ECONOMIC KEYLESS SEMI-QUANTUM POINT-TO-POINT COMMUNICATION (EKSQPC)

Kripa Adhikari | Sara Shajari

COMP4900 A

February 24, 2025

INTRODUCTION

- Quantum computers threaten traditional encryption systems (e.g., RSA).
- Full quantum security is difficult to implement on portable devices.
- Semi-Quantum Communication (SQC) allows secure communication using simpler quantum capabilities.
- EKSQPC offers a lightweight and efficient solution for secure quantum communication.

BACKGROUND – QUANTUM & SEMI-QUANTUM COMMUNICATION

Quantum Key Distribution (QKD)

enables secure communication but **requires full quantum devices**.

Semi-Quantum Communication (SQC)

allows **one party to use a classical device** while still ensuring security.

EKSQPC

overcomes these limitations with a more efficient approach.

Previous SQC protocols

- **Low efficiency** (many qubits wasted).
- **Long entanglement holding time** (impractical in real-world use).

PROPOSED SOLUTION – EKSQPC & REKSQPC

EKSQPC reduces **entanglement preservation time** and **hardware complexity**

Uses **Tele-Fetch** operation to **extract information without direct transmission**.

Implements **Measure and Replay Attack Detection (MRAD)** to detect attackers.

REKSQPC improves security by considering **real-world noise and disturbances**.

STEP 1 — **Create entangled EPR pairs.**

STEP 2 — **Simulate Bob’s choices:** measure or reflect qubits.

STEP 3 — **Implement Tele-Fetch operation.**

STEP 4 — **Implement Measure and Replay Attack Detection (MRAD).**

IMPLEMENTATION PLAN (MATLAB)

EXPECTED RESULTS & CHALLENGES

Results

- Secure **quantum message transmission** using EKSQPC.
- **Detect hacking attempts** using MRAD.
- **High qubit efficiency** (approaching **100%**).

Challenges

- **Simulating quantum behavior** in MATLAB.
- **Understanding and implementing Bell measurements**.
- **Handling real-world noise** in REKSQPC.

MARCH 1 -7

Research & Initial Set up

- Finalize research on **Tele-Fetch (TF), MRAD, and Bell Measurements**.
- Set up **MATLAB** and install necessary quantum simulation libraries.
- Define the **project structure** and initial code framework.

MARCH 8 - 14

Implement Core Functions (EKSQPC)

- Implement **EPR pair generation** and **Bell measurements** in MATLAB.
- Implement **Bob's measurement/reflection process**.
- Implement **Tele-Fetch (TF) function** to infer Bob's results.

MARCH 15 - 21

Implement REKSQPC & Attack Simulations

- Introduce **probing bits** and simulate **Measure and Replay Attack (MRA)**.
- Implement **MRAD (MRA Detection)** in MATLAB.
- Extend **EKSQPC to REKSQPC**, adding **statistical estimation** for noise (optional).

MARCH 22 - 31

Testing, Optimization & Final Report

- Run **full-scale testing** with multiple message transmissions.
- Optimize **qubit efficiency & reduce runtime issues**.
- Document **results, challenges, and improvements**.

EXECUTION PLAN

ALIGNMENT

- **EKSQPC and REKSQPC** provide an **efficient and secure approach** to **semi-quantum communication**.
- Our project will **implement and test these protocols in MATLAB**.
- The findings will **demonstrate feasibility and security**.
- Future work could explore **hardware implementations** for real-world use.

REFERENCES

Lu, H., Barbeau, M., & Nayak, A. (2019, January 11). *Keyless semi-quantum point-to-point communication protocol with low resource requirements*. Nature News. https://www.nature.com/articles/s41598-018-37045-0