use quantum communication on a bigger scale. Even if there are still a lot of challenges to be overcome, quantum communication has a vast and exciting potential for applications. Quantum communication is probably going to be a more crucial instrument for safe and effective data transport as technology develops.

Research funding within the areas of quantum communication and Quantum key distribution protocol is likely to rise as their potential becomes more evident. Quantum research is already receiving significant funding from governments, organizations, and private businesses, and it's likely that this pattern will continue. This funding will provide new discoveries and innovations while also accelerating the development and adoption of quantum communication technologies.

Funding Statement

This research was funded by the authors.

Acknowledgement

Special thanks to the Almighty God for making this possible. In the same vein, I appreciate my supervisor, Dr. (Mrs) Ifeoma Asianuba, for the unwavering support she gave me to make this a success.

More so, I won’t fail to mention my husband, who supported me financially and mentally. Crucial in that order are my parents, Prof and Prof. (Mrs) Uba Nwuba. Special thanks to the Editor of IJRES and his team.

References

[1] Rotem Arnon-Friedman, and Felix Leditzky, “Upper Bounds on Device-Independent Quantum Key Distribution Rates and a Revised Peres Conjecture,” *IEEE Transactions on Information Theory*, vol. 67, no. 10, pp. 6606–6618, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] I.B. Asinuba, *Optical Fiber Communication*, University of Port Harcourt Nigeria, 2024.

[3] S. Athanassias, “Securing the Future: The Rise of Quantum Communication,” National and Kapodistrian Universities of Athens, Greece, 2023.

[4] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert, “Privacy Amplification by Public Discussion,” *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988. [CrossRef] [Google Scholar] [Publisher Link]

[5] B.B. Blinov et al., “Observation of Entanglement between a Single Trapped Atom and a Single Photon,” *Nature*, vol. 428, pp. 153–157, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[6] Chenghao Lao et al., “Quantum Decoherence of Dark Pulses in Optical Microresonators,” *Nature Communications*, vol. 14, pp. 1-8, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] B.G. Christensen et al., “Detection-Loophole-Free Test of Quantum Nonlocality, and Applications,” *Physical Review Letters*, vol. 111, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[8] Daniele Cozzolino et al., “High-Dimensional Quantum Communication: Benefits, Progress, and Future Challenges,” *Advanced Quantum Technologies*, vol. 2, no. 12, pp. 1-17, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Eric A. Dauler et al., “Photon-Number-Resolution with Sub-30-ps Timing Using Multi-Element Superconducting Nanowire Single Photon Detectors,” *Journal of Modern Optics*, vol. 56, pp. 364–373, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[10] A. Einstein, B. Podolsky, and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality be Considered Complete?,” *Physical Review*, vol. 47, no. 10, pp. 777–780, 1935. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ilias P. Galanis, Ilias K. Savvas, and Georgia Garani, “Experimental Approach of the Quantum Volume on Different Quantum Computing Devices,” *The 14th International Symposium on Intelligent Distributed Computing*, vol. 1026, pp. 467-476, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Nicolas Gisin, and Rob Thew, “Quantum Communication,” *Nature Photonics*, vol. 1, pp. 165–171, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[13] Marissa Giustina et al., “Bell Violation Using Entangled Photons without the Fair-Sampling Assumption,” *Nature*, vol. 497, pp. 227–230, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[14] Robert H. Hadfield, “Single-Photon Detectors for Optical Quantum Information Applications,” *Nature Photonics*, vol. 3, pp. 696–705, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[15] M. Hosseini et al., “High Efficiency Coherent Optical Memory with Warm Rubidium Vapour,” *Nature Communications*, vol. 2, pp. 1-5, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[16] Rahul Jain, Carl A. Miller, and Yaoyun Shi, “Parallel Device-Independent Quantum Key Distribution,” *IEEE Transactions on Information Theory*, vol. 66, pp. 5567–5584, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Pierre Jobez et al., “Coherent Spin Control at Quantum Levek in an Ensemble-Based Optical Memory,” *Physical Review Letters*, vol. 114, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[18] Eneet Kaur, Mark M. Wilde, and Andreas Winter, “Fundamental Limits on Key Rates in Device-Independent Quantum Key Distribution,” *New Journal of Physics*, vol. 22, pp. 1-30, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Lijun Ma, Oliver Slattery, and Xiao Tang, "Optical Quantum Memory and Its Applications in Quantum Communication Systems," *Journal of Research of the National Institute of Standards and Technology*, vol. 125, pp. 1-13, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] M. Lucamarini et al., "Overcoming the Rate-Distance Limit of Quantum Key Distribution without Quantum Repeaters," *Nature,* vol. 557, pp. 400–403, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[21] Norbert Lütkenhaus, "Security against Eavesdropping Attacks in Quantum Cryptography," *Physical Review A,* vol. 54, no. 1, pp. 97–111, 1996. [CrossRef] [Google Scholar] [Publisher Link]

[22] Vadim Makarov, and Dag R. Hjelme, "Faked States Attack on Quantum Cryptosystems," *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[23] Vadim Makarov, Andrey Anisimov, and Johannes Skaar, "Effects of Detector Efficiency Mismatch on Security of Quantum Cryptosystems," *Physical Review A*, vol. 74, no. 2, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[24] Hao-Kun Mao et al., "High Performance Reconciliation for Practical Quantum Key Distribution Systems," *Optical and Quantum Electronics,* vol. 54, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Michele Masini, Stefano Pironio, and Erik Woodhead, "Simple and Practical DIQKD Security Analysis via BB84-Type Uncertainty Relations and Pauli Correlation Constraints," *Quantum*, vol. 6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Nikolai Miklin et al., "Exponentially Decreasing Critical Detection Efficiency for Any Bell Inequality," *Physical Review Letters,* vol. 129, no. 23, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] A. Muller et al., "'Plug and Play' Systems for Quantum Cryptography," *Applied Physics Letters,* vol. 70, pp. 793-795, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[28] Margarida Pereira et al., "Quantum Key Distribution with Correlated Sources," *Science Advances,* vol. 6, no. 37, pp. 1-16, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] John Preskill, "Quantum Computing and the Entanglement Frontier," *arXiv*, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[30] Ignatius W. Primaatmaja et al., "Security of Device-Independent Quantum Key Distribution Protocols: A Review," *arXiv,* vol. 7, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] Philip Purpura, *Security and Loss Prevention: An Introduction,* Elsevier Science, 2013. [Google Scholar] [Publisher Link]

[32] Philip Sibson et al., "Integrated Silicon Photonics for High-Speed Quantum Key Distribution," *Optica,* vol. 4, no. 2, pp. 172–177, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[33] Nuno A. Silva et al., "Tunable Light Fluids using Quantum Atomic Optical Systems," *Third International Conference on Applications of Optics and Photonics,* vol. 10453, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[34] Marco Tomamichel, Roger Colbeck, and Renato Renner, "A Fully Quantum Asymptotic Equipartition Property," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5840-5847, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[35] Paul D. Townsend, "Quantum Cryptography on Optical Fiber Networks," *Optical Fiber Technology,* vol. 4, no. 4, pp. 345-370, 1998. [CrossRef] [Google Scholar] [Publisher Link]

[36] Thomas Vidick, "Parallel DIQKD from Parallel Repetition," *arXiv,* 2017. [CrossRef] [Google Scholar] [Publisher Link]

[37] M.A. Vorontsov, G.W. Carhart, and J.C. Ricklin "Adaptive Phase-Distortion Correction Based on Parallel Gradient-Descent Optimization," *Optics Letters,* vol. 22, pp. 907–909, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[38] Kejin Wei et al., "High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics," *Physical Review X,* vol. 10, no. 3, pp. 1-11, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[39] Lixing You, "Superconducting Nanowire Single-Photon Detectors for Quantum Information," *Nanophotonics,* vol. 9, pp. 2673–2692, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] Yanbao Zhang, Honghao Fu, and Emanuel Knill, "Efficient Randomness Certification by Quantum Probability Estimation," *Physical Review Research,* vol. 2, no. 1, pp. 1-26, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[41] Jian Zhao, Yaping Liu, and Tianhua Xu, "Advanced DSP for Coherent Optical Fiber Communication," *Applied Sciences,* vol. 9, no. 19, pp. 1-20, 2019. [CrossRef] [Google Scholar] [Publisher Link]