CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 2

Deadline: September 28; 2022, 1:30PM EST

1 Negligible Functions

(a) (10 points) Prove that $2^{-\omega(\log n)}$ is a negligible function for any $n \in \mathbb{N}$.

(b) (10 points) Give an example f and g which are both negligible, but where $f(n)/g(n)$ is not negligible.

2 Hybrid Lemma

(10 points) For integers $a \leq b$, let $U_{a,b}$ denote the uniform distribution over the integers x, $a \leq x \leq b$. Now consider the following two distributions:

1. $U_{0,2^n-1}$
2. $U_{2^n,2^{n+1}-1}$

Consider the following proof via hybrid argument to establish that $U_{0,2^n-1}$ and $U_{2^n,2^{n+1}-1}$ are indistinguishable: For $0 \leq i \leq 2^n$, let $H_i = U_{i,2^n-1+i}$. Clearly, $H_0 = U_{0,2^n-1}$ and $H_{2^n} = U_{2^n,2^{n+1}-1}$. Also, for every i, $H_i \approx H_{i+1}$ because they are statistically close. Therefore, $U_{0,2^n-1} \approx U_{2^n,2^{n+1}-1}$.

Is the above a valid proof? Explain your answer.

3 Pseudorandom Generators

(a) (10 points) Let G_1 and G_2 be PRGs. Is $G(s) = G_1(s)||G_2(s)$ also a PRG? Prove or give a counterexample.

(b) (10 points) Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Consider a function $H : \{0,1\}^n \to \{0,1\}^{4n}$ that works as follows:

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

Is $H(\cdot)$ also a PRG? Prove or give a counterexample.

(c) (15 points) Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a PRG. Consider a function $H : \{0,1\}^{2n} \to \{0,1\}^{4n}$ that works as follows:

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

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

4 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.