Quantum Computing
Assessed Exercise
Submission date: Tuesday 17th March

Simon Gay

February 14, 2026

Introduction

This exercise is based on a quantum key distribution protocol called Ekert 91 or E91. E91 is similar to BB84 in that it involves a sequence of measurements in randomly chosen bases. The key differences are (1) E91 uses entangled states, and (2) an attacker is detected by checking a Bell inequality. The aim of the exercise is to implement a simulation of E91 in qBraid, demonstrating correct operation of the protocol and showing that an attacker can be detected. It is closely related to both parts of the lab exercise from week 4.

Theory of the Ekert 91 protocol

As usual, Alice and Bob want to establish a shared key consisting of a sequence of N bits. They rely on a seqence of entangled pairs of qubits, which can be sent to them by a third party. Each entangled pair is in the state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

We saw in Lecture 8 that Alice and Bob can test the entanglement of the sequence of pairs of qubits. To do this, for each pair, Alice randomly chooses to measure Z or X, and Bob randomly chooses to measure $W = \frac{1}{\sqrt{2}}(X + Z)$ or $V = \frac{1}{\sqrt{2}}(X - Z)$.

(I have negated Bob's operators here, and changed notation by introducing W and V. This is to align with standard presentations of E91, and it doesn't make any difference to the calculations).

To perform the entanglement test, Alice and Bob do a series of measurements on the sequence of pairs of qubits. They calculate

$$S = |\langle X \otimes W\rangle - \langle X \otimes V\rangle + \langle Z \otimes W\rangle + \langle Z \otimes V\rangle|.$$

What does this mean? $\langle X \otimes W \rangle$ is the average value of the result of measuring $X \otimes W$. Measuring $X \otimes W$ means measuring Alice's qubit in the basis corresponding to operator X and measuring Bob's qubit in the basis corresponding to operator W. The results of these measurements are converted from $\{0, 1\}$ to $\{+1, -1\}$ and multiplied together. The average value is calculated by adding up these results across all the pairs of qubits, and dividing by the length of the sequence. For each measurement, Alice and Bob make independent random choices of measurement, and the results are added to the totals for $\langle X \otimes W \rangle$, $\langle X \otimes V \rangle$, $\langle Z \otimes W \rangle$ or $\langle Z \otimes V \rangle$ as appropriate. Finally take the absolute value. If the value is close to $2\sqrt{2}$ then there is entanglement, but if the value is below 2 then there are only classical correlations. This is all in Lecture 8 and Lab 4B.

In the entanglement test, Alice and Bob never measure in the same basis as each other, so they are never guaranteed to get the same result from both of their measurements. The idea of the E91 protocol is to give Alice and Bob the possibility of measuring in the same basis as each other some of the time, so that in those cases, they are guaranteed to get the same result as each other. Those results can be used as a shared cryptographic key. (Actually they get opposite results, because of the particular entangled state we are using, but they can agree in advance that Bob will invert all of his bits). If Alice and Bob do not measure in the same basis as each other, they use the results to do the calculation for the entanglement test. Given that the sequence of qubits they are working with are constructed as entangled pairs, if the entanglement test fails, this is interpreted as the presence of an attacker who is disrupting the qubits.

Alice and Bob each work with three operators that they can measure. Alice's operators are

$$A_1 = X, \quad A_2 = W, \quad A_3 = Z$$

Bob's operators are

$$B_1 = W, \quad B_2 = Z, \quad B_3 = V$$

If Alice chooses A_3 and Bob chooses B_2 then they are both measuring in the standard basis and their results are guaranteed to be opposite.

Similarly if Alice chooses A_2 and Bob chooses B_1 then they are both measuring in the W basis and their results are also guaranteed to be opposite.

If Alice's and Bob's choices correspond to terms in the definition of S above, then they use the results as part of the calculation of S. This covers the choices (A_1, B_1), (A_1, B_3), (A_3, B_1) and (A_3, B_3). There are three other possible combinations of measurement: (A_1, B_2), (A_2, B_2) and (A_2, B_3). The results of these measurements are discarded.

Now for the protocol itself. Alice and Bob are trying to establish a shared key of length N. They go through the following steps $\frac{9N}{2}$ times, storing the results of their measurements and their choices of basis.

1. Alice and Bob each receive one qubit of an entangled pair in state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.
2. Alice chooses an operator A_i randomly from her set of three, with probability $\frac{1}{3}$ each.
3. Bob chooses an operator B_j randomly from his set of three, with probability $\frac{1}{3}$ each.
4. Alice measures operator A_i on her qubit. The details of how to do this are in Lab 4B.
5. Bob measures operator B_j on his qubit, again as in Lab 4B.

Alice and Bob then share their sequence of operator choices, i and j for each repetition. In the cases when $i = 2$ and $j = 1$, or when $i = 3$ and $j = 2$, their results should be opposite (because the bases are the same) and form part of the final key. This happens $\frac{2}{9}$ of the time on average, producing a key of length N as required. Because Alice and Bob obtain opposite bit values, they agree at the beginning that Bob will invert all of his bits.

For the remaining $\frac{7}{9}$ of the results, Alice and Bob share their results and calculate $|S|$ using the observed freqencies of results. If they find that $|S|$ is close to $2\sqrt{2}$ they are satisfied that they were measuring entangled states and they conclude that they have a secret key. If, however, $|S|$ is significantly less than $2\sqrt{2}$ then they conclude that the entanglement has been disrupted by an eavesdropper's measurements. The extreme case would be that an attacker interfered with every entangled pair, resulting in complete loss of quantum correlation and $|S| \leqslant 2$.

The exercise (finally!)

Along the lines of Lab 4, implement a demonstration of the Ekert 91 protocol, with and without an attacker. This will draw on your work with the BB84 protocol, as well as the illustration of the Bell inequality experiment. To get the probability of $\frac{1}{3}$ that you need for the random choice of basis, you should put a qubit into the state $\frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle$ and measure it. To get that state you will need to construct a suitable unitary operator and use it as a gate in a circuit. For development purposes you can start by using a Python random number library, but your final code should use a quantum measurement.

Practical instructions

The GitHub repository `SimonGay/UoG-QC-Assignment` is a template. You can create your own repository as a copy of it. It contains two notebooks, `Ekert91-Plain` and `Ekert91-Attacker`. They are empty except for the usual imports. Work on the assignment in your repository, then submit it by giving Simon Gay access (user name: SimonGay). The submission deadline is **Tuesday 17th March, 4pm.**