QII Exercise sheet 13

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 $|\psi_1\rangle$ sent.*

1. *Let ρ_{k_1} be the state that Alice sends as a function of k_1. Describe the mixed states ρ_0 and ρ_1. Let $|v\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and $|v^{\perp}\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$. Show that*

$$\rho_0 = \cos^2(\pi/8)|v\rangle\langle v| + \sin^2(\pi/8)|v^{\perp}\rangle\langle v^{\perp}| \quad (1)$$

$$\rho_1 = \sin^2(\pi/8)|v\rangle\langle v| + \cos^2(\pi/8)|v^{\perp}\rangle\langle v^{\perp}| \quad (2)$$

2. *Compute the statistical distance between ρ_0 and ρ_1.*
3. *Compute Eve's optimal strategy to guess k_1. What is the measurement that achieves this guessing probability? What can you say about the overall security of the scheme.*

Solution:

1. Let $|v\rangle = \cos(\pi/8)\,|0\rangle + \sin(\pi/8)\,|1\rangle$ and $\left|v^{\perp}\right\rangle = -\sin(\pi/8)\,|0\rangle + \cos(\pi/8)\,|1\rangle$. We have $\rho_0 = \frac{1}{2}\left(|0\rangle\langle 0| + |+\rangle\langle +|\right) = \cos^2(\pi/8)|v\rangle\langle v| + \sin^2(\pi/8)|v^{\perp}\rangle\langle v^{\perp}|$ and $\rho_1 = \frac{1}{2}\left(|1\rangle\langle 1| + |-\rangle\langle -|\right) = \sin^2(\pi/8)|v\rangle\langle v| + \cos^2(\pi/8)|v^{\perp}\rangle\langle v^{\perp}|$. This can be checked by computing the density matrices.

2. $\Delta(\rho_0, \rho_1) = \left(\cos^2(\pi/8) - \sin^2(\pi/8)\right) = \frac{1}{\sqrt{2}}$.

3. The optimal probability of distinguishing ρ_0 and ρ_1 is $\frac{1}{2} + \frac{\Delta(\rho_0,\rho_1)}{2} = \frac{1}{2} + \frac{\sqrt{2}}{4} = \cos^2(\pi/8)$. You can achieve this probability by measuring in the $\{|v\rangle, \left|v^{\perp}\right\rangle\}$ basis. If Eve tries to recover information about K at this point then she can only recover partial information about K.

□

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, Alice can recover all the string k.*
2. *The issue with this strategy is the test at step 6. If Eve intercepts $|\phi_i\rangle$ 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 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. □

* * *

Exercise 4 (Quantum Weak Coin Flipping)**.** *Alice and Bob interact and want to flip a random coin. Alice wins if they agree on outcome "0" and Bob wins on outcome "1". Describe the construction seen in class (without looking at its description in the lecture notes) that shows how to use a bit commitment protocol with cheating probabilities P_A^*, P_B^* to perform a coin flipping protocol with the same winning probabilities. Hint: consider a protocol where Alice commits to a bit b, receives a message from Bob and then reveals b.*

Solution: We consider the following protocol

- Alice chooses a random bit b and commits to b.
- Bob chooses a random $c \in \{0, 1\}$ and sends c to Alice.
- Alice reveals b. The output of the coin flipping protocol is the bit $a = b \oplus c$. They agree on the value of Bob doesn't abort.

Bob wins if he sends $c = b \oplus 1$ so if he guessee b. This happens wp. at most P_B^*. On the other hand, for any commit phase, Alice wins if she reveals $b = c$. Since c is random, her probability of winning is

$$\frac{1}{2}\Pr[\text{Alice successfully reveals } b = 0] + \frac{1}{2}\Pr[\text{Alice successfully reveals } b = 1] = P_A^*.$$

□

Exercise 5 (Loss tolerant quantum coin flipping protocols with single qubits)**.** *We study the following generic bit commitment based quantum coin flipping scheme:*

Parameters : *two bipartite states* $|\Phi^0_{AB}\rangle$ *and* $|\Phi^1_{AB}\rangle$*. In particular we are interested in* $\rho_0 = Tr_A(|\Phi^0_{AB}\rangle)$ *and* $\rho_1 = Tr_A(|\Phi^1_{AB}\rangle)$

Protocol :

1. *Alice picks a random bit* a*, creates* $|\Phi^a_{AB}\rangle$ *and sends the* B *part to Bob.*
2. *Bob picks a random bit* b *and sends it to Alice.*
3. *Alice reveals her bit* a *and sends the second part of* $|\Phi^a_{AB}\rangle$ *to Bob. Bob checks that he has the correct state by projecting the state he has onto* $|\Phi^a_{AB}\rangle$*.*
4. *The outcome of the coin is* $c = a \oplus b$*.*

Cheating probabilities : *Here, cheating Alice's goal is to enforce outcome* $c = 0$ *while cheating Bob's goal is to enforce* $c = 1$*. We can use that the cheating probabilities for Alice and Bob can be written as*

$$P^*_A = \max \Pr[\textit{Alice cheats}] = \frac{1}{2} + \frac{F(\rho_0, \rho_1)}{2}$$
$$P^*_B = \max \Pr[\textit{Bob cheats}] = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

We also define P^**, the cheating probability of the protocol as* $P^* = \max(P^*_A, P^*_B)$*. Our goal is to study these protocols where the states* ρ_a *are single qubits.*

1. *We add a parameter* $x \in]0, 1[$ *and consider a protocol with states* $\rho_0 = |0\rangle\langle 0|$ *and*
   $\rho_1 = (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$*. In this case, what are the cheating probabilities for Alice and Bob? Find* x *such that* P^* *is minimal. Show that this minimum* P^* *is equal to* $\frac{1+\sqrt{5}}{4}$ *(which is* $\approx 81\%$*).*
2. *We now consider a parameter* $x \in]1/2, 1[$ *and a protocol with states*
   $\rho_0 = x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1|$ *and* $\rho_1 = (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$*. In this case, what are the cheating probabilities for Alice and Bob? Find* x *such that* P^* *is minimal. Show that this minimum* P^* *is equal to* $\frac{1}{2} + \frac{\sqrt{2}}{4}$ *(which is* $\approx 85\%$*).*

Losses: *We are now interested in the case where there are losses in the quantum channel. Losses imply that when Alice sends her qubit to Bob during step* 1*, he might not receive anything. If Bob didn't receive any qubit, he declares 'Loss' to Alice and they start again. Our goal is to see if a cheating Bob can use this to his advantage. A cheating Bob also has losses but when he actually receives the state* ρ_a*, he can still declare 'Loss' and start the protocol again.*

3. *We consider the first studied protocol with* $\rho_0 = |0\rangle\langle 0|$ *and* $\rho_1 = (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$*, for any* $x \in]0,1[$*. Find a measurement* $\{|e_0\rangle, |e_1\rangle\}$ *for Bob with the following properties:*

   - $\Pr[$*Bob outputs* $|e_0\rangle$ $|$*Bob has* $\rho_0] = 1$
   - $\Pr[$*Bob outputs* $|e_0\rangle$ $|$*Bob has* $\rho_1] < 1$

   Use this measurement to describe (informally) a cheating strategy for Bob that works with probability 1 *in the presence of losses.*

4. *We consider the second studied protocol with* $\rho_0 = x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1|$ *and* $\rho_1 = (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$*, for any* $x \in]1/2,1[$*. Show that a measurement* $\{|e_0\rangle, |e_1\rangle\}$ *for Bob such that:*

   - $\Pr[$*Bob outputs* $|e_0\rangle$ $|$*Bob has* $\rho_0] = 1$
   - $\Pr[$*Bob outputs* $|e_0\rangle$ $|$*Bob has* $\rho_1] < 1$

   cannot exist.
   Conclusion: *This shows that even if the second protocol has a larger cheating probability, he cannot use the same strategy as in the for the previous protocol in order to cheat with probability* 1*.*

5. *Finally, we consider the protocol with* $\rho_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|2\rangle\langle 2|$ *and* $\rho_1 = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|$*. For this protocol, describe (informally) a cheating strategy that allows Bob to cheat with probability* 1 *in the presence of losses.*

Solution:

1.

$$P_A^* = \frac{1}{2} + \frac{F(\rho_0,\rho_1)}{2} = \frac{1}{2} + \frac{\sqrt{1-x}}{2}$$
$$P_B^* = \frac{1}{2} + \frac{\Delta(\rho_0,\rho_1)}{2} = \frac{1}{2} + \frac{x}{2}$$

P_A^* is an increasing function of x and P_B^* is a decreasing function of x so the minimum of P^* is achieved for $P_A^* = P_B^*$. This happens for $x = \sqrt{1-x}$ or for $x^2 + x - 1 = 0$. The only correct solution is $x = \frac{\sqrt{5}}{2} - \frac{1}{2}$. This gives $P^* = \frac{1+\sqrt{5}}{4} \approx 81\%$.

2.
$$P_A^* = \frac{1}{2} + \frac{F(\rho_0, \rho_1)}{2} = \frac{1}{2} + \sqrt{x(1-x)}$$
$$P_B^* = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2} = \frac{1}{2} + \frac{2x-1}{2} = x$$

P_A^* is an decreasing function of x for $x \in [1/2, 1]$ and P_B^* is an increasing function of x so the minimum of P^* is achieved for $P_A^* = P_B^*$. This happens when $x - 1/2 = \sqrt{x(1-x)}$ or for $2x^2 - 2x + 1/4 = 0$. The only correct solution is $x = \frac{2+\sqrt{2}}{4}$. This gives $P^* = \frac{2+\sqrt{2}}{4} \approx 85\%$.

3. We take $|e_0\rangle = |0\rangle$ and $|e_1\rangle = |1\rangle$. If Alice has 0, Bob has $\rho_0 = |0\rangle\langle 0|$ and his measurement gives outcome $|0\rangle$ with probability 1. If Alice has 1, Bob has ρ_1 and his measurement gives outcome $|0\rangle$ with probability $\langle 0|\rho_1|0\rangle = 1 - x \neq 1$.

   We consider the following cheating strategy for Bob. When receiving Alice's qubit, he measures in the $\{|0\rangle, |1\rangle\}$ basis. If he measures $|0\rangle$, he declares 'Loss' and they start again. If he measures $|1\rangle$, he continues the protocol. In this second case, Bob knows that Alice has $a = 1$ so he has full control of the output of the coin since now, $c = \overline{b}$.

4. Consider a measurement $\{|e_0\rangle, |e_1\rangle\}$ such that Pr[Bob outputs $|e_0\rangle$ $|a = 0] = 1$. We have

   $$Pr[\text{Bob outputs } |e_0\rangle \ |a = 0] = \langle e_0|\rho_0|e_0\rangle = x|\langle 0|e_0\rangle|^2 + (1-x)|\langle 1|e_0\rangle|^2 = 1$$

   Since $x \in [1/2, 1[$, this gives $|\langle 0|e_0\rangle|^2 = |\langle 1|e_0\rangle|^2 = 1$. This implies

   $$Pr[\text{Bob outputs } |e_0\rangle \ |a = 1] = \langle e_0|\rho_1|e_0\rangle = (1-x)|\langle 0|e_0\rangle|^2 + x|\langle 1|e_0\rangle|^2 = 1$$

   which shows that a measurement $\{|e_0\rangle, |e_1\rangle\}$ with the required properties is impossible.

5. Bob measures in the $\{|0\rangle, |1\rangle, |2\rangle\}$ basis. On outcome $|2\rangle$, he declares 'Loss'. On outcome $|a\rangle$, he declares $b = \overline{a}$. If he measures $|a\rangle$ then Alice necessarily has bit a. This strategy always gives $c = a \oplus b = 1$.

□