1 Theory

BB84 In class we discussed the BB84 QKD scheme.

a) Alice randomly samples two bitstrings $a = 011001$ and $b = 101011$. She prepares a six qubit state $|\psi\rangle$ that encodes the string a in a basis given by b. For the i-th qubit, if $b_i = 0$ then she uses the $|0\rangle$, $|1\rangle$ basis and if $b_i = 1$ then she uses $|+\rangle$, $|-\rangle$. Write down $|\psi\rangle$.

b) Alice sends $|\psi\rangle$ to Bob on a public quantum channel. Eve could intercept it, but say for now she leaves $|\psi\rangle$ untouched. Bob samples a bitstring $b' = 100111$, and measures $|\psi\rangle$ in the basis specified by b'. What is a state that could Bob measure? What bitstring does it correspond to?

c) In BB84 Alice now publicly announces b and Bob publicly announces where it differs from b'. They then discard the parts of a and a' where b and b' differ. What are they left with in each case?

2 Practice

BB84. Today we will build a full BB84 protocol without an eavesdropper (slightly different from the one on the textbook).

0) Re-run yourself the codes in https://qiskit.org/textbook/ch-algorithms/quantum-key-distribution.html without the eavesdropping part. This part is only for you to get used to BB84. The problem of its approach is that it runs a different quantum circuit for each round of the protocol. This means that we cannot run it on a real quantum computer.

1) To overcome this problem, build a circuit that simulates Alice encoding part. It should have 3 qubits. The first qubit will be the actual quantum channel, while the second and the third will be used to randomly choose the bit to encode and which basis to use respectively. Doing that, we can run many shots of the same quantum circuit, where Alice is choosing every time a new bit to encode and a new basis.

2) Now extend the quantum circuit to include also Bob's decoding strategy. You should initialize back to zero the second or the third qubit to use it again as a control to randomly choose a basis at Bob's.

3) Finally, perform sifting and estimate the QBER. With a simulation you should get QBER 0%. How much do you get with a real QC?