CS 276: Homework 1

Due Date: Sunday, Feb 15, 2026 at 8:59pm via Gradescope

Usage of LLMs/Generative AI tools is prohibited. Other online resources (textbooks/lecture notes) are permissible.

1. Let f be a length-preserving one way function $f : \{0,1\}^n \to \{0,1\}^n$. Given $k > 0$, use f to build a one way function g such that g^k is a secure one-way function but g^{k+1} is insecure.

2. Suppose one way permutations exist. Does there exist a one-way permutation $f : \{0,1\}^n \to \{0,1\}^n$ with a fixed point, i.e. $f(0^n) = 0^n$?

3. Prove or disprove the following:

   (a) Let F be a pseudorandom generator. Then, $G(s) := F(s) \oplus F(\bar{s})$ is also a pseudorandom generator.

   (b) Let $F = \{F_k\}$ be a pseudorandom function family with key length equal to input length. Then, $G_k(x) := F_{F_k(x)}(x)$ is a also pseudorandom function.

   (c) Let $F = \{F_k\}$ be a pseudorandom function family with key length equal to input length. Then, $G_k(x) := F_{F_x(k)}(x)$ is also a pseudorandom function.

4. Construct a *puncturable* PRF from a PRG $G : \{0,1\}^n \to \{0,1\}^{2n}$. (Write down the description of F in terms of G, describe the $\mathsf{puncture}$ and eval algorithms, and show that it satisfies the security definition below)
   A PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is called *puncturable* if

   - $\exists$ PPT algorithms
     $\mathsf{puncture}(k, x)$ that outputs a punctured key k_{-x},
     $\mathsf{eval}(k_{-x}, x)$ such that $\mathsf{eval}(k_{-x}, x') = F_k(x')\ \forall\, x' \neq x$.
   - For all x, even given the punctured key, $F_K(x)$ is still (computationally) indistinguishable from random, i.e.,
     for uniform random variables K, U_n

$$(\mathsf{puncture}(K, x), F_K(x)) \approx_c (\mathsf{puncture}(K, x), U_n)$$