CS 435: Introduction to Cryptography **Spring 2020**

Homework 3

Professor Somesh Jha **Due:** March 11

1. Let G and F be PRGs. Prove that $F \circ G$ (where $\circ$ is function composition) is also a PRG.

2. Let G and F be PRGs. Is (F, G) a PRG? Note that $(F, G)(s)$ is $(F(s), G(s))$. Please justify your answer.

3. **Exercise 3.6**

   Let G be a pseudorandon generator with expansion factor $\ell(n) > 2n$. In each of the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

   (a) Define $G'(s) \stackrel{\text{def}}{=} G(s_1 \cdots s_{\lfloor n/2 \rfloor})$, where $s = s_1 \cdots s_n$.

   (b) Define $G'(s) \stackrel{\text{def}}{=} G(0^{|s|} \| s)$.

   (c) Define $G'(s) \stackrel{\text{def}}{=} G(s) \,\|\, G(s+1)$.

   (Note that given a real number x, the floor function $\lfloor x \rfloor$ gives the largest integer less than or equal to x.)

4. **Exercise 3.13**

   Consider the following keyed function F: For security parameter n, the key is an $n \times n$ boolean matrix A and an n-bit boolean vector b. Define $F_{A,b} = \{0,1\}^n \to \{0,1\}^n$ by $F_{A,b}(x) \stackrel{\text{def}}{=} Ax + b$, where all operations are done modulo 2. Show that F is not a pseudorandom function.