Exercise 1. *BB84*

The first QKD protocol was invented by Bennet and Brassard in 1984 (hence its name). In its entanglement based version (called Ekert91), Eve, an adversary, prepares many copies of a two-qubit state ρ_{AB} that she distributes to Alice and Bob (part A goes to Alice, part B goes to Bob). For each entangled state Alice and Bob have, they each randomly choose one of two bases to measure their part of their state in. These bases are: $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. Whenever Alice measures 0 or $+$ she writes down "0", and whenever she measures 1 or $-$ she writes down "1". Likewise, Bob assigns "0" to outcomes 0 or $+$ and "'1" to outcomes 1 or $-$. After that, Alice and Bob carry out the following classical steps (usually referred to as post-processing) involving authenticated classical communication.

1. Basis Sifting*: Alice and Bob will sometimes measure in the same basis, in which case they will keep their measurement outcomes. If they measure in different bases they will throw away their measurement outcomes. To determine when they have measured in the same or different bases, Bob communicates classically to Alice all the bases he measured in. Whenever Alice sees he measured in a different basis, she tells Bob to discard that measurement result (and Alice discards hers as well).*

2. Parameter Estimation*: Since Eve may give any state to Alice and Bob, Alice and Bob want to see what percentage of their signals are errors, which will help them do the next two steps. One way of doing this is te following: Bob can pick a random subset of his string and communicate it to Alice. Alice can compare Bob's results with hers, and tell Bob what percentage of those results were errors. This will give them an estimate of the percentage of errors they have in the remainder of their string. Bob discards all of the bits that he communicated to Alice to do this step, and Alice removes the corresponding bits in her string.*

   Alice and Bob only continue to the next steps if the error rate is below some threshold. If the error rate is too high, it means Eve has too much information about the states that were sent, and no amount of privacy amplification (the last step) can create a secret key.

3. Error Correction*: Now that we know how many errors we have, Alice and Bob would like to remove them from their shared string. There exist ways for them to do this at the expense of reducing the length of their shared string.*

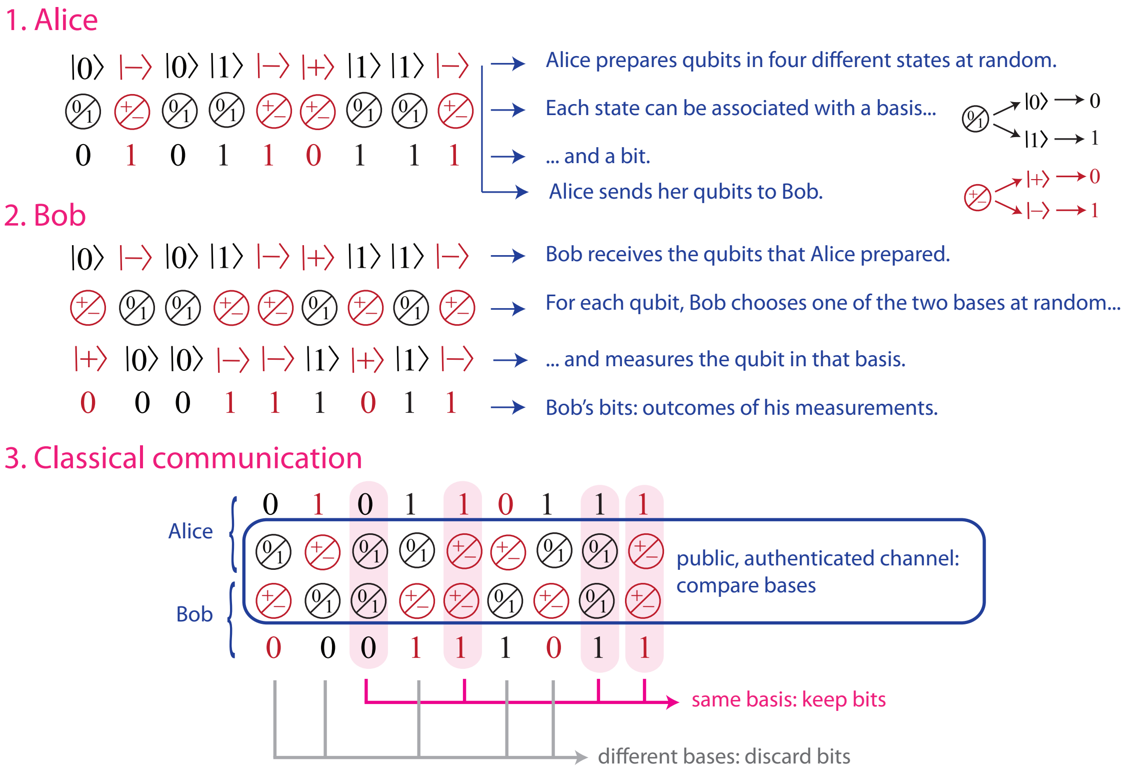
4. Privacy Amplification*: Once the errors are removed, it is possible that Eve has some information about what their shared string is. At the expense of reducing the length of their string, they can reduce Eve's knowledge about their string to a negligible amount (much less than one bit, for example), with high probability. The amount they need to reduce their shared string can be quantified, and it depends on the error probability that Alice and Bob estimated. At the end of this step, we say that Alice and Bob share a secret string. By 'secret' we mean that Eve has at most a very small amount of information about their string with high probability.*

(a) *Show that the optimal state ρ_{AB} for Alice and Bob to be sent by Eve is the maximally entangled state: $|\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$.*
Hint: *Show that with this state Alice and Bob always obtain the same outcomes and that Eve has no information about the them.*

(b) *Show that the optimal strategy for Eve (given that she has to send i.i.d. states to Alice and Bob) is to keep a purification of ρ_{AB}, namely $|\phi\rangle_{ABE}$.*
Hint: *One way of showing this is to argue that for pure states ρ_{ABE} with fixed marginal ρ_{AB}, $H(A|E)$ is maximal. Why?*

(c) *Show that the entanglement based scheme is the same as a prepare and measure scheme outlined in Figure 1. In a prepare and measure scheme, Alice randomly prepares one of the quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then sends them through an insecure quantum channel, where Eve can influence the quantum states as she wants, as long as she obeys quantum mechanics. Bob receives* *the states from Eve and performs the same measurement he did in the entanglement based version.* Hint: *Directly reduce the prepare and measure scheme to the entanglement based version.*

(d) *Describe three problems that could arise when implementing a quantum key distribution scheme experimentally.*



1. Alice
|0⟩ |−⟩ |0⟩ |1⟩ |−⟩ |+⟩ |1⟩ |1⟩ |−⟩
0 1 0 1 1 0 1 1 1
Alice prepares qubits in four different states at random.
Each state can be associated with a basis...
... and a bit.
Alice sends her qubits to Bob.
|0⟩ → 0
|1⟩ → 1
|+⟩ → 0
|−⟩ → 1
2. Bob
|0⟩ |−⟩ |0⟩ |1⟩ |−⟩ |+⟩ |1⟩ |1⟩ |−⟩
Bob receives the qubits that Alice prepared.
For each qubit, Bob chooses one of the two bases at random...
|+⟩ |0⟩ |0⟩ |−⟩ |−⟩ |1⟩ |+⟩ |1⟩ |−⟩
... and measures the qubit in that basis.
0 0 0 1 1 1 0 1 1
Bob's bits: outcomes of his measurements.
3. Classical communication
Alice
0 1 0 1 1 0 1 1 1
Bob
0 0 0 1 1 1 0 1 1
public, authenticated channel: compare bases
same basis: keep bits
different bases: discard bits

Figure 1: The BB84 prepare and measure protocol

Solution.

(a) To show that this state is optimal, we need to show that Alice and Bob always get the same measurement outcome for both measurement bases, and that Eve has no information about their outcomes.

If Alice and Bob both measure in the Z-basis, then the probability that they get the same outcome is $\operatorname{tr}(P_{00}\,|\phi^+\rangle\langle\phi^+|)+\operatorname{tr}(P_{11}\,|\phi^+\rangle\langle\phi^+|) = 1$, where P_{ii} is the projection onto $|ii\rangle\langle ii|$. Similarly, if they both measure in the X-basis, then $\operatorname{tr}(P_{++}\,|\phi^+\rangle\langle\phi^+|)+\operatorname{tr}(P_{--}\,|\phi^+\rangle\langle\phi^+|) = 1$.

Eve is interested in learning either Alice or Bob's system, as this gives her access to both of their measurement outcomes. We can purify the state shared between Alice and Bob (which is already pure) and add Eve's ancilla E: $\rho_{ABE} = |\phi^+\rangle\langle\phi^+|_{AB} \otimes \rho_E$. Now consider $H(A|E) = H(AE) - H(E)$, by definition. Using the fact that ρ_{AE} has product form, and that ρ_A is a maximally mixed state, we get $H(A|E) = H(A) + H(E) - H(E) = 1$. This implies that Eve has no information about Alice's state (or her measurement outcomes, due to the data processing inequality). Eve could equivalently try to find out about Bob's system. By symmetry we have $H(B|E) = 1$.

Alternatively, one could consider the mutual information Eve has with Alice and Bob: $I(A:E) = H(A) + H(E) - H(AE) = H(A) + H(E) - H(A) - H(E) = 0$, again due to the form of ρ_{ABE}. Similarly, $I(B:E) = 0$.

(b) The fact that we reduce Eve's strategies to i.i.d. strategies means that in n rounds of the protocol, the total state distributed by Eve must be of the form $\eta^{(n)}_{ABE} = \rho^{\otimes n}_{ABE}$. Hence, instead of the total state $\eta^{(n)}_{ABE}$ for n rounds it is enough to consider only the state of one round, ρ_{ABE}.

Let us now compare two cases, one in which $\rho_{ABE} = |\psi\rangle\langle\psi|_{ABE}$ is pure, and one where $\rho_{ABE} = \sigma_{ABE}$ is mixed. The mixed state can be purified to $|\varphi\rangle\langle\varphi|_{ABEE'}$ and due to the data processing inequality (or, mainly, strong subadditivity) we have

$$H(A|E)_\sigma \geq H(A|EE')_{|\varphi\rangle} \,. \tag{S.1}$$

But now $|\varphi\rangle$ and $|\psi\rangle$ are two purifications of the same marginal ρ_{AB}, hence can be related by a local isometry on the purifying system (which cannot change the eigenvalues of the marginals). Thus: $H(A|EE')_{|\varphi\rangle} = H(A|E)_{|\psi\rangle}$. Altogether we find that purifications always give more information to Eve than mixtures of them, $H(A|E)_\sigma \geq H(A|E)_{|\psi\rangle}$. The same can be shown for Eve's knowledge about Bob's state, $H(B|E)$ using symmetry under exchange of A and B.

(c) In the prepare and measure scheme, Alice chooses one of four states to send to Bob. She could model this as preparing a bipartite state on $\mathbb{C}^4 \otimes \mathbb{C}^2$, sending the two-dimensional part to Bob and performing a measurement in her four-dimensional space (projecting onto one of $|0\rangle, |1\rangle, |2\rangle, |3\rangle$). The state would then be

$$\begin{aligned}
|\Psi\rangle &= \frac{1}{2}(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|+\rangle + |3\rangle|-\rangle) \\
&= \frac{1}{2}\left(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + |3\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\
&= \frac{1}{2}\left(\left(|0\rangle + \frac{|2\rangle + |3\rangle}{\sqrt{2}}\right)|0\rangle + \left(|1\rangle + \frac{|2\rangle - |3\rangle}{\sqrt{2}}\right)|1\rangle\right) \\
&\equiv \frac{1}{\sqrt{2}}\left(|\tilde{0}\rangle|0\rangle + |\tilde{1}\rangle|1\rangle\right),
\end{aligned} \tag{S.2}$$

where $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$ are orthonormal states that are linear combinations of the basis vectors in Alice's four-dimensional space. This way of seeing the prepare and measure scenario makes it obvious that it just another way of distributing entangled states to Alice and Bob. Now Alice and Bob could as well perform the same procedure as in the entanglement based scheme.

(d) There are several practical problems with QKD, some examples are:

(i) The measurement devices to do not act exactly as described in the protocol, leaving options to Eve to gain more information about the outcomes than otherwise possible.

(ii) The states that are required to be prepared, are not prepared exactly.

(iii) Eve can do an attack on the protocol by using other degrees of freedom, such as the frequency of the light used to communicate, use multiple photons/qubits to send into the measurements on Alice and/or Bob, monitoring the relative phases of the pulses between Alice and Bob, etc. These are called side-channel attacks and have been shown to be a major problem when implementing QKD protocols.

(iv) The classical channel is not perfectly authenticated. However, an authenticated channel is necessary so Alice and Bob know who they are communicating with in the post processing steps.

If you are interested in more detail how QKD can be hacked, see http://www.vad1.com/lab/.