EE 720: Introduction to Number Theory and Cryptography (Autumn 2026)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 2: 20 points Date: August 17, 2026

1. [10 points] Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a pseudorandom generator with expansion factor $l(n) > n$. **Prove or disprove** that the following functions are pseudorandom generators where $s \in \{0,1\}^n$ and s_i is the ith bit of s. The $\|$ denotes the string concatenation operator.
   (a) $G_1(s) = G(s)\|0$.
   (b) $G_2(s) = G(s_1, s_2, \ldots, s_{|s|-1})\|s_{|s|}$.
   (c) $G_3(s) = G(s\|0)$.

2. [10 points] Let F be a length-preserving pseudorandom function having key length, input length, and output length all equal to n bits. Consider the following keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \mapsto \{0,1\}^{2n}$ defined as

$$F'_k(x) = F_k(0\|x)\|F_k(x\|1).$$

   Prove that the F' is **not** a pseudorandom function. Here $F'_k(x) = F'(k,x)$, $F_k(y) = F(k,y)$, and $\|$ is the string concatenation operator.

   Note 1: All pseudorandom functions are not necessarily length-preserving. We defined pseudorandomness for length-preserving functions in class just for the sake of convenience. See the note below for the definition of pseudorandomness for F'.

   Note 2: F' is a pseudorandom function if for any PPT distinguisher D, there is a negligible function $\texttt{negl}$ such that:

$$\left|\Pr\left[D^{F'_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| \leq \texttt{negl}(n),$$

   where the first probability is taken over uniform choice of $k \in \{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $f \in \texttt{Func}_{n-1,2n}$ and the randomness of D. The set $\texttt{Func}_{n-1,2n}$ is the set of all functions with domain equal to $\{0,1\}^{n-1}$ and range equal to $\{0,1\}^{2n}$. By $D^{F'_k(\cdot)}(1^n)$ and $D^{f(\cdot)}(1^n)$, we mean distinguishers D who have oracle access to F'_k and f respectively.