Exercise sheet 2

Notations. $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. " $+$ " corresponds to the $\{|0\rangle, |1\rangle\}$ basis and " $\times$ " corresponds to the $\{|+\rangle, |-\rangle\}$ basis. We have $|b\rangle^{+} = |b\rangle$ and $|b\rangle^{\times} = H|b\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b |1\rangle\right)$. Recall the main steps of the BB84 protocol

1. Alice picks a random initial raw key $K = k_1, \ldots, k_n$ uniformly at random.
2. For each $i \in \{1, \ldots, n\}$, Alice picks a random $b_i \in \{+, \times\}$, constructs $|\psi_i\rangle = |k_i\rangle^{b_i}$ and sends $|\psi_i\rangle$ to Bob.
3. Bob picks some random basis $b'_1, \ldots, b'_n \in \{+, \times\}$ and measures each qubit $|\psi_i\rangle$ in the b'_i basis. Let c_i be the outcome of this measurement.
4. Bob sends to Alice the basis $\mathbf{b}' = b'_1, \ldots, b'_n$ he used for his measurements using a public channel. Alice sends back the subset $I = \{i \in [n] : b_i = b'_i\}$ to Bob.
5. Alice then picks a random subset $J \subseteq I$ of size $\frac{|I|}{2}$ which is the subset of indices for which Alice and Bob check that there wasn't any interception and sends J to Bob. For $j \in J$, Alice also sends k_j to Bob.
6. For each $j \in J$, Bob checks that $k_j = c_j$. If one of these checks fail, he aborts.
7. Let $L = I \backslash J = l_1, \ldots, l_{|L|}$ be the subset of indices used for the final raw key. Alice has $K_A = \{k_l\}_{l \in L}$ and Bob has $K_B = \{c_l\}_{l \in L}$. They perform key reconciliation and privacy amplification to obtain the final common key K_{final}.

Exercise 1. *We consider the BB84 quantum key distribution protocol seen in class. We want to analyze the information that an eavesdropper Eve can have about each k_i if she measures the qubits $|\psi_i\rangle$ at step 2. We first consider here the case $n = 1$, so there is a single k_1, b_1 and a single state $|\psi_1(b_1, k_1)\rangle$ sent.*

1. *Write the 4 states $|\psi_1(b_1, k_1)\rangle$ as a function of b_1, k_1.*
2. *Knowing that each b_i, k_i are chosen uniformly at random. What information does an eavesdropper have about b_i given this state? Justify your answer.*
3. *What is the eavesdropper probability of guessing k_1 given his state? Justify your answer.*

Solution:

1. We have

$$
\begin{aligned}
|\psi_1(+,0)\rangle &= |0\rangle \\
|\psi_1(+,1)\rangle &= |1\rangle \\
|\psi_1(\times,0)\rangle &= |+\rangle \\
|\psi_1(\times,1)\rangle &= |-\rangle
\end{aligned}
$$

2. If $b_i = +$, then the eavesdropper has $|\psi_1(+,0)\rangle$ with probability $\frac{1}{2}$ and $|\psi_1(+,1)\rangle$ with probability $\frac{1}{2}$. This means he has the state $\rho_+ = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. On the other hand, if $b_i = \times$, the eavesdropper has the state $\rho_\times = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$. Notice that $\rho_+ = \rho_\times$ so an eavesdropper has no information about b_i.

3. If $k_i = 0$, then the eavesdropper has $|0\rangle$ with probability $\frac{1}{2}$ and $|+\rangle$ with probability $\frac{1}{2}$ so the eavesdropper has the state $\sigma_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$. On the other hand, if $k_i = 1$, the eavesdropper has the state $\sigma_1 = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|-\rangle\langle -|$. One can check that $\Delta(\sigma_0, \sigma_1) = \frac{1}{\sqrt{2}}$ and that an eavesdropper can guess k_i with probability at most $\cos^2(\pi/8)$.

□

Exercise 2. *We consider another cheating strategy. The second cheating strategy for Eve consists in intercepting and storing the states $|\psi_i\rangle$ at step 2 and wait until she sees $\mathbf{b}', I, J$ after step 5 in order to get some information about the key.*

1. *Show that with this strategy, Eve can recover all the string k.*
2. *The issue with this strategy is the test at step 6. If Eve intercepts $|\psi_i\rangle$ then Bob doesn't get any state at the end of step 2. For each i, Eve sends a state $|\xi_i\rangle$ which is independent of b_i and k_i (since Eve doesn't know them). For a index i, compute the probability that Bob outputs c_i for each choice b'_i, depending on $|\xi_i\rangle$. Show that the probability of outputting $b'_i = b_i$ and $k_i \neq c_i$ is $\frac{1}{4}$.*
3. *Conclude on the efficiency of this cheating strategy.*

Solution:

1. Eve keeps $|\psi_i\rangle = |k_i\rangle^{b_i}$ and then receives $b'_1, \ldots, b'_n$ as well as I. From this information, Eve can recover all of b_i. If she measures each $|\psi_i\rangle$ in the b_i basis, she can recover each k_i.

2. If Bob chooses $b'_i = 0$, he outputs c_i wp. $|\langle \xi_i | c_i \rangle|^2$. If $b'_i = 1$, he outputs c_i wp. $|\langle \xi_i| H |c_i\rangle|^2$. Assume that $b_i = b'_i$. This happens wp $\frac{1}{2}$ since these bits are uniform random bits and independent. Assume these are both 0. Let p_c the probability that Bob outputs $c_i = c$. We clearly have $p_0 + p_1 = 1$. Moreover, since k_i is random, we have $Pr[k_i \neq c_i] = \frac{1}{2}p_0 + \frac{1}{2}p_1 = \frac{1}{2}$. A similar analysis can be done when $b_i = b'_i = 1$. We conclude that the probability that $b_i = b'_i$ and $k_i \neq c_i$ is $\frac{1}{4}$.

3. With this strategy, Eve can recover a bit of key but is caught wp. $\frac{1}{4}$ each time.

□

Exercise 3. *We consider now a more realistic scenario where there are imperfection in the quantum devices. Consider the honest setting without eavesdropper and assume that Bob obtains the state* $\frac{2}{100}\rho_I + \frac{98}{100}|\phi_i\rangle\langle\phi_i|$ *where* $\rho_I = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$.

1. *How does this impact the protocol?*
2. *Can you think of a way to modify the protocol in order to make it work? You don't need to prove that your solution works but just give an intuition.*

Solution:

- When projecting on $|\phi_i\rangle$, Bob will get the wrong answer with probability 1%, so he will abort the protocol even if there is no eavesdropper.
- Change step 6 by adding a threshold. Say that Bob aborts if more than 2% of the checks fail. Since in the honest case, it is 1%, the check will be passed with high probability. On the other hand, we can show that in the cheating setting it will be much more.

□

Exercise 4. *We consider yet another cheating strategy in the case the classical channel is not authenticated, meaning that Eve can modify the messages sent in the classical portion. Show how can Eve can cheat in this setting (recall that she can also tamper the quantum channel).*

Solution: Eve performs a man in the middle attack and measures: she intercepts all the classical messages. She impersonated Bob when interacting with Alice and impersonates Alice when interacting with Bob. At the end, Eve shares with Alice a key K_1 and with Bob a key K_2. □