1 Practice

Quantum Money. Imagine the following procedure to counterfeit one quantum coin (a qubit). Among 3 qubits, initialize the first two qubits to $|0\rangle$ and let the third qubit be the qubit from the original banknote to be counterfeited. Then apply a 3-qubit unitary transformation. Finally, discard the first qubit and output the state given by the second two qubits.

a) Run the protocol using a random unitary[1] on a quantum computer and compute what is the probability that both the qubits get validated by the bank.

b) it turns out that the optimal choice is a unitary whose effect is the following mapping:

$$|000\rangle \to \frac{\sqrt{3}}{2}|000\rangle + \frac{|110\rangle + |101\rangle + |011\rangle}{\sqrt{12}} \tag{1}$$

$$|001\rangle \to \frac{\sqrt{3}}{2}|111\rangle + \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{12}} \tag{2}$$

Try to run a circuit with this mapping and show that the counterfeiting probability is 3/4.

Attacks on BB84. On Friday you have successfully built the BB84 protocol on the IBM machine. However, you just tested it without anyone trying to attack the system. Today we will focus instead on the bad guys and how they can try to attack our protocol.

1) Build on Qiskit a general Intercept-and-Resend attack to the BB84:

   a) Randomizing Eve's basis choice between $|0\rangle$, $|1\rangle$, i.e. basis $\{0, \pi/2\}$ and $|+\rangle$, $|-\rangle$, i.e. basis $\{\pi/4, 3\pi/4\}$. How much noise is Eve adding? what is the probability P_E of guessing each bit? This means that Eve is able to eavesdrop $I_E = 1 - h_2(P_E)$ bits per sifted bit.

   b) Choosing always an intermediate basis, called Breidtbart basis $\{\pi/8, 5\pi/8\}$. What is the QBER and the probability P_E of guessing the bit in this case?

2) [difficult] Let's try a more general approach: build the optimal individual attack on BB84, called the *economical cloner*. See Figure 1. In individual attacks, Eve interacts with each qubit in the channel separately and independently. Each of Eve's ancilla systems are prepared independently and each interact with only one qubit in the channel before being measured independently. The measurement is performed after the sifting to be sure of picking the right basis. The secret key rate corresponding to this attack is

$$K = h_2(Q_E) - h_2(Q), \text{ bits/sifted photon,} \tag{3}$$

where Q_E is the error rate Eve incurs in her measurement of Alice's information, given by

$$Q_E = \frac{1}{2}\left[1 - 2\sqrt{Q(1-Q)}\right]. \tag{4}$$

Analyze the attack varying Q.

[1] to implement given unitary with the correct gates check https://qiskit.org/documentation/tutorials/simulators/4_custom_gate_noise.html and to pick a random unitary check https://qiskit.org/documentation/stubs/qiskit.quantum_info.random_unitary.html

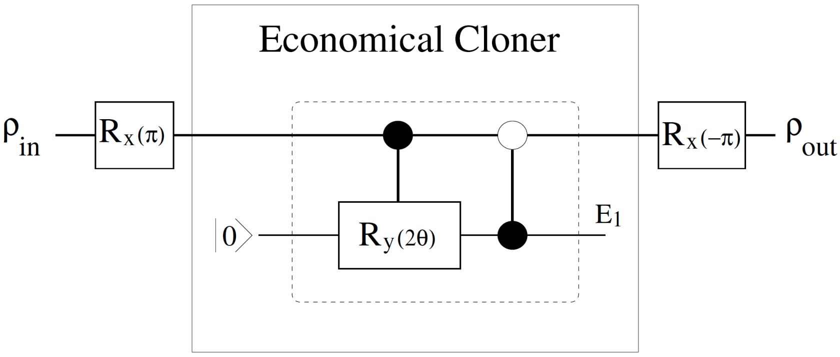

Figure 1: Quantum circuit diagram for the economical cloner. Eve prepares her ancilla in the state $|0\rangle$. Eve applies a π-rad rotation about the Bloch-sphere's x axis to the input qubit and the inverse rotation to the output qubit. In between these rotations, she interacts her ancilla with Alice's state through a controlled rotation of 2θ ($cos\theta \equiv 1 - 2Q$) about the Bloch-sphere's y axis followed by a cnot. Once the cloning is finished, Eve sends the outgoing qubit to Bob.