COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 9

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. **Information reconciliation based on 2-universal hash functions**
   In this exercise we consider a protocol for information reconciliation based on a family of 2-universal hash functions. Fix a distribution P_{XY} on pairs of strings $x, y \in \{0,1\}^n$. For a $y \in \{0,1\}^n$ we let $X_y = \{x : \ P_{XY}(x,y) > 0\}$. That is, X_y is the set of possible "neighbors" of y under the distribution P_{XY}.

   Let $\mathcal{F} \subseteq \{f : \{0,1\}^n \to \{0,1\}^k\}$ be a family of 2-universal hash functions. Here, k is a parameter that will be determined later. The protocol is as follows:

   - Alice, on input x, selects a random $f \leftarrow \mathcal{F}$, evaluates $z := f(x)$ and sends both f and z to Bob.
   - Bob computes the set $D = \{x' \in X_y : f(x') = z\}$ of preimages of z under f that are also neighbors of Bob's input y.
   - If D is not empty, then Bob returns a random x' from D. Otherwise, he aborts. Alice returns x.

   Our goal is to show that, provided the parameter k is chosen correctly (as a function of the distribution P_{XY}), this protocol is correct and leaks a bounded amount of information to the eavesdropper.

   (a) Use the property of being 2-universal to show that, for a given pair (x,y), $\mathbf{Pr}(x' \neq x) \leq |X_y| 2^{-k}$, where x' is Bob's output and the probability is over the random choice of f.

   (b) For any random variables X, Y jointly distributed according to P_{XY} we define the *conditional max-entropy* of X, given Y, as $H_{max}(X|Y) = \log \max_y |X_y|$. Deduce a value for k, as a function of $H_{max}(X|Y)$ and a parameter ε, that will guarantee that the protocol is ε-correct.

   (c) How much information is leaked to the eavesdropper in this protocol?

   (d) Consider the following distribution P_{XY}: X is uniformly random in $\{0,1\}^n$, and Y is such that for each $i \in \{1, \ldots, n\}$, $Y_i = X_i$ with probability $1 - \delta$ and $Y_i = 1 - X_i$ otherwise. What is $H_{max}(X|Y)$?

(e) For $\varepsilon' > 0$, show that there is a distribution P'_{XY} such that $\|P'_{XY} - P_{XY}\|_{TV} \leq \varepsilon'$ but, for P', $H_{max}(X|Y) \approx C(\delta)n$ for some $C(\delta)$ that you can compute (or show an upper bound on) and that goes to zero as $\delta \to 0$.

(f) Argue that in this situation, where $(x, y) \sim P_{XY}$, it is possible to execute the protocol using the parameter k that would be computed from the distribution P' and still obtain a protocol that remains $(\varepsilon + \varepsilon')$-correct.