Quantum Secure Direct Communication Simulation

Group Members: Mahad Munir (21k-3388), Rafed Naeem (21k-3385)

A Quantum Cryptography Approach using Qiskit and Simulated Eavesdropping

Abstract

This project simulates Quantum Secure Direct Communication (QSDC) using Qiskit. Classical messages are encoded into quantum states for secure transmission. Eavesdropping is detected through qubit measurement discrepancies, showcasing the reliability of quantum cryptography for secure data exchange.

Objectives

- Simulate Quantum Secure Direct Communication (QSDC) to ensure secure communication between parties, leveraging quantum entanglement and quantum key distribution for encryption.
- Detect eavesdropping through quantum measurement discrepancies, analyzing how the presence of an eavesdropper affects the integrity of transmitted quantum states.
- Test and analyze Qiskit simulations for quantum circuits, including performing multiple iterations to evaluate performance, detect errors, and optimize the protocols used in QSDC.

Methodology

- **Quantum Circuit Design:** Encode messages with Hadamard and X gates.
- **Eavesdropping Simulation:** Introduce measurements on qubits by eavesdropper.
- **Error Detection:** Compare received qubits with originals.
- **Qiskit Simulations:** Perform end-to-end testing.

Results

- Secure message transmission achieved without eavesdropping.
- Eavesdropping creates measurable errors in qubits.
- High success rate in detecting quantum interference.

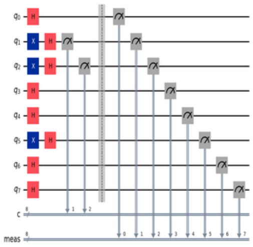

Figure 1: Evesdropping detected

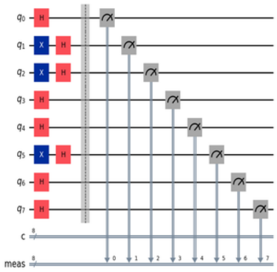

Figure 2: No Evesdropping detected

Conclusion

- QSDC ensures message integrity by detecting eavesdropping attempts.
- Future improvements: Real quantum hardware testing and advanced error-correction techniques.

Recommendations

- Integrate QSDC into real-world quantum networks.
- Explore hybrid quantum-classical communication systems.

Presented by: Mahad Munir (21k-3388) and Rafed Naeem (21k-3385)