COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 11

This exercise sheet is designed to help you review the concepts discussed in the lecture and explore some additional interesting results that were not covered in the lecture. Exercises marked with * will have solutions provided after the exercise session, while those marked with ⧫ will be the main focus during the exercise session. You are encouraged to discuss with other students, and ask for help if you get stuck for too long.

1. (*, ⧫)**Coin flipping from bit commitment**
   Suppose given a scheme for bit commitment that is ε_h-hiding (i.e. Bob can guess Alice's commited bit with probabilitiy at most $\frac{1}{2} + \varepsilon_h$) and ε_b binding (i.e. the maximum probabilities with which Alice can force a 0 or a 1 outcome, for a given commitment phase, satisfy $p_0 + p_1 \leq 1 + \varepsilon_b$).

   (a) Design a simple protocol for coin-flipping, using the bit commitment scheme.

   (b) Determine the maximum bias of the coin flipping protocol, for both cheating Alice and cheating Bob, as a function of ε_h and ε_b.

2. (*)**Different flavors of oblivious transfer**
   The variant of oblivious transfer that we saw in class is called 1-out-of-2 OT, because Bob obtains one out of two possible Alice inputs. (For this problem, we consider only the case $\ell = 1$, i.e. Alice has two bits as inputs.) We can consider a couple other variants:

   - Rabin OT: Alice transmits a bit b to Bob, who receives b with probability 1/2 while Alice does not know which is the case. That is, the output of Bob is either b or $\perp$ (indicating that the bit was not received).
   - 1-out-of-k OT for $k > 2$: Alice holds k bits $b_1, \ldots, b_k$. For $c \in \{1, \ldots, k\}$ of Bob's choice, he can learn b_c but none of the others, and Alice does not learn c.

   Prove the equivalence of these three variants, by providing the following reductions:

   (a) 1-out-of-k OT $\Longrightarrow$ 1-out-of-2 OT

   (b) 1-out-of-2 OT $\Longrightarrow$ 1-out-of-k OT *[Hint: In your protocol, the sender should choose k random bits and invoke the 1-out-of-2 OT protocol k times.]*

   (c) 1-out-of-2 OT $\Longrightarrow$ Rabin OT

   (d) Rabin OT $\Longrightarrow$ 1-out-of-2 OT *[Hint: Use Rabin OT to send sufficiently many random bits. In your protocol, the receiver might learn both bits, but with negligible probability only.]*