CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 3

Deadline: September 28; 2020, 11:59 AM EST

1 Pseudorandom Generators

1. (15 points) Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a PRG. Consider a function $H : \{0,1\}^n \to \{0,1\}^{6n}$ that works as follows:

   $$H(s) : \text{First compute } s_1||s_2||s_3 \coloneqq G(s), \text{ then compute and output } G(s_1)||G(s_3)$$

   Prove via reduction that $H(\cdot)$ also a PRG.

2 One-Way Functions

Let $f : \{0,1\}^n \to \{0,1\}^n$ be any one-way function. Prove via reduction or disprove (by building an efficient inverter) each of the following statements.

1. (10 Points) Can a function that leaks some bits of the input still be a OWF? More precisely, let $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be s.t. for every $x_1||x_2 \in \{0,1\}^{2n}$, $|x_1| = |x_2|$, $f'(x_1||x_2) = f(x_1)||x_2$. Then is f' also a one-way function?

2. (10 Points) Let $f' : \{0,1\}^{2n} \to \{0,1\}^n$ be s.t. for every $x_1||x_2 \in \{0,1\}^{2n}$, $|x_1| = |x_2|$, $f'(x_1||x_2) = f(x_1) \oplus x_2$. Then f' is also a one-way function.

3 Bonus Question

1. (15 points) We will later see in the course that one-way functions are sufficient for (i.e., imply) PRGs. Here, you must prove that they are *necessary* (i.e., PRGs imply one-way functions).

   Let $g : \{0,1\}^n \to \{0,1\}^{2n}$ be a length-doubling PRG. Prove that g is also a one-way function.