# 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. **(*, ♦)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 $100\cdots00$ 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.