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

Exercise Sheet 9

Out: November 6, 2013 Due: November 12, 2013

Problem 1: Breaking a Protocol

Consider the following commitment protocol (where n is some security parameter).

- *Commit phase.* Alice wants to commit to a bit b. First, she chooses n uniformly random bits $x_1, \ldots, x_n \in \{0,1\}$. If $b = 0$ she encodes them in the computational basis; if $b = 1$, in the diagonal basis. I.e., if $b = 0, x_i = 0$, then $|\Psi_i\rangle := |0\rangle$, if $b = 0, x_i = 1$, then $|\Psi_i\rangle := |1\rangle$, if $b = 1, x_i = 0$, then $|\Psi_i\rangle := |+\rangle$, if $b = 1, x_i = 1$, then $|\Psi_i\rangle := |-\rangle$.

  Then Alice sends the qubits $|\Psi_1\rangle, \ldots, |\Psi_n\rangle$ to Bob.

- For each of the qubits, Bob randomly chooses whether to measure it in the computational or the diagonal basis. Let the outcomes of these measurements be denoted $\tilde{x}_i$.

- *Unveil phase.* Alice sends $b, x_1, \ldots, x_n$ to Bob.

- Bob checks whether $x_i = \tilde{x}_i$ for all i where Bob measured in the right basis (computational in the case of $b = 0$, diagonal in the case of $b = 1$).

The intuition behind this protocol is as follows: It is hiding because Bob cannot distinguish which bases Alice used. It is binding because of the following reason: If Bob measures some $|\Psi_i\rangle$ in, say, the computational basis, but $|\Psi_i\rangle$ was not one of $|0\rangle, |1\rangle$, then the outcome of the measurement is to some extend random, and Alice cannot predict the output $\tilde{x}_i$ of Bobs measurement. On the other hand, if Bob measures $|\Psi_i\rangle$ in the diagonal basis, but $|\Psi_i\rangle$ was not one of $|+\rangle, |-\rangle$, then the outcome of the measurement is again random, and Alice cannot predict the output $\tilde{x}_i$ of Bobs measurement. So whatever state $|\Psi\rangle$ Alice sends, there is some probability that she will not know $\tilde{x}_i$. And since to unveil both as $b = 0$ and as $b = 1$, Alice needs to know all $\tilde{x}_i$, she will fail.

Of course, this intuition cannot be correct since we know from the lecture that this (and any other) commitment protocol cannot be secure.

(a) Show that this protocol is perfectly hiding (i.e., ε_H-hiding for $\varepsilon_H = 0$).

(b) Show that this protocol is not ε_B-binding for any $\varepsilon_B < 1$. (I.e., it is possible for Alice to commit in a way such that she can unveil both as $b = 0$ and as $b = 1$.)

Note: You have to actually give an attack. It is not sufficient to say that there exists an attack due to Theorem 5 in the lecture notes and (a).

Hint: Think of Bell pairs. Try out what happens if you measure both qubits of $|\beta_{00}\rangle$ in the diagonal basis.

Problem 2: 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?

(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 2: 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).