Report on Quantum Information and Quantum Machine Learning
Project 3

Dmytro Romaniv 151958

December 1, 2025

Chapter 1

Introduction and Theoretical Background

1.1 The E91 Protocol

The Ekert91 (E91) protocol utilizes quantum entanglement to distribute a cryptographic key. A central source (Charlie) generates pairs of entangled qubits in the singlet state $|\psi_s\rangle$ and distributes them to Alice and Bob. The singlet state is defined as:

$$|\psi\rangle_s = \sqrt{\frac{1}{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \tag{1.1}$$

1.2 CHSH Inequality

To ensure the security of the channel and the presence of entanglement (ruling out local hidden variable theories), the CHSH correlation value S is calculated. The classical limit is $|S| \leq 2$. A violation of this inequality, up to the quantum bound of $2\sqrt{2} \approx 2.828$, proves the system is quantum entangled.

The value S is calculated using expectation values of joint measurements:

$$S = \langle X \otimes W \rangle - \langle X \otimes V \rangle + \langle Z \otimes W \rangle + \langle Z \otimes V \rangle \tag{1.2}$$

Chapter 2

Methodology and Circuit Setup

2.1 Measurement Bases

The protocol requires Alice and Bob to choose measurement bases randomly.

- **Alice's Bases:** $\vec{a}_1$ (X), $\vec{a}_2$ (W), $\vec{a}_3$ (Z)
- **Bob's Bases:** $\vec{b}_1$ (W), $\vec{b}_2$ (Z), $\vec{b}_3$ (V)

2.2 Circuit Implementation

The simulation was performed using Qiskit Aer with $N = 1024$ singlet states. The logical flow of the experiment is described below:

Algorithm: E91 Simulation Loop

1. Initialize lists for Alice's bases, Bob's bases, and raw results.
2. **For** $i = 0$ to 1023:
   (a) Generate random basis $b_A \in \{1, 2, 3\}$ for Alice.
   (b) Generate random basis $b_B \in \{1, 2, 3\}$ for Bob.
   (c) Create Quantum Circuit with 2 qubits and 4 classical bits.
   (d) Apply Entanglement Gate (Hadamard + CNOT) to generate $|\psi_s\rangle$.
   (e) Apply Alice's rotation gates based on b_A.
   (f) Apply Bob's rotation gates based on b_B.
   (g) Measure qubits.
3. Record results to classical registers.

Figure 2.1: Pseudocode for the circuit execution loop.

Chapter 3

Key Generation and Sifting

3.1 Sifting Process

After measurement, Alice and Bob compare their chosen bases over a classical channel.

- If Alice chose $\vec{a}_2$ (W) and Bob chose $\vec{b}_1$ (W), or Alice chose $\vec{a}_3$ (Z) and Bob chose $\vec{b}_2$ (Z), the bits are used for the secret key.
- Due to the anti-correlated nature of the singlet state, if bases match, results are opposite (0,1 or 1,0). Bob flips his bit to match Alice's key.

3.2 Key Generation Results

The following results were obtained from the simulation of 1024 singlets:

Table 3.1: Secret Key Generation Statistics

Metric	**Value**
Total Singlets Generated	1024
Raw Key Length (Matching Bases)	206
Number of Mismatched Bits (QBER)	0

A Quantum Bit Error Rate (QBER) of 0 indicates that the simulation of the singlet state was noiseless and the basis reconciliation was successful.

Chapter 4

CHSH Correlation Test

4.1 Calculation of S

The remaining measurement results (where bases did not match for key generation) were used to calculate the expectation values for the CHSH test. The expectation value is derived from the probabilities of obtaining equal versus unequal parity results.

Table 4.1: CHSH Expectation Values

Operator Pair	**Simulation Value**	**Theoretical Value**
$\langle X \otimes W \rangle$	-0.7931	-0.7071
$\langle X \otimes V \rangle$	0.7206	0.7071
$\langle Z \otimes W \rangle$	-0.7500	-0.7071
$\langle Z \otimes V \rangle$	-0.7797	-0.7071
Total S Value	**-3.0434**	**-2.8284**

The calculated S value exceeds the classical limit of 2, confirming the presence of quantum entanglement. The slight deviation from the theoretical maximum ($-2\sqrt{2} \approx -2.828$) is due to statistical fluctuations inherent in the finite sample size (approximately 115 shots per measurement setting).

4.2 Visualization

The bar chart below compares the simulated expectation values against the theoretical predictions of Quantum Mechanics.

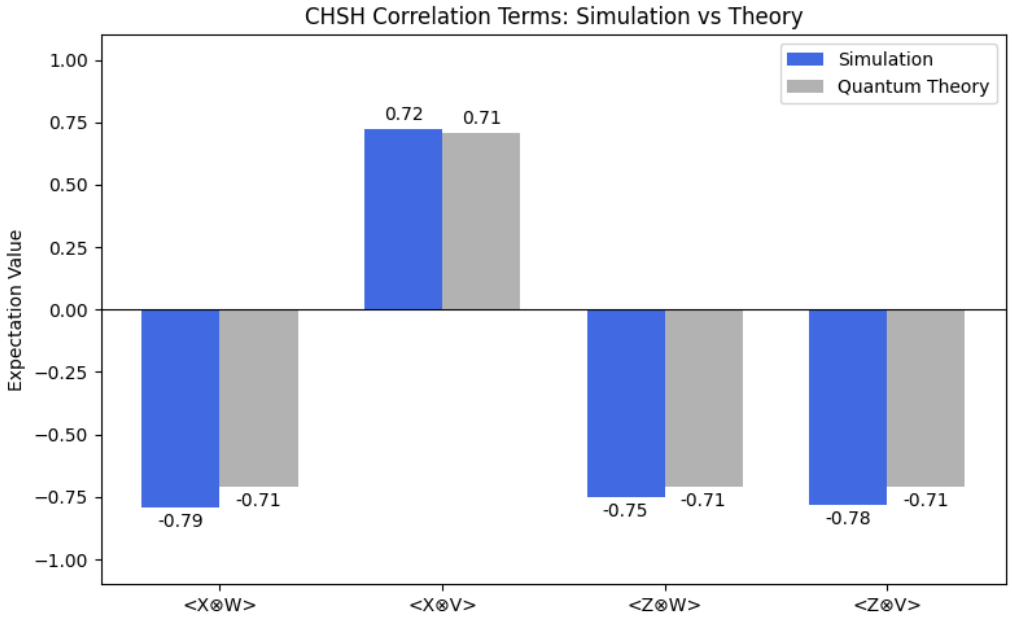

Figure 4.1: Comparison of Simulated CHSH terms vs Quantum Theory. The magnitude of the simulation results clearly follows the theoretical predictions required to violate the CHSH inequality.

Chapter 5

Conclusion

The experiment successfully demonstrated the E91 protocol. A secure key of 206 bits was generated with a 0% error rate (QBER), verifying the perfect anti-correlation of the singlet state in matching bases. Furthermore, the CHSH test resulted in $|S| \approx 3.04 > 2$, definitively violating the classical limit and proving the presence of quantum entanglement in the channel.