Entanglement-Based QKD: Simulation of the E91 Protocol with Bell Inequality Verification, provide a brief overview

Investigators:

- ➔ Deep Amit Lodaya - [CB.AI.U4AID23004]
- ➔ Pranav Sivakumar - [CB.AI.U4AID23028]
- ➔ R Ashwin - [CB.AI.U4AID23029]
- ➔ SS Rithesh - [CB.AI.U4AID23031]

Summary:

The E91 protocol is an entanglement-based quantum key distribution (QKD) scheme that uses pairs of entangled photons to establish a secure key between two parties. Unlike prepare-and-measure protocols like BB84, E91 relies on the quantum correlations of entangled particles and tests for violations of Bell's inequality to ensure security. In a simulation of the E91 protocol, entangled photon pairs are generated and measured at different angles chosen randomly by the two parties. A subset of the measurement outcomes is used to calculate the CHSH (Clauser-Horne-Shimony-Holt) inequality, and a statistically significant violation confirms the presence of genuine quantum entanglement, ruling out local hidden variable theories and potential eavesdropping. The remaining correlated measurement results are then processed to generate a shared secret key. This simulation not only demonstrates secure quantum communication but also reinforces the fundamental principles of quantum entanglement and non-locality.

Background and Motivation

Quantum key distribution (QKD) aims to enable two parties to securely share cryptographic keys using the principles of quantum mechanics, ensuring security even against adversaries with unlimited computational power. Traditional QKD protocols like BB84 rely on the no-cloning theorem and measurement-induced disturbance to detect eavesdropping. However, the E91 protocol, introduced by Artur Ekert in 1991, takes a fundamentally different approach by utilizing entangled quantum states and the violation of Bell's inequality to guarantee security. The use of entanglement not only strengthens the theoretical foundation of QKD but also connects it deeply with the foundational questions of quantum physics, such as non-locality and realism. The motivation for simulating the E91 protocol lies in its ability to provide a practical and visual understanding of how quantum entanglement can be exploited for secure communication, and how Bell inequality violations can serve as a robust test against eavesdropping. It also paves the way for studying future device-independent QKD schemes that can operate even when the devices themselves are untrusted.

Problem Statement

While quantum key distribution protocols like BB84 have been widely studied and implemented, they depend on the trustworthiness of the quantum devices used. The E91 protocol offers a more robust approach by leveraging quantum entanglement and Bell inequality violations to detect eavesdropping, potentially enabling **device-independent security**. However, understanding and validating the security of E91 in practice requires careful simulation of entangled state generation, measurement, and statistical analysis of quantum correlations. The problem is to **simulate the E91 protocol**, generate entangled photon pairs, perform measurements at various angles for two parties, compute the CHSH Bell inequality parameter, and verify its violation. This will demonstrate how entanglement-based QKD ensures security and highlight the practical feasibility and limitations of using Bell tests for secure quantum communication.

Objectives

- ➔ Simulate the E91 protocol using entangled photon pairs and perform measurements with randomly chosen bases.
- ➔ Compute and verify the violation of the CHSH Bell inequality to confirm the presence of entanglement and detect potential eavesdropping.
- ➔ Extract a secure key from the correlated outcomes and analyze its reliability under ideal and noisy conditions.

Methodology

The simulation begins by generating entangled photon pairs in a maximally entangled Bell state, such as the singlet state. These entangled qubits are distributed between two simulated parties, Alice and Bob. Each party randomly selects one of three predefined measurement angles to simulate realistic quantum measurements. Using these measurements, outcomes are recorded for many entangled pairs. A subset of the results is used to calculate correlation coefficients and evaluate the CHSH Bell inequality expression. If the inequality is violated (i.e., the CHSH value exceeds 2), it confirms the presence of quantum entanglement and rules out eavesdropping based on local hidden variable theories. The remaining outcomes, which are strongly correlated due to entanglement, are then processed to extract a shared key using classical post-processing techniques like error correction and privacy amplification. Optionally, noise can be introduced into the simulation to analyze the robustness and practical limitations of the protocol.

Expected Outcomes

- ➔ Successful violation of the CHSH Bell inequality, confirming the presence of quantum entanglement and enabling secure key distribution.
- ➔ Generation of a shared secret key between Alice and Bob from correlated measurement outcomes.
- ➔ Insight into how noise and measurement errors affect the reliability and security of the E91 protocol.

Timeline

- ➔ **Month 1:** Conduct in-depth research on the E91 protocol, CHSH inequality, and quantum entanglement; set up the simulation environment and implement entangled state generation.
- ➔ **Month 2:** Develop the full simulation including random measurements, CHSH inequality calculation, and verification of Bell violation.
- ➔ **Month 3:** Implement key extraction with post-processing, test the protocol under ideal and noisy conditions, and finalize documentation and presentation.

Required resources

- ➔ Python (with NumPy and Matplotlib)
- ➔ Qiskit (for quantum simulation)

References

- ➔ Ekert, A. K. (1991). *Quantum cryptography based on Bell's theorem*. Physical Review Letters, 67(6), 661–663.
- ➔ Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.