TeleQ – A Quantum Teleportation Demonstration

Prepared by **Saurabh Suman**
Department of Electronics and Telecommunication Engineering
Jabalpur Engineering College

Abstract

The project "TeleQ" seeks to showcase the potential for secure communication using quantum teleportation. This innovative approach involves the direct transfer of quantum states, moving away from traditional encryption methods or key-based quantum key distribution (QKD). By utilizing principles of quantum mechanics like entanglement and the no-cloning theorem, TeleQ offers robust security against eavesdropping. This proposal details the theoretical framework, methodology, and societal implications of TeleQ. Although the implementation is currently simulated due to hardware constraints, this project lays the groundwork for future large-scale quantum communication systems. Anticipated outcomes include a deeper understanding of quantum communication and its scalability for practical applications.

Introduction

Background

Quantum computing is making significant strides, with quantum processors such as Google's Willow and IBM's quantum systems not only increasing their qubit counts but also minimizing errors. These advancements bring us closer to a time when quantum computers could potentially compromise traditional encryption methods like RSA and ECC through algorithms like Shor's.

Current solution, including Quantum Key Distribution (QKD), still depend on classical encryption (although using quantum techniques), which leaves them open to certain vulnerabilities. TeleQ presents a forward-thinking alternative by utilizing quantum teleportation to transfer quantum states directly, thereby removing the necessity for cryptographic keys. This initiative showcases the potential for secure and scalable quantum communication, paving the way for a post-quantum era.

Problem Statement

Modern communication systems are becoming more susceptible to sophisticated cyberattacks, and the future development of quantum computers could threaten their security. Current quantum communication techniques, such as Quantum Key Distribution (QKD), also struggle with issues related to scalability and complexity. This project seeks to showcase a secure, scalable, and efficient alternative through the use of quantum teleportation.

Objectives

- To demonstrate the feasibility of quantum teleportation for secure communication.
- To identify advantages of TeleQ over classical encryption and QKD.
- To provide a conceptual roadmap for real-world scalability of TeleQ.

Review and Gap Analysis

Current Research

1. **QKD:** A widely researched protocol for secure key distribution. However, it requires substantial resources and still depends on classical encryption.
2. **Classical Encryption:** Vulnerable to quantum algorithms like Shor's algorithm.
3. **Quantum Teleportation:** Successfully demonstrated in experiments, such as China's satellite-based teleportation and metropolitan fiber networks.

Identified Gaps

- Dependency on pre-shared keys in QKD introduces vulnerabilities.
- Scalability issues with QKD due to resource demands.
- Complexity in detecting eavesdropping in QKD increases latency.

How TeleQ Addresses These Gaps

TeleQ eliminates the need for keys, scales efficiently with data size, and integrates eavesdropping detection directly into its process through entanglement disturbance monitoring and randomization of carrier entangled qubits.

Methodology

Theoretical Background

Key Concepts:

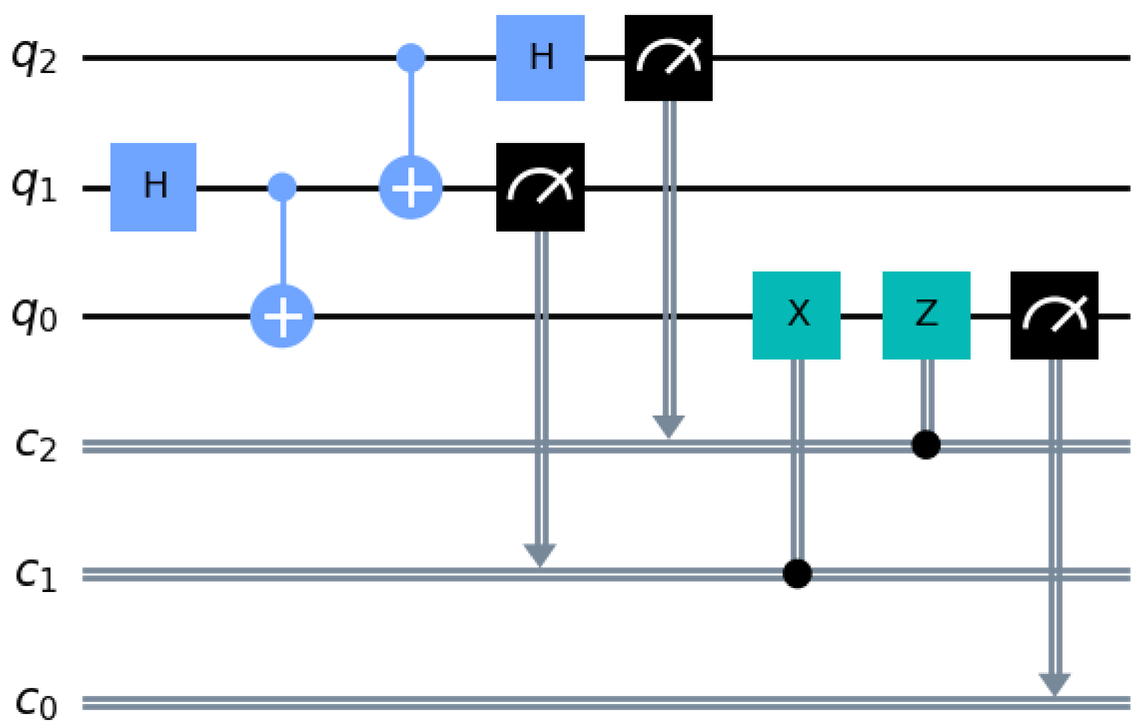
- **Entanglement:** A phenomenon where particles share a quantum state, ensuring a strong correlation between them irrespective of distance.
- **Superposition:** A fundamental property of quantum mechanics where particles exist in multiple states simultaneously until measured.
- **No-Cloning Theorem:** A principle stating that it is impossible to create an exact copy of an arbitrary quantum state, ensuring inherent security.
- **Collapse Due to Measurement:** A phenomenon where the act of measuring a quantum state forces it into a definite state, disrupting entanglement if tampered with.

- **Quantum Information:** Encodes classical information into qubits using quantum states ($|0\rangle$ and $|1\rangle$).
- **Bell States:** Four maximally entangled states used in quantum teleportation and several other quantum computing applications:
  - $|\boldsymbol{\Phi}^{+}\rangle = \frac{1}{\sqrt{2}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle)$
  - $|\boldsymbol{\Phi}^{-}\rangle = \frac{1}{\sqrt{2}}(|\mathbf{00}\rangle - |\mathbf{11}\rangle)$
  - $|\boldsymbol{\Psi}^{+}\rangle = \frac{1}{\sqrt{2}}(|\mathbf{01}\rangle + |\mathbf{10}\rangle)$
  - $|\boldsymbol{\Psi}^{-}\rangle = \frac{1}{\sqrt{2}}(|\mathbf{01}\rangle - |\mathbf{10}\rangle)$

Quantum Teleportation Theory

Quantum teleportation transfers a quantum state ($|\Psi\rangle = a|0\rangle + b|1\rangle$) from one location to another using shared entanglement and classical communication. Steps include:

1. **Entanglement Creation:** A pair of entangled qubits is shared between the sender and receiver.
2. **Measurement:** Sender measures their entangled qubit and the qubit holding ($|\Psi\rangle$), collapsing them into a specific state.
3. **Classical Communication:** Sender sends the results of their measurement (two classical bits) to the receiver.
4. **State Reconstruction:** Receiver applies correction based on the sender's classical bits to recreate ($|\Psi\rangle$).



Above is a sample teleportation circuit where q_2 is the message qubit, while q_1 and q_0

are the qubits forming the entangled Bell state $|\Phi^+\rangle$. Here, c_2, c_1 and c_0 are classical bits carrying the measured information at different stages.

Implementation of TeleQ

1. **Data Conversion:** Input data is converted into binary format, where each character is represented as 8-bit ASCII.
2. **Entanglement Generation:** Entangled qubits are prepared for teleportation by randomly choosing one out of four Bell states.
3. **Bit-by-Bit Teleportation:** Each bit is teleported individually using the steps of quantum teleportation.
4. **Classical Bit Transfer:** Correction bit (c_1, c_2) are sent over classical channels.
5. **Reconstruction:** The receiver reconstructs the original binary data and converts it back to the message format.

Probability of Eavesdropping

To reconstruct one bit, an eavesdropper must correctly identify the Bell state ($\frac{1}{4}$ chance) and intercept the classical correction bits. For a byte (8 bits):

$$P_{correct} = \left(\frac{1}{4}\right)^8 = \frac{1}{65{,}536} \approx 0.0015\%$$

This probability is for one single byte. As more information is transferred, the probability of correctly guessing the upcoming byte **decreases exponentially**, making eavesdropping virtually impossible.

Feasibility and Scalability

Feasibility with Current Technology

The project is highly feasible with current technologies in photonic qubits and fiber-optic networks. Quantum teleportation has already been demonstrated in laboratories, and photonic qubits can travel long distances through optical fibers or satellite links. The main challenges are attenuation and noise, which can be addressed using quantum repeaters, error correction, and advanced detectors. While more technical advancements are required, we have sufficient technology to start implementing the project in pilot phases.

Scalability for Large-Scale Communication

TeleQ scales efficiently with data size due to its linear resource requirement (one entangled pair per bit). By leveraging quantum repeaters, the ranger can be extended without compromising qubit fidelity. Integration with existing fiber-optic infrastructure via wavelength-division multiplexing (WDM) allows quantum signals to coexist with classical data, minimizing deployment costs. Satellite-based communication further enhances scalability, enabling intercontinental connections.

Results and Analysis

Advantages of TeleQ

In the following table, different features of Classical Encryption, Quantum Key Distribution (QKD), and TeleQ are compared. Wherever a feature is desirable, it is marked in green; if undesirable, then in red, and if normal, then in blue.

Feature	Classical Encryption	QKD	TeleQ
Dependency on Keys for Safety	Yes	Yes	No
Vulnerable to Quantum Computers	Yes	No	No
Eavesdropping Detection	No	Yes	Yes
Scalability	High	Limited	High
Complexity	Low	High	Moderate

In the above table, we can see that on most parameters, TeleQ performs well.

Simulation-Based Demonstration

- **Purpose:** The simulation only demonstrates the core idea of TeleQ due to limitations in quantum hardware availability. Since simulators only work on local systems, both sending and receiving of the messages were done on the same device. On real quantum devices with available quantum channels, this will not be a problem.
- **Scope:** Simplifies the process for conceptual understanding, with future potential for real-world application with required optimizations and adjustments.

Significance and Societal Impact

- **Future-Proof Security:** Protects against quantum threats to classical encryption.
- **Applications:** National security, finance, healthcare, and secure personal communication.
- **Alignment with the National Quantum Mission:** Directly supports India's goals to develop secure quantum communication infrastructure.

References

1. **Quantum Teleportation Theory:** Provides a foundational overview of the theoretical framework and principles of quantum teleportation. https://en.wikipedia.org/wiki/Quantum_teleportation
2. **National Quantum Mission (India):** Discusses India's initiatives to establish quantum communication networks as part of its National Quantum Mission. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2083199

3. **Metropolitan Quantum Teleportation:** Highlights quantum teleportation at a rate of 7.1 Hz over metropolitan fiber networks, showcasing scalability for urban infrastructure.
   https://www.nature.com/articles/s41377-023-01158-7
4. **China's Satellite-Based Teleportation:** Describes a groundbreaking experiment demonstrating quantum teleportation over 1,400 km using the Micius satellite.
   https://www.nature.com/articles/nature23675
5. **A Simple Demonstration of TeleQ using Simulators:** Using Python programming language and Qiskit framework, this program effectively demonstrates the basic idea behind the working of TeleQ.
   https://github.com/saurabhyahihai/TeleQ

Appendices

1. **Quantum Repeaters:** Devices extending quantum communication range through entanglement swapping and error correction, ensuring low loss over long distances.
2. **Quantum Error Correction:** Detects and errors in quantum states caused by decoherence or noise, critical for maintaining fidelity in communication.
3. **Wavelength-Division Multiplexing (WDM):** Combines multiple signals on a single fiber using different wavelengths, allowing quantum and classical signals to coexist.