# COM-440, Introduction to Quantum Cryptography, Fall 2025

## Exercise # 6

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. **Using the Pretty-Good-Measurement**

   Alice sends Bob one of the three states

   $$\rho_0 = |0\rangle\langle 0| = 1000,\ \rho_1 = \frac{1}{2}id = \frac{1}{2}1001,\ \rho_2 = |1\rangle\langle 1| = 0001$$

   with equal probability. Bob wants to determine which state Alice sent him. In this problem we work out the success probability of different possible strategies for Bob. A strategy is a POVM $\{B_0, B_1, B_2\}$ and its success probability is

   $$p_{succ}(B) \ = \ \frac{1}{3}\mathrm{Tr}(B_0\rho_0) + \frac{1}{3}\mathrm{Tr}(B_1\rho_1) + \frac{1}{3}\mathrm{Tr}(B_2\rho_2)$$

   i.e. it is the probability that Bob correctly guesses the state sent by Alice, assuming that Alice sends him each of the three states with equal probability $\frac{1}{3}$.

   The first strategy that we consider consists in Bob measuring in the Hadamard basis.

   (a) Bob sets $B_0 = |+\rangle\langle +|$, $B_1 = 0$ and $B_2 = |-\rangle\langle -|$. That is, if he measures $|+\rangle$, then he guesses that the state sent was $\rho_0 = |0\rangle\langle 0|$ and if he measures $|-\rangle$ he guesses that the state sent was $\rho_2 = |1\rangle\langle 1|$. What is Bob's success probability?

   After trying that procedure, Bob decides to switch to measuring $\rho$ in the standard basis.

   (b) Bob sets $B_0 = |0\rangle\langle 0|$, $B_1 = 0$ and $B_2 = |1\rangle\langle 1|$. What is his new success probability?

   Bob decides that he's done with ad-hoc approaches and wants to use a measurement that will be somewhat reliable.

   (c) What is Bob's success probability if he uses the pretty-good measurement?

   Bob wants to know whether he's found the optimal measurement. To help find this out, he will apply the following fact. Suppose that $\sigma$ is a positive semidefinite matrix (not necessarily of trace 1) such that $p_i\rho_i \leq \sigma$ for each $i$. Then the optimal success probability of a distinguishing measurement on the ensemble $\rho = \sum_i p_i\rho_i$ is at most $\mathrm{Tr}\sigma$. (Recall that $A \leq B$ means that $B - A$ is positive semidefinite.)

(d) What is the best upper bound Bob can derive from this fact?

(e) Can you prove the above-claimed fact?

2. **Deterministic Extractors on Bit-Fixing Sources.** We saw in class that no deterministic function can serve as an extractor for all random sources of a given length. However, this doesn't rule out the possibility that a deterministic extractor can work for some restricted class of sources.

(a) Fix an even integer $n$ and integer $t < \frac{n}{2}$. Consider the following sources.

- $X_0$ is $100 \cdots 00$ on the first $t$ bits and uniformly random on the last $n - t$ bits.
- $X_1$ is uniformly random over the set of strings with an even number of 0s.
- $X_2$ is uniformly random over the set of strings where the first $\frac{n}{2}$ bits are the same as the last $\frac{n}{2}$ bits.

Compute the min-entropy $H_{\min}(X_i)$ for each $i \in \{0, 1, 2\}$.

(b) Consider the following deterministic functions:

- $f_0(x) :=$ the XOR of the first $t$ bits of $x$.
- $f_1(x) := x_L \cdot x_R$, where $x = (x_L, x_R)$ are the left and right halves of $x$ and the inner product is taken modulo 2.
- $f_2(x) :=$ the XOR of all of the bits of $x$.

For which pairs $(i, j)$ is $f_i(X_j)$ distributed as a uniformly random bit?

(c) Alice and Bob share a classical secret $X \in \{0, 1\}^n$ generated uniformly at random. Alice and Bob make an error in their secure communication protocol and as a result, Eve learns $t$ bits of $X$. Give a deterministic function $f$ such that $f(X)$ is uniformly random over strings of length $\left\lfloor \frac{n}{t+1} \right\rfloor$ and is totally uncorrelated from Eve's bits. Justify, with proof, that your function $f$ achieves the desired task.