Quantum Cryptography (fall 2013) Prof. Dr. Dominique Unruh

Exercise Sheet 10

Out: November 13, 2013 Due: November 19, 2013

Problem: A toy QKD protocol

Consider the following protocol:

- Alice chooses n random bits $x_1, \ldots, x_n \in \{0,1\}$ and n random bases $b_1, \ldots, b_n \in \{+, \times\}$. Let $x := x_1 \ldots x_n$ and $b := b_1 \ldots b_n$.
- 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).

[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.