CS65500: Advanced Cryptography Instructor: Aarushi Goel

Homework 1

Due: January 30; 2025 (11:59 PM)

1 Negligible/Non-Negligible Functions

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

1. **(10 points)** $f(k) = 2^{-\omega(\log k)}$
2. **(10 points)** $f(k) = k^{-1000000000} + 40^{-k}$
3. **(10 points)** $f(k) = g(k)^{-h(k)}$, where $g, h : \mathbb{N} \to \mathbb{R}$ are negligible functions.

2 Indistinguishability

For each $k \in \mathbb{N}$, let $\{A_k\}$ and $\{B_k\}$ be statistically indistinguishable distribution ensembles. Determine whether the following statements are true or false and write a proof to support your claim.

1. **(5 points)** For all non-uniform PPT M, $\{M(A_k)\}$ and $\{M(B_k)\}$ are also statistically indistinguishable.
2. **(5 points)** For all M, $\{M(A_k)\}$ and $\{M(B_k)\}$ are also statistically indistinguishable.

3 Proofs by Reduction

Determine whether the following functions are pseudorandom generators (PRGs). If they are, provide a proof by reduction; otherwise, present a counterexample.

1. **(15 points)** $G(s) = G_2(G_1(s))$, where $G_1 : \{0,1\}^k \to \{0,1\}^{2k}$ and $G_2 : \{0,1\}^{2k} \to \{0,1\}^{2k+1}$ are distinct PRGs.
2. **(15 points)** $G(s) = \begin{cases} G_1(s) & \text{if } s \text{ is odd,} \\ G_1(s) & \text{if } s \text{ is even.} \end{cases}$, where $G_1 : \{0,1\}^k \to \{0,1\}^{2k}$ and $G_2 : \{0,1\}^k \to \{0,1\}^{2k}$ are distinct PRGs.