Quantum Cryptography (fall 2017) Dominique Unruh

Exercise Sheet 10

Out: 2017-12-30 Due: 2018-01-07

This is a bonus homework. Each problem gives up to 10 points. Pick at most three problems to solve (to keep the work of correcting down).

Problem 1: Quantum Operations

Describe the partial trace as a quantum operation. More exactly, let $\mathcal{H}_A = \mathbb{C}^n$, $\mathcal{H}_B = \mathbb{C}^m$. Find operators $E_k : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A$ such that these define a quantum operation $\mathcal{E} = \{E_k\}_k$ with the property that $\mathcal{E}(\rho) = \mathrm{tr}_B\, \rho$ for all ρ. Show that $\mathcal{E}$ is indeed a quantum operation (i.e., that the E_k are valid operators for defining a quantum operation).

Hint: For density operators ρ we have $\mathrm{tr}\, \rho = \sum_k \langle k|\rho|k\rangle$. Note that here $\langle k|$ is a linear operator from $\mathcal{H}_B$ to $\mathbb{C}$. And $I \otimes \langle k|$ is a linear operator from $\mathcal{H}_A \otimes \mathcal{H}_B$ to $\mathcal{H}_A \otimes \mathbb{C} = \mathcal{H}_A$.

Problem 2: Alice and Bob are being clever

Alice and Bob had a few clever ideas. In each case, explain why the idea is not a good one.

1. Alice noticed that with a sufficiently strong laser pointer, she can make a beam that is still easily seen on the moon. Since Bob is on a holiday on the moon, they decide to do a key exchange. For this, they take an off-the-shelf QKD protocol (one that only requires that Alice sends randomly polarised photons, and that Bob measures in a random polarisation direction – no quantum computers needed). And as the photon source, Alice uses her laser pointer. That is, she sends short light flashes of the laser pointer through her polarisation filter as specified by the QKD protocol.

2. Alice and Bob want to use some QKD protocol over a long distance (300 km). Unfortunately, all QKD protocols and implementations they know of do not manage to do more than 250 km (because otherwise the error rate on the channel would become too high). Fortunately, in the middle between Alice and Bob lives Charlie, an untrusted yet helpful person. To get rid of the errors, they let Charlie work as an amplifier: Each qubit is sent to Charlie, and Charlie measures the qubit and resends it using a fresh photon.

3. In a usual QKD protocol Alice would first send the qubits. Then she would wait for Bob to receive these. Then Alice sends the bases in which she produced the check qubits (or some other classical information needed for the check/purification/privacy amplification; this depends on the protocol they use). Alice and Bob decide to be more efficient and do a "compressed QKD". Since it is only Alice that sends something, anyway, she sends all information simultaneously. I.e., she sends the qubits and the classical information at the same time (over the quantum and the authenticated classical channel, respectively) and thus achieves at least doubled throughput.

Problem 3: Concrete parameters

Consider the QKD scheme described in Definition 45 in the lecture notes. Theorem 5 in the lecture notes shows that the protocol is ε-secure for a certain ε that depends on the protocol parameters.

Suggest a choice of parameters such that $\varepsilon \leq 2^{-80}$ and $\ell = 256$. How many qubits are transmitted for that choice?

Note: The parameter choice should be possible! That is, you need to make sure that there is a universal hash function F and an error correcting code with the right parameters.

Note: For any integers $a, b > 0$ with $b < 2^a - 1$, there exists a so-called Reed-Solomon code with code words of length $a(2^a - 1)$, correcting $\lfloor b/2 \rfloor$ errors, and with syndrome length ab.

Note: You do not need to find an optimal solution.

Problem 4: Impossibility of Quantum Commitments

(a) In the lecture, we have seen that bit commitment using quantum channels is impossible against adversaries with unlimited computational power. On the other hand, we have seen a commitment protocol that is secure against adversaries with a bound on their quantum memory, but still no bound on their computational abilities.

Explain why the proof given in the lecture does not apply to that protocol. In other words, where did we use that the adversary can store quantum memory between the commit and open phase?

(b) Explain why the impossibility proof does not rule out bit commitment protocols against computationally bounded adversaries using suitable complexity assumptions (e.g., one-way function that are hard to invert even for quantum computers).

Problem 5: Hiding without communicating

In the lecture we saw a commitment protocol where Alice does not send any data during the commit phase. I said that since Alice does not send anything, obviously Bob does not

learn anything, and thus the protocol is perfectly hiding (i.e., 0-hiding). This, however, is not really a proof because it only addressed the intuitive meaning of "hiding". Show that in fact the protocol is secure with respect to the formal definition of hiding (Definition 53 in the lecture notes).

Problem 6: A toy QKD protocol

Consider the following protocol:

- Alice chooses n random bits $x_1, \dots, x_n \in \{0,1\}$ and n random bases $b_1, \dots, b_n \in \{+, \times\}$. Let $x := x_1 \dots x_n$ and $b := b_1 \dots b_n$.
- Alice sends $|\Psi\rangle := |x\rangle_b$ to Bob, i.e., the string x encoded with bases b. Bob stores $|\Psi\rangle$.
- Then Alice waits time Δ.
- Then Alice sends b to Bob over an authenticated but public channel.
- Bob measures $|\Psi\rangle$ using bases b. Let the outcomes be x'.
- Alice outputs the key x, Bob outputs the key x'.

We will show that this protocol has some security against adversaries Eve that have no quantum memory. (More precisely, we assume that when Alice waits time Δ, Eve's quantum memory is erased.)

Of course, since Bob has to use quantum memory while we assume that it is infeasible for the adversary to have quantum memory, this protocol is not very useful.

We will only consider security of Alice's key, i.e., we will show that Eve cannot guess Alice's key.[1] We will not show that Bob's key (which might be different from Alice's key if Eve interferes) is in any way secure.

(a) Show that if Eve has unlimited quantum memory (for unlimited time), she can guess Alice's key.

(b) Change the protocol so that Alice uses Bell pairs instead of picking and encoding x. Change Bob's behavior in such a way that the analysis becomes simpler (without changing what Eve observes, of course), i.e., let Bob destroy data as early as possible, and let Bob never perform any operation that does not influence Eve's observations (in particular, there is no need for Bob to compute the final key). Make sure that Alice can chose the measurement basis b as late as possible.

[1] Notice that this is only a very weak security notion. Normally, one would show that Alice's key is indistinguishable from a uniform key. But the present protocol does not satisfy such a stronger security definition.

(c) In the modified protocol, let ρ denote the state after Alice has waited time Δ, but before Alice has chosen b. Give a formula for ρ.

Note: Your description should express the fact that Eve's state is classical. The formula will then contain density operators ρ_e describing Alice's state in case that Eve has the classical state e (you do not need to give a formula for those ρ_e, of course).

(d) Let x_e and b_e be random variables denoting the values x and b under the condition that Eve's state is e. Give a lower bound for $H_\infty^\varepsilon(x_e|b_e)$ (for suitable ε).

(e) Give a lower bound for $H_\infty^\varepsilon(x|b,e)$.

Hint: You are allowed to use the fact that H_∞^ε is convex. That is: Let X_i, Y_i and I be random variables. Then $H_\infty^\varepsilon(X_I|Y_I,I) \geq \sum_i \Pr[I=i] H_\infty^\varepsilon(X_i|Y_i)$. (Here X_I denotes a value x chosen as $i \leftarrow I$, $x \leftarrow X_i$.)

Hint: You should get the same bound as in (d).

(f) Show that the probability is negligible that Eve guesses Alice's key. You may ignore the ε, i.e., you may assume that that you computed a bound on $H_\infty(x|b,e)$, not on $H_\infty^\varepsilon(x|b,e)$ in the preceding step.