E91 QKD protocol

Minjae Cho, Elijah Olive, Brian Bahk

Original BB84 QKD protocol

- Developed by Charles Bennett and Gilles Brassard in 1984
- Stands for Quantum Key Distribution protocol
- Models a scenario where two people named Alice and Bob wish to send bit information to each other using keys of polarized light
    - Alice generates a string of “secret keys” which after being put through a basis, are sent to Bob for him to use a basis to create inferred keys. These two sets of keys are then compared to create a list of sifted keys
- Sometimes, a third party eavesdropper “Eve” would interfere and eavesdrop on Alice’s bit stream in an attempt to know what message Alice is trying to send to Bob

New E91 QKD protocol

- Proposed by: Artur Ekert, 1991
- Key Mechanism: Utilizes Bell states (SPDC) for maximal entanglement of two qubits, shared between Alice and Bob (specifically Psi-).
- Process:
  - Alice and Bob independently choose random polarization bases to measure their respective photons.
  - Both parties interpret the states to form an identical key.
- Security Check:
  - Detection of eavesdropping is possible through disruption of entanglement; if an eavesdropper intercepts and resends photons, the original entanglement is lost.
  - Alice and Bob verify security by testing violations of Bell's inequalities, indicating no eavesdropper interference.

Our QKD simulator

We adapted the original BB84 protocol to create an E91 simulator. Using Qiskit, we implemented entanglement with the Bell State $|\Psi^-\rangle$, which links the state of two photons. When one photon is measured, the state of its entangled partner is instantaneously affected due to quantum entanglement.

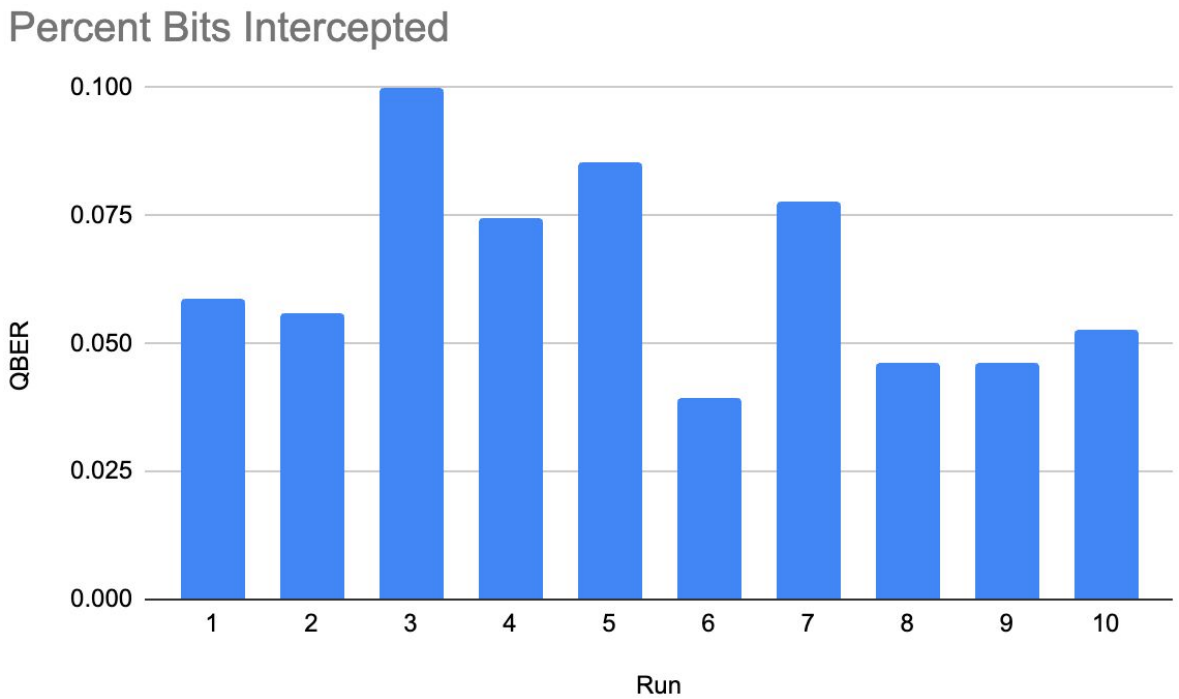
In this setup:

- Alice measures one of the entangled photons with her random basis.
- Unlike BB84, where Alice sends a randomly chosen key bit, in E91, Alice’s measurement automatically determines the state of Bob’s entangled photon due to the collapse of the entangled state. This collapse ensures that Bob’s photon directly correlates with Alice's measurement, maintaining their shared entanglement unless interfered with by an eavesdropper.
- Two different setups—one with and one without dark counts

Benefits of E91 over BB84

- Like we talked about in BB84, if multiple of same state photons are sent and eve can somehow split it to measure one while sending another, there may be security risk.
- For E91, there are two qubit states entangled instead of one in BB84, and when paired with Bell's inequality, it is more likely to detect Eve
    - Believed it was out of scope as another project is entirely based on this; instead implemented more naive and simple version of Eve
- E91 does not use randomly generated padding, but instead use inherent randomness of entangled states, which also removes possible security risk

QBER Across Trials w/ eve & w/out dark counts



Bell Inequality (ex. CHSH)

$$|\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle| \leq 2 \,.$$

Sum of avg. of bob alice terms following classical should be less than equal to^^

$$|S| = 2\sqrt{2}.$$

Maximally entangled states give ^^

- Eve Detection method
- Models classical physics, hidden variables affect events
  - If variables proven not to exist, weird quantum effect must be happening(entanglement)
- After sharing measurement basis (rectilinear/diagonal) use subset of matching basis to check for correlation
  - Checks whether bits are still entangled or not
  - Breaking this correlation means entanglement ergo no listener Eve

```
def calculate_correlations(self, shots=1000):
  settings = [('H', 'V'), ('H', 'D'), ('D', 'V'), ('D', 'D')]
  results = {setting: 0 for setting in settings}
  for _ in range(shots):
    for setting in settings:
        results[setting] += self.bell_measurement(*setting)
  return results
```

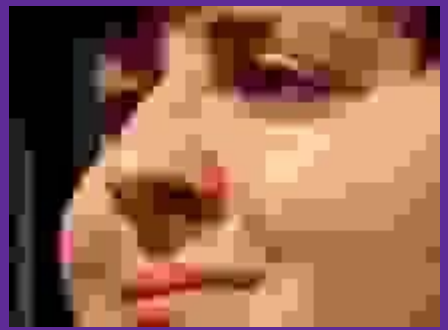
Highlights and Issues

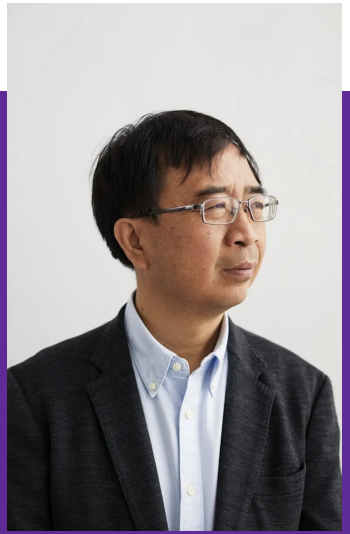
BB84	E91
• Alice sends polarized state directly to Bob • Employed an allowable error rate of 15%, which was effective for catching eavesdroppers • Much Easier to implement	• Uses entangled states, meaning no polarized state needs to be sent directly, although each entangled state has to be shared • If an eavesdropper were to measure them, Alice would know immediately because the photon being sent to her would lose its entanglement to the photon being sent to Bob • Efficiency of Entangling Photons very difficult (SPDC)

Both

- Alice and Bob share measurement bases, the photons bits can then be used as a one-time key
- The programs simulate protons in a perfect, error free world. In reality, errors could occur due to randomness unassociated with Eve

Questions?





Sources used:

https://mpl.mpg.de/fileadmin/user_upload/Chekhova_Research_Group/Lecture_4_12.pdf

https://youtu.be/V3WzH2up7Os?si=wiOwvdZZGbKn9QiO