Simulating Multi-Node Quantum Key Distribution Using Quantum Secret Sharing

Dhalia Sweetlin J
Department of Information Technology
MIT Campus, Anna University
Chennai, India
dhaliasweetlin@gmail.com

Nithin Srivatsan S
Department of Information Technology
MIT Campus, Anna University
Chennai, India
nithinsrini2003@gmail.com

Sowmiya S
Department of Information Technology
MIT Campus, Anna University
Chennai, India
sowmiyaslatha@gmail.com

***Abstract*— This project implements Quantum Key Distribution (QKD) with Quantum Secret Sharing (QSS) to securely distribute encryption keys among multiple nodes. QSS splits keys into fragments, allowing only specific node groups to reconstruct the complete key. These keys are then used for encryption and decryption, ensuring data confidentiality. Intermediate nodes enhance security by introducing quantum protections during key transmission. The system addresses real-world challenges like scalability and efficient network handling, demonstrating that QKD combined with QSS is a reliable framework for secure communication in quantum networks. This approach paves the way for building highly secure and scalable quantum communication systems in the future.**

***Keywords*— Quantum Key Distribution (QKD), Quantum Secret Sharing(QSS), Quantum Networks, Quantum Cryptography, Secure Communication, Secure Key Exchange, Encryption and Decryption.**

I. INTRODUCTION

Quantum Key Distribution (QKD) leverages quantum mechanics to enable secure sharing of secret keys. Unlike conventional methods, QKD relies on principles like superposition and entanglement, making it extremely challenging for attackers to intercept or duplicate the keys. Any attempt to eavesdrop disturbs the quantum states, enabling detection and safeguarding the communication. While traditional QKD typically involves two participants, such as Alice and Bob, real-world scenarios often require multiple devices or nodes to exchange information. To address this, Quantum Secret Sharing (QSS) is employed. In QSS, a secret key is divided into fragments and distributed among various nodes. Only a specific group of nodes can collaboratively reconstruct the complete key, ensuring no single node can access the secret independently, thereby enhancing security.

This project explores the integration of QKD and QSS in a multi-node quantum network. The system utilizes quantum entanglement to securely distribute information across nodes. Each node receives a fragment of the key, and only the designated group of nodes can combine their fragments to regenerate the full key. The project also demonstrates how the distributed keys are applied for encryption and decryption. Sensitive data is encrypted using the keys generated through QKD and QSS, ensuring secure communication, and decryption is only possible when the original key is reconstructed by the authorized nodes.

The results of our simulations demonstrate that combining QKD with QSS enhances the reliability and security of key distribution. By incorporating encryption and decryption mechanisms, this approach highlights its potential for creating robust and secure quantum communication systems suitable for future applications.

II. LITERATURE SURVEY

Quantum Key Distribution (QKD) is a secure communication method that uses quantum physics to detect eavesdropping and ensure safe key sharing. The BB84 protocol is a foundational QKD method, but combining QKD WITH Quantum Secret Sharing (QSS) offers better security for multi-node networks by splitting keys intoparts and requiring specific groups to reconstruct them. Despite challenges like limited distance and high costs, advances such as trusted relays, quantum repeaters,and phase-coding techniques have improved scalability and reliability. Recent research explores integrating QKD with classical networks, creating hybrid system for
better flexibility. This project implements a multi-node QKD system using modified QSS to study its performance in noiseless and eavesdropping scenarios, contributing to secure quantum communication in complex networks.【1】

Uses quantum mechanics principles, like Heisenberg's Uncertainty Principle and the No-Cloning Theorem, to make sure keys are securely exchanged. The BB84 protocol, one of the earliest and most-used QKD methods, encodes information in photon states to create a secure key. While it is effective, QKD faces challenges like limited distance and vulnerability to hacking methods like Photon Number Splitting (PNS) and detector attacks.

To improve security, advanced techniques like Decoy-State QKD and Measurement-Device-Independent QKD (MDI-QKD) have been introduced. These methods address vulnerabilities in photon sources and detectors, making QKD more robust against attacks. Another focus is integrating QKD into existing optical fiber networks. This requires managing weak quantum signals alongside strong classical signals, which is achieved through multiplexing techniques like Wavelength Division Multiplexing (WDM) and Time Division Multiplexing (TDM). These studies highlight the importance of trusted relays and advanced architectures to extend QKD's range and efficiency. Efforts to combine QKD with Quantum Secret Sharing (QSS) are also being explored to enhance security in multi-node networks, paving the way for secure global communication. 【2】

Uses quantum physics to create secure cryptographic keys, ensuring protection against future quantum computing threats. QKD networks integrate quantum and classical channels to securely transmit keys over distances, using techniques like trusted repeaters and multi-path routing to overcome challenges like signal loss and limited communication range. Advances such as Software-Defined Networking (SDN) and key pool-based routing help improve efficiency and scalability in QKD networks. These developments aim to build secure and robust quantum communication systems while addressing current limitations like high costs and the lack of practical quantum repeaters. 【3】

Current methods have problems like limited distance, slow key generation, and issues with trusted relay (CTR) systems, which require all relay nodes to be secure. If even one node is hacked, the whole system becomes unsafe. To fix this, a new solution called SDQTRF uses Software-Defined Networking (SDN). SDN separates the control and data parts of the network, making it easier to manage. The SDQTRF model introduces better ways to handle failures in key relays, such as recycling failed keys, using smart recovery techniques, and finding new secure routes when needed.

This new model performs much better than older systems. It generates keys more efficiently, recovers quickly after failures, and reduces blocked services. Tests on different types of networks showed that it makes QKD systems more reliable and secure. By reusing failed keys and creating backup plans, it ensures better use of resources while keeping communications safe. Future upgrades, like smarter learning methods, could make it even more effective for larger quantum networks. 【4】

Quantum Key Distribution (QKD) is a safe way to share secret keys, but using it over long distances requires relays. Relays can be a problem because if even one is hacked, the whole system is at risk. This paper introduces a simple method to make QKD relay networks safer using secret sharing. Instead of using multiple physical paths, the method creates several logical channels on the same path by randomly turning relays on and off. This way, an attacker would need to hack all the relays to steal the key, making it much more secure.

The method also adds one extra relay to improve safety without making the system too complicated. If a relay is hacked, the attacker can't get the full key because the key is spread across the different channels. The system can also detect if someone tries to tamper with the relays. This technique is simple but very effective, and it can make QKD networks much safer and ready for real-world use. 【5】

Quantum secret sharing (QSS) is a way to split a secret into parts and share it with a group of people so they can work together to rebuild the secret. This paper introduces a new and easier method for QSS using a special type of quantum state. It lets the participants check if the shared secret is correct and recover it with simple steps. This method is faster and cheaper because it avoids using complicated tools like hash functions and instead uses basic math, making it more practical for everyday use. This new method is easier to use compared to older ones because it doesn't rely on complex quantum systems or difficult operations. It is also safer, as it protects the secret from both hackers and dishonest participants. The method can be improved further to work with bigger quantum systems, making it flexible and useful for future secure communication and data sharing. 【6】

III. QKD - QUANTUM KEY DISTRIBUTION

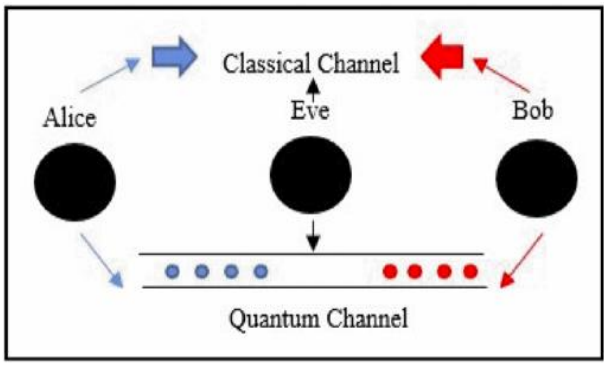

Figure 1 : Quantum Key Distribution

Quantum Key Distribution (QKD) is a method used to send secret keys securely between two people, Alice and Bob. It uses the strange rules of quantum mechanics to make sure no one can listen in on the key exchange.

Quantum Superposition and Entanglement: In quantum mechanics, particles like photons (light particles) can be in many states at once. When particles are entangled, they are connected in such a way that changing one particle also changes the other, no matter how far apart they are.

Uncertainty Principle: This rule says that some properties of particles (like position and speed) cannot be known perfectly at the same time. This helps QKD because if someone tries to eavesdrop, it will change the state of the particles, and Alice and Bob will know someone is listening.

No-Cloning Theorem: This rule says that quantum information can't be copied perfectly. So, if someone tries to copy the key, they will be caught.

SECURITY OF QKD:

Eavesdropping Detection: If someone tries to intercept the key, it will change the state of the quantum particles. Alice and Bob can check for errors and detect eavesdropping. If there are too many errors, they will discard the key and try again.

Quantum Bit Error Rate (QBER): This is a measure of how many errors there are in the key exchange. A low QBER means no one is listening, while a high QBER means there might be an eavesdropper.

Post-Quantum Cryptography: While QKD is secure, it may still need protection against future quantum computers. Researchers are working on new methods to keep data safe even with powerful quantum computers.

QSS – QUANTUM SECRET SHARING

Quantum Secret Sharing (QSS) is a method used to share a secret safely between multiple people, using the rules of quantum mechanics. It is like splitting a secret into pieces and giving each piece to a different person in such a way that no single person can understand the secret alone. Only when everyone comes together can the secret be revealed.

WORKING:

1. Encoding the Secret:

The secret is encoded into quantum particles (usually photons). Alice (the person who has the original secret) creates an entangled set of qubits. Alice shares these entangled qubits with multiple people (Bob, Charlie, etc.). Each person receives part of the information but cannot understand the secret alone.

2. Measurement and Sharing:

The people holding the quantum bits are called **shareholders**. Each shareholder measures their part of the secret. The measurements are designed in such a way that, when all the measurements are combined, the secret is revealed.

3. Eavesdropping Prevention:

If any shareholder tries to reveal their part of the secret without the others, the secret cannot be properly reconstructed. This ensures that the secret can only be reconstructed when all shareholders collaborate.

IV. PROPOSED WORK

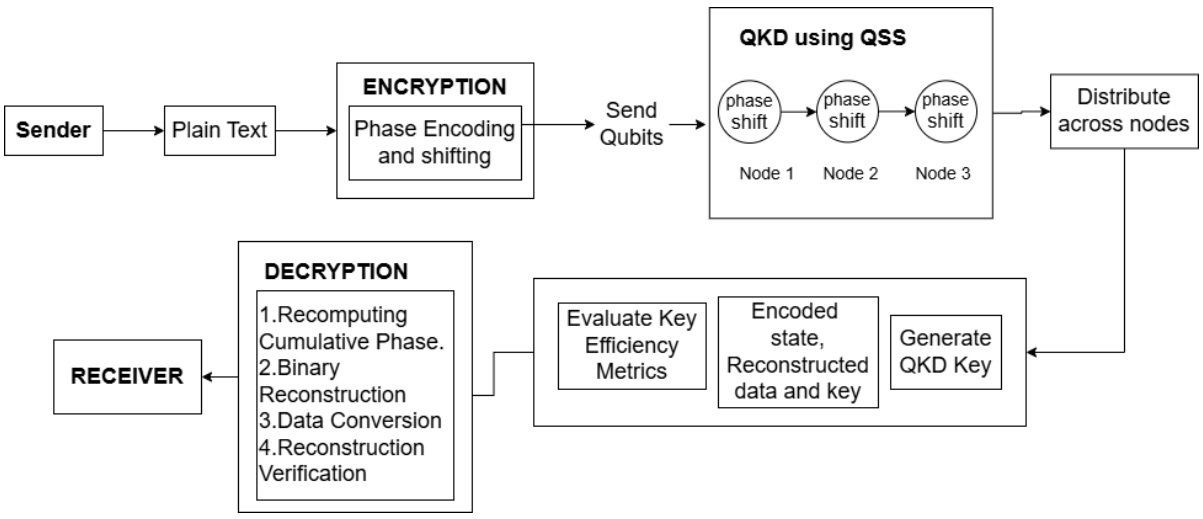

Figure 2 : Architecture Diagram

The proposed work focuses on simulating a robust and efficient Quantum Key Distribution (QKD) protocol integrated with Quantum Secret Sharing (QSS) for secure communication in multi-node networks. This approach utilizes quantum principles such as phase encoding and phase shifting to ensure data confidentiality, integrity, and resistance to eavesdropping.

Initially, a secure random key is generated using QKD, which is a fundamental step in establishing quantum-secured communication. The key is generated dynamically within a predefined range, ensuring variability and enhancing security. This key is later used for encrypting sensitive data using a quantum-inspired secret sharing mechanism.

The data encryption process involves converting the input data into binary format and applying phase encoding to each bit. To simulate the quantum behavior, random phase shifts are introduced for each bit across multiple nodes. The cumulative phase shifts are calculated to represent the encoded quantum states, effectively distributing the secret across all participating nodes. This approach ensures that no single node can reconstruct the data independently, thereby enhancing security. For decryption, the proposed system employs a quantum reconstruction process. This involves validating the cumulative phase shifts received from all nodes to reconstruct the original data. The consistency of phase calculations ensures that any tampering or interception is immediately detected, maintaining the integrity of the communication channel.

To evaluate the system's performance, metrics such as key utilization efficiency, encryption time, and decryption time are analyzed. The simulation demonstrates how efficiently the QKD key is utilized for encrypting and decrypting the data, offering insights into the practical feasibility of implementing such protocols in real-world quantum communication systems.

This proposed work aims to provide a foundational framework for secure quantum communication, emphasizing multi-node environments where security and efficiency are critical. The integration of QKD with QSS offers a novel approach to addressing the challenges of secure data sharing in modern network. The proposed system incorporates a modular and scalable design, enabling adaptability to various network sizes and configurations. By supporting multiple nodes, the approach ensures that the secret can be distributed among several participants, making it ideal for applications such as distributed computing, secure voting systems, and multi-party transactions. The modular framework also allows the integration of advanced quantum techniques and error correction mechanisms in future iterations.

V. RESULTS AND DISCUSSION

The output provides a detailed view of the Quantum Key Distribution (QKD) process, which involves encrypting and decrypting data using quantum states. Here's an explanation of the key components in the output:

1. Generated QKD Key (Binary):

This is the binary sequence generated as part of the quantum key exchange process. Each bit in the binary sequence corresponds to a specific quantum state (0 or 1). These bits are used for encryption and decryption in the QKD protocol.

Figure 3 : QKD Key Generation

2. Encoded States:

These represent the quantum states of the qubits encoded with phase shifts (represented in radians). The encoded states are generated using the QKD key and are used for transmitting the encrypted data.

Each tuple consists of:

- The bit value (0 or 1) of the encoded bit.
- The phase shift associated with that bit (the second value in the tuple).
- A list of phase shifts that encode the data for multiple qubits (the third value in the tuple).

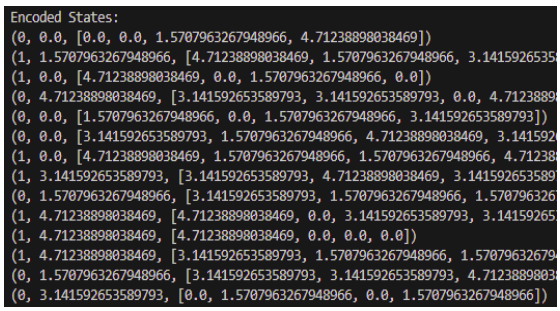

Figure 4 : Encoded States

3. Reconstructed Data:

This is the final step of decryption, where the originally encrypted data (crypto) is reconstructed after being transmitted and decoded using the quantum states. The reconstructed data should match the original input data if the decryption process was successful.

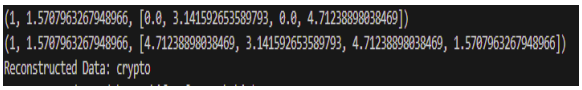

Figure 5 : Reconstructed Data

4. Reconstructed Key (Phase Shifts for Each Bit):

The reconstructed key consists of the phase shifts for each bit of the QKD key, which were used for the encryption. These phase shifts were initially applied to the qubits during the encoding process.This key is then used to decode the quantum data and retrieve the original plaintext message.

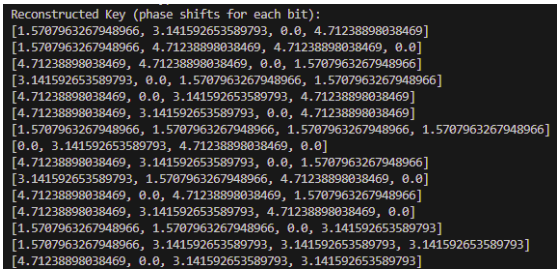

Figure 6 : Reconstructed Key

5. Key Efficiency Metrics:

The key efficiency metrics for the system reveal that the key length is significantly larger than the number of bits used for encryption, leading to a relatively low key utilization efficiency. The system efficiently employs a small portion of the key for encryption and decryption processes, while the key generation time is almost instantaneous, showcasing a rapid key generation capability.

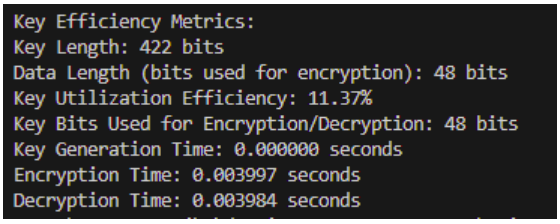

Figure 7 : Key Efficiency Metrics

VI. FUTURE WORK

Future work for this project will focus on improving the system to work well in real-life situations. Right now, the system assumes that everything is perfect, but in reality, noise and errors in hardware can cause problems. So, more work is needed to create better ways to fix these errors and improve the system's reliability. The hardware used in quantum communication also needs to be better, especially for long-distance communication, to make it more accurate and efficient. In addition, the system needs to be able to handle bigger networks with many nodes, which is important for using it in global communication. Making the system use less energy and work together with current communication technologies will make it more practical. As quantum computers become stronger, the system should also include quantum-resistant algorithms to keep the communication safe for a long time. Even though this project is based on simulations, testing it in real-world conditions is crucial to see how it performs in practice. Lastly, as the system grows, more research is needed to protect it from smart eavesdroppers and other advanced attacks. Future work could also look at improving the speed of the system, making it easier to use in different environments, and ensuring it can handle different types of data securely.

VII. CONCLUSION

This project highlights that combining Quantum Key Distribution (QKD) with Quantum Secret Sharing (QSS) is an effective and secure approach for distributing secret keys across multiple parties. The system leverages quantum mechanics to generate and distribute keys that are subsequently used for encrypting and decrypting sensitive information, ensuring the confidentiality and integrity of data. Intermediate nodes play a crucial role in securing the communication process by introducing random phase shifts to the quantum states. This added layer of complexity makes it extremely challenging for unauthorized individuals to intercept or manipulate the keys. The encrypted data remains protected, and decryption is only possible when the correct group of nodes collaborates to reconstruct the original key.

Simulation results show that this method is scalable and efficient, handling complex networks with numerous nodes without compromising performance. By enabling secure encryption and decryption processes, the integration of QKD and QSS provides a reliable framework for building advanced and secure communication systems for the future.

VIII. REFERENCES

[1]. O. Shirko and S. Askar, "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking," in *IEEE Access*, vol. 11, pp. 21641-21654, 2023, doi: 10.1109/ACCESS.2023.3251649.

[2]. P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," in *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2049-2083, 2021, doi: 10.1109/OJCOMS.2021.3106659.

[3]. D. Rathi, S. Kumar and R. Grover, "Multi-dimensional Quantum Secret Sharing Scheme with Noisy Environment," 2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS), KOTTAYAM, India, 2023, pp. 1-6.

[4]. S. M. Barnett and S. J. D. Phoenix, "Securing a quantum key distribution relay network using secret sharing," 2011 IEEE GCC Conference and Exhibition (GCC), Dubai, United Arab Emirates, 2011, pp. 143-145.

[5]. F. Li, T. Chen, M. Li and C. Lin, "Efficient and Verifiable General Quantum Secret Sharing Based on Special Entangled State," in IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14127-14135, 15 April15, 2024.

[6]. P. -Y. Kong, "A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security," in IEEE Systems Journal, vol. 16, no. 1, pp. 41-54, March 2022.

[7]. P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2049-2083, 2021.

[8]. L. Yanyan and X. Chengqian, "Three-Party Quantum Secret Sharing Based on Secure Direct Communication," 2009 International Forum on Information Technology and Applications, Chengdu, China, 2009, pp. 126-130.

[9]. L. Noirie, "From Existing Quantum Key Distribution Systems Towards Future Quantum Networks," 2024 13th International Conference on Communications, Circuits and Systems (ICCCAS), Xiamen, China, 2024, pp. 339-344.

[10]. M. Harmalkar, K. Jain, K. B. Aneesh Kumar and P. Krishnan, "Quantum Secure Key Management & Delivery Protocol in the QKD framework," 2024 IEEE 5th India Council International Subsections Conference (INDISCON), Chandigarh, India, 2024, pp. 1-6.