CS442: Introduction to Cryptography Instructor: Aarushi Goel

Homework 2

Due: February 22; 2026 (11:59 PM)

1 Negligible/Non-Negligible Functions

For each $n \in \mathbb{N}$, determine whether the following functions are negligible, non-negligible, or neither. Write a proof for your conclusion in each case.

1. **(10 points)** $f(n) = n^5 \cdot g(n)$, where $g : \mathbb{N} \to \mathbb{R}$ is a negligible function.
2. **(10 points)** $f(n) = n^{-1000000000} + 40^{-n}$
3. **(10 points)** $f(n) = g(n)^{-h(n)}$, where $g, h : \mathbb{N} \to \mathbb{R}$ are negligible functions.

2 Hybrid Lemma

(10 points) Recall the hybrid lemma discussed in class: let $\{\mathcal{D}_n^1\}, \ldots, \{\mathcal{D}_n^m\}$ be distributions such that, for every $1 \leq i \leq m-1$, the adjacent ensembles $\{\mathcal{D}_n^i\}$ and $\{\mathcal{D}_n^{i+1}\}$ are computationally indistinguishable. If $m = \mathsf{poly}(n)$, then $\{\mathcal{D}_n^1\}$ and $\{\mathcal{D}_n^m\}$ are also computationally indistinguishable.

Explain why $\{\mathcal{D}_n^1\}$ and $\{\mathcal{D}_n^m\}$ are not guaranteed to be computationally indistinguishable if $m = 2^n$.

3 Pseudorandom Generators

Let $G_1 : \{0,1\}^n \to \{0,1\}^{2n}$ and $G_2 : \{0,1\}^n \to \{0,1\}^{2n}$ be two (possibly different) pseudorandom generators (PRGs). Define a function $G : \{0,1\}^{2n} \to \{0,1\}^{4n}$ by

$$G(s_1 \| s_2) = G_1(s_1) \| G_2(s_2).$$

In this problem, we will prove that G is also a pseudorandom generator.

Proof. The function G is clearly deterministic and expands its input from $2n$ bits to $4n$ bits. To show that G is a PRG, it therefore suffices to prove that its output is pseudorandom. Equivalently, we must show that the following distributions are computationally indistinguishable:

- $\{\, G(s_1 \| s_2);\ s_1 \leftarrow\!\$\ \{0,1\}^n,\ s_2 \leftarrow\!\$\ \{0,1\}^n \,\}$
- $\{\, r \leftarrow\!\$\ \{0,1\}^{4n} \,\}$

We prove this using a hybrid argument. Consider the hybrids:

- $\mathcal{H}_0 \coloneqq \{\, G(s_1 \| s_2);\ s_1 \leftarrow\!\$\ \{0,1\}^n,\ s_2 \leftarrow\!\$\ \{0,1\}^n \,\}$
- $\mathcal{H}_1 \coloneqq \{\, G_1(s_1) \| r_2;\ s_1 \leftarrow\!\$\ \{0,1\}^n,\ r_2 \leftarrow\!\$\ \{0,1\}^{2n} \,\}$
- $\mathcal{H}_2 \coloneqq \{\, r \leftarrow\!\$\ \{0,1\}^{4n} \,\}$

By the hybrid lemma, it suffices to prove that

$$\mathcal{H}_0 \approx_c \mathcal{H}_1 \quad \text{and} \quad \mathcal{H}_1 \approx_c \mathcal{H}_2.$$

1. **(10 points) Explain how the pseudorandomness of G_1 and G_2 implies that $\mathcal{H}_0 \approx_c \mathcal{H}_1$ and $\mathcal{H}_1 \approx_c \mathcal{H}_2$.**

2. **(10 points) Prove via a reduction that $\mathcal{H}_0 \approx_c \mathcal{H}_1$.**

   Hint: Assume toward contradiction that $\mathcal{H}_0$ and $\mathcal{H}_1$ are distinguishable; that is, there exists a non-uniform PPT adversary $\mathcal{A}$ with non-negligible advantage in distinguishing them. Construct a PPT adversary $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine to break the pseudorandomness of G_2, thereby deriving a contradiction.

3. **(10 points) Prove via a reduction that $\mathcal{H}_1 \approx_c \mathcal{H}_2$.**