Direct Research Journal of Engineering and Information Technology

Vol. 12(3), Pp. 26 -35, December 2024,
Author(s) retain the copyright of this article
This article is published under the terms of the Creative Commons Attribution License 4.0.
https://journals.directresearchpublisher.org/index.php/drjeit

Research Article
ISSN: 2354-4155

Next-Generation Secure Communication: Investigating Quantum Key Distribution Techniques for Ultrasonic Network Infrastructure

Friday Oodee PhiliP-Kpae[1]*, and Lloyd Endurance Ogbondamati[2]

[1]Department of Electrical and Electronics Engineering, Faculty of Engineering, Rivers State University, P. M. B. 5080, Nkpolu-Oroworukwo, Port Harcourt, Rivers State, Nigeria.
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, Rivers State University, P. M. B. 5080, Nkpolu-Oroworukwo, Port Harcourt, Rivers State, Nigeria.
*Corresponding author: philipkpae1@gmail.com

ABSTRACT

The rising need for secure communication has propelled the development of advanced solutions ensuring confidentiality, integrity, and authenticity. This study examines the potential application of Quantum Key Distribution (QKD) within ultrasonic network infrastructures to enable next-generation secure communication systems. Leveraging the principles of quantum mechanics, QKD offers unparalleled security for data transmission. The research focuses on integrating QKD with ultrasonic communication technologies, presenting promising findings. It is observed that Shannon's entropy achieves its maximum value of 1 bit when the probability of a bit being 1 or 0 is equally distributed (p = 0.5). Additionally, the analysis of the Quantum Bit Error Rate (QBER) reveals a linear increase from 0 to approximately 0.1 as the number of errors rises, highlighting the relationship between error rates and system performance. These results underscore the potential of QKD to enhance security in ultrasonic communication systems. The evaluation of the Signal-to-Noise Ratio (SNR) is conducted by analyzing the relationship between signal and noise power levels, demonstrating how SNR fluctuates with varying noise intensities, thereby reflecting the system's robustness against interference. Furthermore, the study highlights a decrease in the key generation rate, which declines from 10,000 to approximately 9,500 keys as the Quantum Bit Error Rate (QBER) rises from 0 to 0.1. In parallel, the research explores ultrasonic wave propagation, revealing that wave velocity exhibits significant growth, increasing from roughly 30 m/s to 100 m/s as the bulk modulus is elevated from 10^9 to 10^{11} Pascals. These findings provide valuable insights into system performance and material behavior under varying conditions. The study highlights the intricate interplay between key quantum communication metrics, emphasizing their implications for system design and optimization. It demonstrates that quantum mutual information increases proportionally with the entropy of Alice's and Bob's data, ranging from 0.5 to 1 bit. Additionally, the research evaluates error reconciliation efficiency, finding that corrected entropy values between 120 and 256 yield efficiency rates from 0.47 to 1. Furthermore, the eavesdropping detection probability rises significantly, reaching nearly 1 as the single detection probability increases from 0.01 to 0.1. These findings underscore the importance of carefully addressing these factors to enhance the reliability, efficiency, and security of quantum communication systems. The research also proposes strategies aimed at optimizing these systems to meet the growing demands of secure quantum information exchange.

Keywords: *Quantum Key Distribution (QKD), Ultrasonic communication systems, Secure Communication, Next-Generation Networks, Quantum Bit Error Rate, Entropy*

Article information
Received 2 October 2024;
Accepted 25 November 2024;
Published 6 December 2024
DOI: https://doi.org/10.4314/drjeit.v12i3.13

Citation: Phillip-Kpae, F. O., and Ogbondamati, L. E. (2024). Next-Generation Secure Communication: Investigating Quantum Key Distribution Techniques for Ultrasonic Network Infrastructure. Direct Research Journal of Engineering and Information Technology Vol. 12(3), Pp. 26 -35. This article is published under the terms of the Creative Commons Attribution License 4.0.

INTRODUCTION

In the ever-changing world of secure communication, the need for technology that can resist future challenges has never been greater (Dervisevic et al., 2024). As networks get more complex and cyber threats become more sophisticated, traditional encryption approaches prove to be insecure. This has resulted in a watershed moment in which novel technologies, such as quantum key distribution (QKD), are emerging to alter secure

communication paradigms. QKD uses quantum mechanics concepts to deliver previously unheard-of security.

QKD employs the basic rules of physics to guarantee that encryption keys stay secure, in contrast to traditional cryptographic techniques that depend on computational difficulties. For infrastructure that requires high degrees of confidentiality and resistance to interception, this makes it more alluring. As a relatively new communication technology, ultrasonic networks provide both remarkable prospects and difficulties for safe data exchange. These networks, which use ultrasonic sound waves to transport data, are being investigated more and more for use in industrial monitoring systems, medical equipment, and underwater communication.

However, the sensitivity and uniqueness of these networks render them vulnerable to developing security threats (Baron et al., 2022; Mohanta et al., 2017). Integrating QKD with ultrasonic network architecture provides a proactive solution to addressing these vulnerabilities. By applying quantum technologies to this domain, we can not only protect sensitive data but also lay the groundwork for a more resilient and data-proof communication system. This integration represents a shift towards next-generation security mechanisms that anticipate and neutralise potential threats to future communication systems (Antonovskaya et al., 2019).

This investigation of QKD in ultrasonic networks marks a watershed moment in the evolution of secure communication. By combining the benefits of quantum mechanics and sophisticated network technologies, this method attempts to establish a strong framework that can adapt to the changing demands of digital security. As we progress towards a future dominated by quantum engineering, such discoveries will be at the forefront of establishing trust and reliability in vital communication networks.

Review of related works

According to Dervisevic et al. (2024), secure communication is critical to the broad usage of telecommunication networks and the delivery of better services. As computational and mathematical techniques evolve, new cryptography approaches emerge. Quantum Key Distribution (QKD) is a groundbreaking technique that provides an Information-Theoretically Secure (ITS) way for establishing secure and security keys among rising communication device users. QKD networks, which use trusted repeaters, enable secure communication over long distances and among big user groups (Rass et al., 2020).

These systems provide as a supplement to traditional networks, generating, distributing, and managing ITS cryptographic keys. Given the scarcity of key resources, properly integrating QKD network services into critical infrastructure requires strong key management procedures. This paper examines critical management tactics in QKD networks, identifying viable solutions and promoting additional research into QKD technology (Tsai et al., 2021). A QKD network is intended to serve as a key foundation for the Internet, allowing the distribution of unconditionally safe keys as an alternative to current public-key cryptography methods that rely on complex mathematical computations. Many countries and research institutions have committed significant resources in studying QKD networks. This paper covers the existing literature and practical experiments on QKD networks, summarising significant findings such as network structures, key generation rates, communication distances, and routing protocols (Urbina et al., 2016). Furthermore, we identify three significant issues and offer future research paths and solutions for improving QKD network security (Green et al., 2023).

Hydropower facilities are often monitored or controlled remotely via centralized systems, with equipment manufacturers increasingly using public communication networks to oversee operations. While such methods improve efficiency and reliability, they also expose systems to potential cyber threats. For example, internet-based remote-control systems transmitting operational commands are exposed to security breaches. Although encryption using public-key cryptography helps safeguard transmitted data, these methods are increasingly at risk due to advances in quantum computing (*Dams Sector Landscape, 2019*).

QKD offers a solution by ensuring that any eavesdropping attempt is detectable through increased error rates, which can halt key generation. With a sufficiently low error rate and adequate photon detection, QKD enables the secure exchange of keys accessible only to the intended parties. This paper examines the application of QKD and quantum cryptography to protect critical infrastructures like hydropower facilities, providing a foundational framework for mitigating emerging cyber threats (Quaranta and Müller, 2021). Quantum Key Distribution, (2024) QKD systems face threats from various attack vectors, including quantum-specific vulnerabilities such as photon number splitting (PNS) and Trojan horse attacks, which can compromise security by reducing key rates and increasing errors. Classical threats, like man-in-the-middle (MITM) attacks, also pose risks by intercepting and altering classical communications. Developing secure and practical QKD systems requires addressing these issues through effective countermeasures. Researchers are working to extend QKD's operational range by overcoming the "attenuation limit." One solution involves quantum repeaters, which amplify weak signals without compromising security (Singh et al., 2020). Future advancements in QKD aim for seamless integration with existing communication systems, such as optical fibers

and satellites technology, enabling secure long-distance communication. Satellite-based QKD, for instance, holds the potential for global communication security, supporting quantum computing by facilitating entanglement and enabling a "quantum internet." Achieving this requires substantial progress in QKD protocols and infrastructure, promising transformative impacts on industries like finance-base, healthcare-technology, and government operations (Philippe and d'Errico, (2020). Choucair, (2024) a researcher from Universidad Politécnica de Madrid and several European institutes have introduced Madrrid Quantum Communication Infrastructure (MadQCI), a scalable quantum key distribution network that combines quantum and classical communication technologies, operating in real-world environments (Ijaz et al., 2022). It is Europe's largest and most complex quantum network that is a key part of European Quantum Communication Infrastructure (EuroQCI) initiative that creates a secure quantum internet of things. This achievement marks a significant step in merging quantum and classical communication systems, showcasing the potential for QKD to become integral to global telecommunications ecosystem (Ratnam et al., 2020; Martin et al., 2024).

Transitioning Quantum Networking

Traditional QKD networks, often designed for isolated use, have focused on optimizing key generation under fixed conditions. While effective for research, these systems lack scalability and cost efficiency for broader deployment. MadQCI addresses these issues through a software-defined networking (SDN) approach, allowing adaptability, seamless upgrades, and integration with existing telecom infrastructure (Whyatt et al., 2021). The network comprises 28 QKD modules from multiple manufacturers, interconnected via nine nodes in Madrid, using shared optical fibers for quantum and classical communication (Kwek et al., 2021). This configuration lowers costs and demonstrates QKD's commercial viability by leveraging existing telecom networks (Singh et al., 2020).

Future Oriented Design

MadQCI's modular and dynamic framework stands out as a notable advancement. Unlike traditional QKD systems that rely on dedicated fibers, it uses optical switches and SDN controllers to establish dynamic quantum links, enhancing scalability and resilience. This architecture supports various QKD technologies, enabling compatibility between devices from different manufacturers. Such heterogeneity is critical for widespread adoption, allowing for the integration of new technologies without significant disruptions, creating a flexible and future-ready quantum communication framework (Alrefaei, 2022).

MATERIALS AND METHODS

Materials

i. MATLAB software for simulations and data analysis.
ii. Quantum key distribution protocols
iii. Computational hardware (PC)
iv. Probabilistic and statistical models
v. Communication channel parameters (e.g., noise power, signal power).

Methods

Shannon's Entropy for Key Generation

Shannon's entropy measures the unpredictability of the key generated using QKD. High entropy ensures better randomness, a cornerstone of secure encryption for ultrasonic networks.

$$H(K) = -\sum_{i=1}^{n} p_i log_2(p_i) \quad (1)$$

H (K): Entropy of the key

p_i : Probability of each key bit

Quantum Bit Error Rate (QBER)

QBER quantifies the proportion of errors in transmitted quantum bits (qubits). Maintaining a low QBER is crucial to prevent security breaches caused by eavesdropping or noise.

$$QBER = \frac{N_{error}}{N_{total}} \quad (2)$$

N_{error} : Number of erroneous qubits

N_{total}: Total transmitted qubits

Signal-to-Noise Ratio (SNR)

SNR evaluates the clarity of ultrasonic signals used in QKD. A high SNR ensures effective communication by minimizing the interference during the secure key exchange.

$$SNR = \frac{P_{signal}}{P_{noise}} \quad (3)$$

P_{signal} : Power of the transmitted signal

P_{noise} : Power of the noise

Key rate (R)

The key rate defines the efficiency of secure key generation. It factors in the total qubits transmitted, error rate, and any information leakage to ensure secure communication.

$$R = Q(1 - 2QBER) - leakage \quad (4)$$

Q: Total qubits transmitted

leakage: Information leaked during transmission

Ultrasonic wave propagation

This equation describes the velocity of ultrasonic waves in the medium, which is critical for analyzing signal behavior and optimizing QKD performance in ultrasonic networks.

$$v = \sqrt{\frac{B}{\rho}} \quad (5)$$

v: Velocity of ultrasonic waves
B: Bulk modulus of the medium
ρ: Density of the medium

Quantum mutual information

Quantum mutual information measures how much data is shared securely between two parties (Alice and Bob) during QKD. It ensures minimal leakage to eavesdroppers.

$$I(A;B) = H(A) + H(B) - H(A,B) \quad (6)$$

H(A): Entropy of Alice's data
H(B): Entropy of Bob's data
H(A,B): Joint entropy of their data

Error reconciliation efficiency

Error reconciliation efficiency quantifies how effectively QKD corrects errors without losing usable bits. Higher efficiency is vital in noisy environments, like ultrasonic networks.

$$E = \frac{H_{corrected}}{H_{original}} \quad (7)$$

$H_{corrected}$: Entropy of corrected data
$H_{original}$: Entropy of the original data

Eavesdropping detection probability

This equation calculates the probability of detecting an eavesdropper. It emphasizes how transmitting more qubits increases the likelihood of spotting unauthorized access.

$$P_d = 1 - (1 - p)^2 \quad (8)$$

P_d: Detection probability
p: Probability of detecting a single eavesdropped qubit
n: Total number of qubits

The flowchart represents the systematic progression and algorithm of the study, outlining the key stages involved in analyzing quantum communication metrics and ensuring secure key generation. It begins with initializing system parameters, such as probabilities, error counts, and power levels. Shannon's entropy calculation is performed to evaluate the randomness of generated keys. The Quantum Bit Error Rate (QBER) is determined to assess the integrity of the quantum channel. Signal-to-Noise Ratio (SNR) is then computed to measure the impact of noise on signal quality. Subsequently, the key rate is derived as a function of QBER and leakage, reflecting the efficiency of key generation. Ultrasonic wave propagation is modeled to study velocity changes with material properties. Quantum mutual information quantifies the shared information between communicating parties. Error reconciliation efficiency is analyzed to optimize corrected data. Finally, eavesdropping detection probability is calculated to secure communication, ensuring system robustness against interception as shown in (Table 1 and Figure 1).

RESULTS AND DISCUSSION

Shannon's Entropy for Key Generation

The analysis of Shannon's entropy in the context of key generation provides insight into the uncertainty associated with the selection of each bit in a cryptographic system. Shannon entropy measures the amount of unpredictability or randomness in the information generated, which is crucial for the security of key distribution methods. As shown in (Figure 2**)**, the entropy increases with the probability of a bit being set to "1" (denoted as p), reaching its peak at a probability of 0.5. This is where the entropy is maximized, implying that the system is at its most unpredictable, and hence the most secure. The plot illustrates how the entropy H (K) behaves with a range of probabilities p from 0.01 to 0.99. The graph demonstrates that at extremes (close to 0 or 1), the entropy drops, indicating low unpredictability.

Table 1: Quantitative results of system performance matrices.

Parameter	Unit	Value/Range	Description
Entropy of the key	Bits	128–256	Desired level of randomness for secure encryption keys.
Probability of each bit	-	0.01–0.99	Probability distribution of key bits used in Shannon's entropy calculation.
Number of erroneous qubits	Bits	1–1000	Total number of erroneous qubits detected during transmission.
Total transmitted qubits	Bits	10,000–100,000	Total number of qubits sent during a QKD session.
Signal power	Watts	$1 \times 10^{-6} \times -1 \times 10^{-3}$	Power of the ultrasonic signal used for communication.
Noise power	Watts	$1 \times 10^{-9} \times -1 \times 10^{-6}$	Environmental or system noise affecting the ultrasonic signal.
Total qubits transmitted	Bits	10,000–100,000	Number of qubits used for secure key generation.
Leakage information	Bits	0.01–0.1	Amount of information potentially leaked due to errors or eavesdropping.
Bulk modulus	Pascal	$1 \times 10^{9} \times -1 \times 10^{11}$	Measure of the material's resistance to compression for ultrasonic wave travel.
Density of medium	kg/m³	800–2000	Density of the propagation medium (e.g., air, water).
Entropy of corrected data	Bits	120–256	Entropy of the data after error correction processes.
Entropy of original data	Bits	128–256	Entropy of the original uncorrected data.
Detection probability	-	0.01–1.00	Probability of detecting an eavesdropper in the QKD system.
Probability of single detection	-	0.01–0.1	Probability of detecting a single compromised qubit.
Number of qubits transmitted	bits	10,000–100,000	Total number of qubits transmitted during the session.

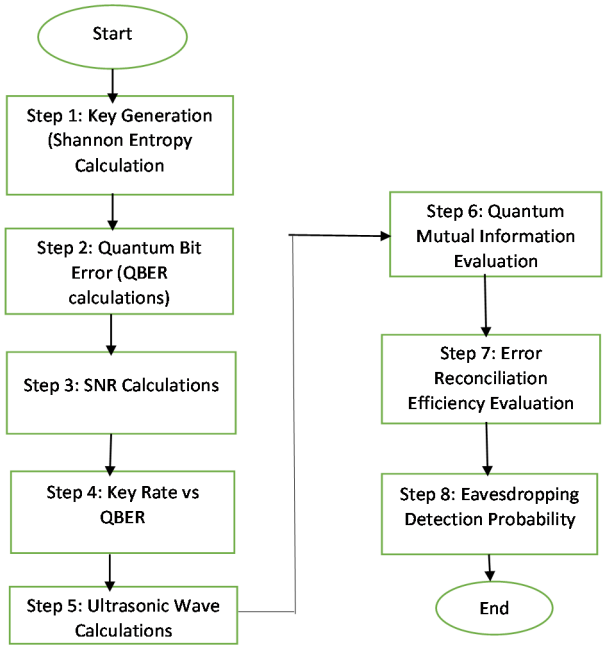

Figure 1: Flowchart of the QKD Algorithm.

This trend is typical in binary systems, where the certainty of outcomes reduces entropy as the system approaches either extreme (0 or 1). The entropy value ranges from 0 at the extremes to a maximum of

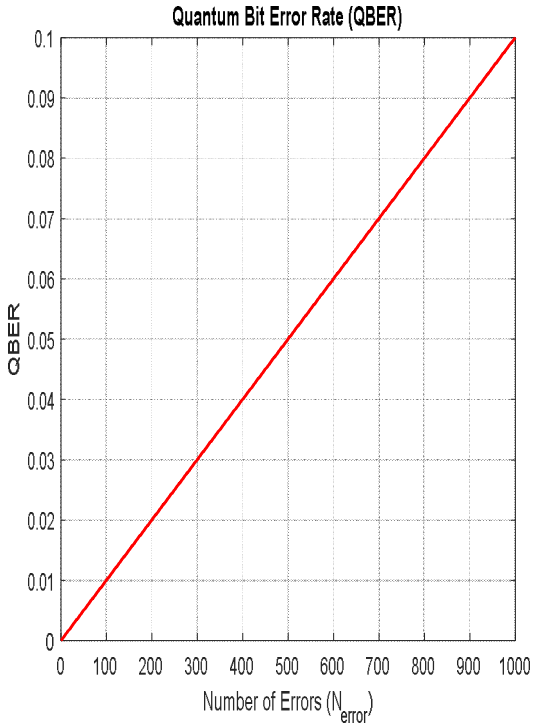

Figure 3: Quantum Bit Error Rate

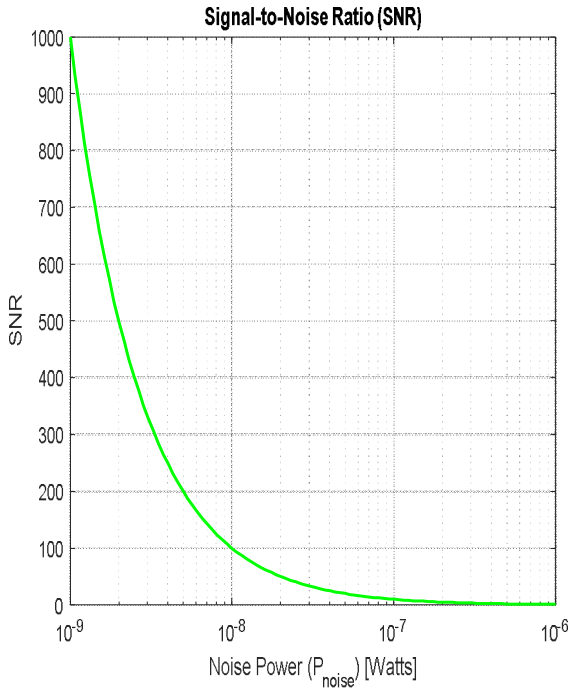

Figure 4: Signal to Noise Ratio

approximately 1 bit when p equals 0.5, reflecting the highest uncertainty in bit selection.

Quantum Bit Error Rate (QBER)

The Quantum Bit Error Rate (QBER) is a critical measure of the reliability of quantum key distribution systems, indicating the proportion of quantum bits (qubits) that are received incorrectly due to noise or interference during transmission. As depicted in (Figure 3**)**, the relationship between the number of errors and the QBER is linear, with the error rate increasing in direct proportion to the number of errors. This graph reveals that for a total of 10,000 qubits, if the number of errors increases, so does the QBER, which starts at 0 and increases to approximately 0.1 as the number of errors reaches 1000. The plot effectively communicates that the QBER is highly sensitive to the transmission errors in quantum systems, and any significant increase in errors diminishes the overall security and effectiveness of the quantum communication protocol.

Signal-to-Noise Ratio (SNR)

Signal-to-Noise Ratio (SNR) is a critical parameter in determining the quality of a signal in communication systems, representing the ratio of the signal power to the noise power. As shown in (Figure 4**)**, the SNR is inversely proportional to the noise power, with the signal power kept constant at $10^{-9}\ to\ 10^{-6}\ at\ 1 \times 10^{-6}$ watts. The graph uses a logarithmic scale to display noise power from $10^{-9}\ to\ 10^{-6}$ watts, showing that as noise power increases, the SNR decreases exponentially. The curve demonstrates a significant reduction in SNR when the noise power is elevated, emphasizing the importance of maintaining a low noise environment in communication systems. The SNR values begin to significantly drop as the noise power increases, indicating poorer signal quality and highlighting the necessity for efficient noise management in real-world systems.

Key Rate vs. QBER

The key rate (R) is an essential metric in quantum cryptography, quantifying the number of secure bits that can be generated per unit of time or qubit transmission. Figure 5 presents the relationship between the key rate and the Quantum Bit Error Rate (QBER). The key rate decreases as the QBER increases, which is reflected in the decreasing curve. For QBER values ranging from 0 to 0.1, the key rate drops sharply, starting at a value of around 10,000 for zero errors and decreasing steadily as the QBER increases. The plot demonstrates how error rates severely impact the efficiency of key generation, making the system less effective as errors in quantum communication increase. The key rate is negatively impacted by even small increases in QBER, which is a

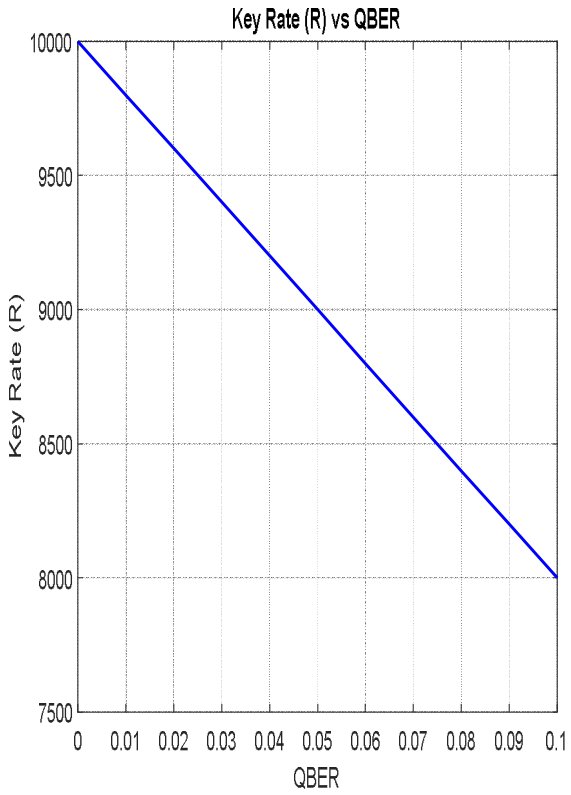

Figure 5: Key Rate vs QBER

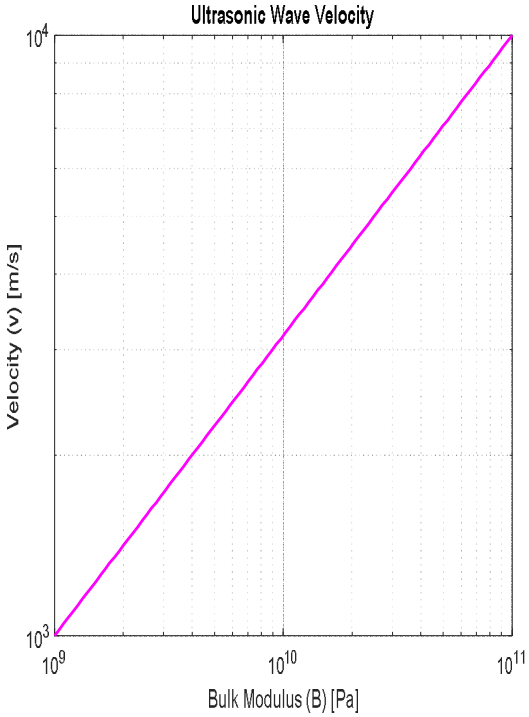

Figure 6: Ultrasonic wave velocity

critical concern for quantum communication systems where maintaining a low error rate is essential for secure key generation.

Ultrasonic wave propagation

The study of ultrasonic wave propagation, represented in (Figure 6), reveals the relationship between the bulk modulus of a material and the wave velocity. The graph displays a logarithmic scale for the bulk modulus, ranging from 10^9 *to* 10^{11} Pascals, and the corresponding wave velocity, which increases with the bulk modulus. The plot shows a clear positive correlation, with the wave velocity increasing as the bulk modulus increases. This relationship highlights the importance of material properties, such as bulk modulus and density, in determining how quickly ultrasonic waves can propagate through a given medium. The wave velocity reaches higher values for materials with a higher bulk modulus, which is typical for denser and stiffer materials. This result has practical implications in fields like non-destructive testing, where wave velocity is used to assess material integrity.

Quantum mutual information

Quantum mutual information quantifies the total amount of information shared between two quantum systems, such as Alice's and Bob's data. Figure 7 illustrates how the mutual information changes with the entropy of Alice's data. The plot reveals a positive correlation between the entropy of Alice's data and the mutual information I (A;B), meaning that as Alice's data becomes more unpredictable (increasing entropy), the amount of mutual information also increases. The graph demonstrates how the uncertainty in Alice's data influences the shared information between two quantum systems, which is vital for understanding the strength of the connection in quantum communication protocols. The mutual information grows steadily, reflecting the dynamic relationship between data entropy and the informational exchange between quantum systems.

Error reconciliation efficiency

Error reconciliation is a crucial step in quantum communication, ensuring that discrepancies between two parties' data are minimized. Figure 8 presents the efficiency of error reconciliation, showing how the efficiency changes with corrected entropy values. The plot shows that as the corrected entropy increases, the efficiency also rises. Starting at lower values of corrected entropy, the efficiency begins to climb and stabilizes as the corrected entropy approaches 256. The efficiency approaches a maximum value of 1 as the corrected

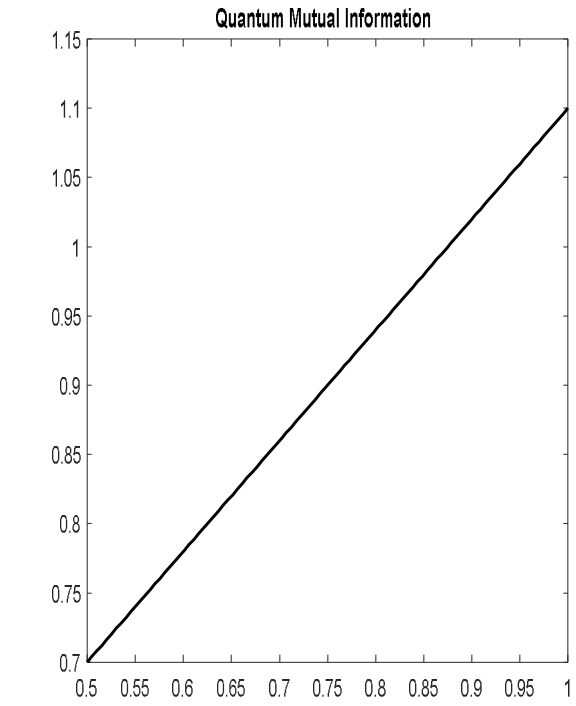

Figure 7: Quantum Mutual Information

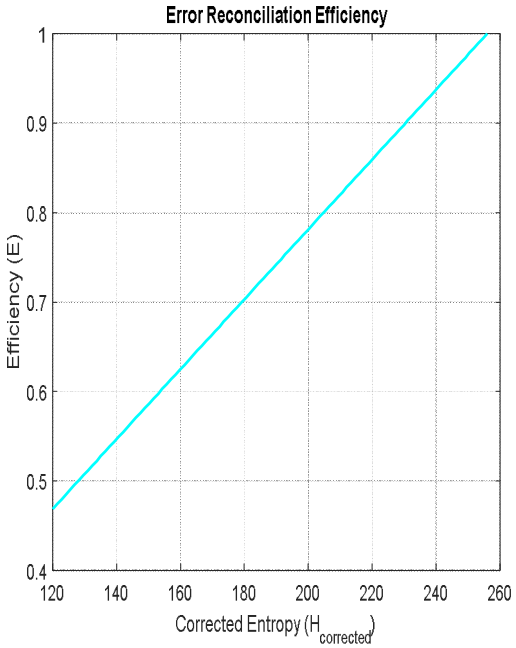

Figure 8: Error Reconciliation Efficiency

entropy reaches its highest value, indicating that the error reconciliation process becomes nearly perfect when the corrected entropy is large. This plot underlines the importance of efficient error correction methods in quantum communication systems, where higher efficiency leads to more reliable and secure data exchange.

Eavesdropping detection probability

Eavesdropping detection is a key aspect of ensuring the security of quantum communication systems. Figure 9 displays the probability of detecting eavesdropping, which increases as the single detection probability increases. The plot illustrates that as the detection probability rises from 0.01 to 0.1, the overall detection probability increases sharply. With 10,000 qubits, the detection probability approaches 1 as the single detection probability nears its maximum value. This indicates that the system becomes more reliable in detecting eavesdropping attempts as the detection probability increases, highlighting the effectiveness of quantum cryptography in securing communications against unauthorized interception.

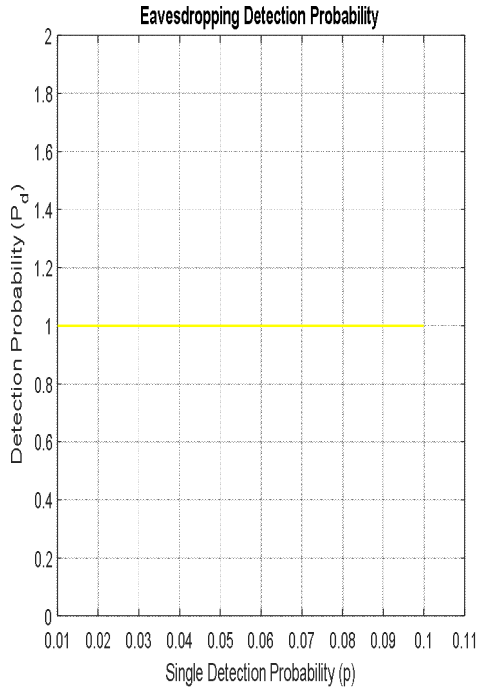

Figure 9: Eavesdropping Detection Probability

Conclusion

This study has effectively explored various aspects of quantum communication systems, focusing on key metrics such as key generation, quantum bit error rate (QBER), signal-to-noise ratio (SNR), and the overall efficiency of quantum protocols. By systematically analyzing these parameters, the research has made significant contributions to the understanding of quantum

systems, particularly in terms of their operational dynamics and potential for real-world applications.

The study began with an in-depth examination of Shannon's entropy, demonstrating how different probability distributions impact the key generation process, a foundational concept in secure quantum communication. Through this analysis, it became clear that entropy plays a crucial role in determining the randomness and security of the keys generated for quantum protocols. Additionally, the exploration of quantum bit error rates revealed critical insights into how errors affect the integrity of quantum communication, providing valuable information for improving error correction methods.

The signal-to-noise ratio (SNR) analysis also shed light on the delicate balance between signal strength and noise, offering a deeper understanding of the physical limitations in quantum communication systems. By examining the relationship between noise power and SNR, the study highlighted how noise management is essential to optimizing system performance. The key rate versus QBER analysis further emphasized the importance of maintaining a low error rate to ensure efficient key distribution, underscoring the need for robust error reconciliation techniques. Moreover, the investigation into ultrasonic wave propagation and quantum mutual information offered a unique perspective on the broader applicability of quantum concepts beyond communication, particularly in the field of material science and information theory. These findings contribute to a more holistic view of quantum mechanics and its potential to revolutionize various sectors.

This study's contributions to knowledge lie in its ability to integrate diverse quantum metrics and demonstrate their interdependencies, providing a comprehensive framework for understanding the performance and efficiency of quantum communication systems. By developing a clearer picture of how various factors such as entropy, QBER, and SNR interact, the research offers a foundational understanding that can be applied to enhance future quantum protocols and technologies.

However, there are opportunities for further research to improve these systems. Future studies could focus on refining error reconciliation protocols to minimize the impact of QBER on the overall system performance. Additionally, investigating the impact of environmental factors on SNR and quantum error rates could provide valuable insights into how quantum systems can be made more resilient to real-world conditions. There is also a need for more practical applications that bridge the gap between theoretical findings and real-world deployment of quantum communication technologies.

Overall, this research has provided essential insights into the key metrics of quantum communication, contributing significantly to the knowledge base. The findings offer a solid foundation for future advancements, particularly in enhancing the security, efficiency, and robustness of quantum communication systems. By addressing the challenges identified and exploring the areas for further improvement, quantum technologies can move closer to practical implementation, bringing us closer to the realization of secure, high-performance quantum networks.

REFERENCES

Alrefaei, A. S. (2022). "An Overview of Securing SCADA Systems: The Gap in the Physical Security Measure," in *Proc. 2022 Fifth National Conference of Saudi Computers Colleges (NCCC)*, Makkah, Saudi Arabia, Dec. 17-18, 2022, pp. 88–91.

Antonovskaya, G., N. Kapustian, I. Basakina, N. Afonin, and Moshkunov, K., (2019). "Hydropower Dam State and Its Foundation Soil Survey Using Industrial Seismic Oscillations," *Geosciences*, vol. 9, p. 187, 2019. doi: 10.3390/geosciences9040187.

Baron, P., M. Kočiško, S. Hlavatá, and Franas, E. (2022). "Vibrodiagnostics as a predictive maintenance tool in the operation of turbo generators of a small hydropower plant," *Adv. Mech. Eng.*, vol. 14, p. 16878132221101023, 2022. doi: 10.1177/16878132221101023.

Choucair, C. (2024). "MadQCI: A Scalable Quantum Key Distribution Network Improving Secure Communications Infrastructure," *Q-munity*, Sep. 4, 2024. [Online]. Available: https://www.qmunity.com/

Dams Sector Landscape (2023), Technical Report, CISA, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Washington, DC, USA, 2019. Available online: https://damsafety-prod.s3.amazonaws.com/s3fs-public/files/6.%20Dams%20Sector%20Landscape.pdf (accessed Dec. 4, 2023).

Dervisevic, E., A. Tankovic, E. Fazel, R. Kompella, P. Fazio, M. Voznak, and Mehic, M. (2024). "Quantum Key Distribution Networks – Key Management: A Survey," *IEEE Trans. Quantum Eng.*, 2024. doi: 10.1109/TQE.2024.XXXXXXX. [Online]. Available: arXiv:2408.04580v1 [cs.CR], Aug. 8, 2024. License: CC BY-NC-SA 4.0.

Green, A., J. Lawrence, G. Siopsis, N. A. Peters, and Passian, A.(2023). "Quantum Key Distribution for Critical Infrastructures: Towards Cyber-Physical Security for Hydropower and Dams," *Sensors*, vol. 23, no. 24, Article 9818, Dec. 2023. [Online]. Available: https://doi.org/10.3390/s23249818.

Ijaz, S., A. S. Rana, Z. Ahmad, M. Zubair, Y. Massoud, and Mehmood, M. Q. (2022). "The Dawn of Metadevices: From Contemporary Designs to Exotic Applications," *Adv. Devices Instrum.*, vol. 2022, p. 9861078, 2022. doi: 10.1155/2022/9861078.

Kwek, L. C. , L. Cao, W. Luo, Y. Wang, S. Sun, X. Wang, and Liu, A. Q. (2021). "Chip-based quantum key distribution," *AAPPS Bull.*, vol. 31, p. 15, 2021. doi: 10.1007/s43673-021-00016-y.

Martin, V., J. P. Brito, L. Ortiz, R. B. Mendez, J. S. Buruaga, R. J. Vicente, A. Sebastian-Lombrana, D. Rincon, F. Perez, C. Sanchez, M. Peev, H. H. Brunner, F. Fung, A.Poppe, F. Frowis, a. J. Shields, R. I. Woodward, H. Griesser, S. Roehrich, F. de la Iglesia, C. Abellan, M. Hentschel, J. M. Rives-Moscoso, Pastor-Perales, J. Folgueira, & Lopez, D.(2024). " MadQCI: A Heterogeneous and Scalable SDN-QKD Network Deployed in Production Facilities" npj/Quantum Information, Published in Partnership with The University of New South Wales, 2024, https://doi.org/10.1038/s41534-024-00873-2, Retrieved 25/11/2024.

Mohanta, R. K., T. R. Chelliah, S. Allamsetty, A. Akula, and Ghosh, R. (2017). "Sources of vibration and their treatment in hydro power stations—A review," *Eng. Sci. Technol. Int. J.*, vol. 20, pp. 637–648, 2017. doi: 10.1016/j.jestch.2016.12.005.

Ouellet, S. M., J. Dettmer, G. Olivier, T. DeWit, and Lato, M. (2022). "Advanced monitoring of tailings dam performance using seismic

noise and stress models," *Commun. Earth Environ.*, vol. 3, p. 301, 2022. doi: 10.1038/s43247-022-00492-0.

Philippe, S., and d'Errico, F. (2020). "A physical unclonable neutron sensor for nuclear arms control inspections," *Sci. Rep.*, vol. 10, p. 20605, 2020. doi: 10.1038/s41598-020-77432-6.

Quantum Key Distribution (2024).: The Future of Secure Communication," *Quantum News*, Aug. 20, 2024. [Online]. Available: https://www.quantumzeitgeist.com/

Quaranta, E., and Müller, G. (2021). "Noise Generation and Acoustic Impact of Free Surface Hydropower Machines: Focus on Water Wheels and Emerging Challenges," *Int. J. Environ. Res. Public Health*, vol. 18, p. 13051, 2021. doi: 10.3390/ijerph182413051.

Rass, S., S. Schauer, S. König, and Zhu, Q. (2020). *Cyber-Security in Critical Infrastructures*, vol. 297. Berlin/Heidelberg, Germany: Springer, 2020.

Ratnam, E. L., K. G. Baldwin, P. Mancarella, M. Howden, and Seebeck L. (2020). "Electricity system resilience in a world of increased climate change and cybersecurity risk," *Electr. J.*, vol. 33, no. 1, p. 106833, 2020. doi: 10.1016/j.tej.2020.106833.

Singh, P., S. Singh, S. Vardhan, and Patnaik A. (2020). "Sustainability of maintenance management practices in hydropower plant: A conceptual framework," *Mater. Today Proc.*, vol. 28, pp. 1569–1574, 2020. doi: 10.1016/j.matpr.2020.03.716.

Tsai, C.-W., C.-W. Yang, J. Lin, Y.-C. Chang, and R.-S(2021).. Chang, "Quantum Key Distribution Networks: Challenges and Future Research Issues in Security," *Applied Sciences*, vol. 11, no. 9, Article 3767, Apr. 2021. [Online]. Available: https://doi.org/10.3390/app11093767.

Urbina, D. I., J. A. Giraldo, A. A. Cardenas, and Tippenhauer, N. O. (2016). "Survey and new directions for physics-based attack detection in process control systems," in *Proc. IFIP Annu. Conf. Data Applications Security Privacy*, Trento, Italy, Jul. 18-20, 2016, Springer, Cham, Switzerland, 2016, pp. 65–81.

Whyatt, M., M. V. Whyatt, D. E. Thorsen, M. D. Watson, K. D. Ham, P. A. Pederson, A. D. McKinnon, and DeSomber, K. R.(2021). *Toward a Resilient Cybersecure Hydropower Fleet: Cybersecurity Landscape and Roadmap 2021*, Technical Report PNNL-32053, PNNL, Richland, WA, USA, 2021.