Research Plan: Cryptography in Counterfactual Communication in Photonics Setup

Project Title:
Cryptography in Counterfactual Communication Using Photonic Setups Based on Sohail Zubairy's Protocol

Duration: 6 Weeks
Intern Level: Undergraduate/early postgraduate with basic quantum mechanics background

---

Objective:

To study, simulate, and analyze counterfactual quantum communication protocols, particularly focusing on their cryptographic applications. Interns will use photonics-based setups inspired by the Zubairy-Salih 2013 protocol to explore secure transmission of information without the physical travel of photons.

Week-by-Week Plan

Week 1: Background Study & Conceptual Foundation

- **Goal:** Understand the physical principles behind counterfactual communication.
- **Activities:**
  - Read and review key literature:
    - Salih et al., "Protocol for Direct Counterfactual Quantum Communication" (PRL, 2013)
    - Concepts of interaction-free measurements (Elitzur–Vaidman bomb tester)
    - No-cloning theorem and quantum Zeno effect
  - Discuss basic beam splitter operations, single-photon interference, and nested Mach-Zehnder Interferometers.
- **Deliverable:** Summary report on principles of counterfactual communication and its differences from standard quantum communication.

Week 2: Understanding the Suhail Zubairy Protocol

- **Goal:** Break down the architecture of the Zubairy setup.
- **Activities:**
  - Analyze and draw the setup (nested interferometers, photon source, detectors)
  - Understand the role of Alice and Bob in this setup
  - Simulate basic beam splitter behavior using Python/Qiskit/Strawberry Fields
- **Deliverable:** Visual flow of the protocol and logic table of photon detection outcomes.

Week 3: Coding & Simulation – Base Interferometer

- **Goal:** Create and simulate a simplified Mach-Zehnder interferometer.
- **Activities:**
  - Build simulation of single-photon interferometry
  - Add absorbers/obstacles in Bob's path to test interaction-free detection
  - Validate simulation results with theoretical expectations
- **Deliverable:** Working simulation of the basic MZI setup and interference patterns.

Week 4: Expanding to Nested Interferometers

- **Goal:** Simulate the full counterfactual setup from the Zubairy protocol.
- **Activities:**
  - Implement outer and inner loops (nested MZIs)
  - Test logical information transfer (bit 0 and bit 1) based on Bob's block/no-block actions
  - Identify critical parameters: number of beam splitters, visibility, probability of error
- **Deliverable:** Functional nested interferometer simulating counterfactual transmission of bits.

Week 5: Cryptographic Application

- **Goal:** Apply the protocol to quantum key distribution (QKD).
- **Activities:**
    - Study BB84 briefly, then contrast with counterfactual QKD proposals
    - Introduce eavesdropper (Eve) in simulation; analyze detection and disturbance
    - Evaluate protocol security: Does Eve gain information? Is detection possible?
- **Deliverable:** Preliminary results on security features of counterfactual QKD.

Week 6: Finalization and Reporting

- **Goal:** Document findings and propose improvements or extensions.
- **Activities:**
    - Prepare final report and presentation
    - Suggest next steps (e.g., multi-photon counterfactual QKD, entanglement-enhanced variants)
    - Discuss limitations and practical implementation challenges (detector efficiency, decoherence)
- **Deliverable:** Final presentation and report including simulation codes, graphs, and potential real-world outlook.

Tools & Resources

- **Coding Tools:** Python with Qiskit, Strawberry Fields, or QuTiP
- **Reference Papers:**
    - Salih, Zubairy et al., PRL 2013
    - Elitzur–Vaidman Bomb Tester (1993)
    - Counterfactual QKD proposals (e.g., Noh's protocol)

Future Work

- Extension to entangled-state counterfactual setups
- Explore machine learning optimization of beam splitter configurations
- Build noise-tolerant or error-corrected versions of the protocol
- Compare practical implementability on quantum photonic chips (e.g., Xanadu hardware)