Homework 2

Posted: Wednesday, October 11, 2023 – 11:59pm
Due: Wednesday, October 18, 2023 – 11:59pm

Task 1 – Negligible Functions (10 points)

The goal of this task is to develop a better sense about negligible functions. Let $\mathbb{R}_{\geq 0}$ be the set of non-negative real numbers. Recall that a function $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ being *negligible* means that for all $d \geq 1$, there exists k_0 (dependent on d) such that for all $k > k_0$, it holds that $f(k) < k^{-d}$.

a) [4 points] Is the function

$$f(k) = k^{-\log^2(k)}$$

negligible? Prove your answer. (The logarithm has base 2.)

b) [6 points] Let $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$ be negligible functions and $c > 0$ a positive constant. Prove that the following functions are also negligible:

$$\textbf{(i)}\ h_1(k) = f(k) + g(k), \qquad \textbf{(ii)}\ h_2(k) = k^c f(k).$$

Task 2 – Block Ciphers (10 points)

The purpose of this task is to illustrate that it is always possible to break a block cipher (and as you will see later, most cryptographic objects) with a *huge* amount of computing resources.

Consider a block cipher $\mathsf{E} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, and the following distinguisher D for distinguishing $\mathsf{KF}[\mathsf{E}]$ from $\mathsf{RP}[n]$:

distinguisher D^{O}:
$Y_0 \leftarrow \mathsf{O.Eval}(0^n)$
$Y_1 \leftarrow \mathsf{O.Eval}(1^n)$
for all $K' \in \{0,1\}^n$ **do**
  if $\mathsf{E}(K', 0^n) = Y_0$ and $\mathsf{E}(K', 1^n) = Y_1$ **then**
    return 1
return 0 (if the loop ends without returning)

a) [2 points] What is the probability that D outputs 1 when given access to the oracle $\mathsf{O} = \mathsf{KF}[\mathsf{E}]$ which evaluates the block cipher E under a random uniform key?

b) [6 points] Give an upper bound on the probability that D outputs 1 when given oracle access to $\mathsf{O} = \mathsf{RP}[n]$. What is the advantage $\mathsf{Adv}^{\mathrm{prp}}_{\mathsf{E}}(D)$?

Hint: What is the probability that $\mathsf{E}(K', 0^n) = Y_0$ and $\mathsf{E}(K', 1^n) = Y_1$ for *some* $K' \in \{0,1\}^n$ when D interacts with $\mathsf{O} = \mathsf{RP}[n]$? For how many $Y_0, Y_1 \in \{0,1\}^n$ does there exist a key K' with $\mathsf{E}(K', 0^n) = Y_0$ and $\mathsf{E}(K', 1^n) = Y_1$?

c) [2 points] Explain why the above distinguisher does not contradict the existence of secure pseudorandom permutations.

Task 3 – IND-CPA Security (9 points)

Let $\Pi = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption scheme with *deterministic* Enc, whose message space is the set of n-bit strings.

a) [5 points] Show that Π *cannot* be IND-CPA secure. In particular, explicitly describe an efficient distinguisher D for which $\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\Pi}(D) = 1$.

b) [3 points] Argue that perfect secrecy of Π implies $\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\Pi}(D) = 0$ *for all* one-query distinguishers, even inefficient ones.

c) [1 points] Given the one-time pad is deterministic, why does **b)** not contradict **a)**?

Task 4 – More IND-CPA Security (8 points)

Let $\Pi = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure symmetric encryption scheme with message space $\mathcal{M}$. Define a new symmetric encryption scheme $\Pi' = (\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ with $\mathsf{Kg}' = \mathsf{Kg}$ and $\mathsf{Enc}'(K, M)$ first running $\mathsf{Enc}(K, M)$ to obtain C then outputting $C' = C \| 0$, where $\|$ denotes string concatenation.

a) [2 points] Describe a suitable Dec' so that Π' is correct (assuming Π is correct).

b) [6 points] Show that Π' is IND-CPA secure.

Hint: Show that for every distinguisher D (against the IND-CPA security of Π'), there exists a distinguisher D' (against the IND-CPA security of Π) such that D' is roughly as efficient as D and they have the same advantage, i.e., $\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\Pi'}(D) = \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\Pi}(D')$.

Task 5 – Pseudorandom Functions (8 points)

Let $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a PRF and define the keyed function

$$\begin{aligned} &\mathsf{H} : \{0,1\}^{2k} \times \{0,1\}^{3n} \to \{0,1\}^n, \\ &\mathsf{H}(K_1 \| K_2, x_1 \| x_2 \| x_3) = \mathsf{E}(K_1, x_1) \oplus \mathsf{E}(K_2, x_1 \oplus x_2 \oplus x_3) \oplus \mathsf{E}(K_2, x_3) \\ &\qquad \text{for } K_1, K_2 \in \{0,1\}^k \text{ and } x_1, x_2, x_3 \in \{0,1\}^n. \end{aligned}$$

Prove that H is *not* a PRF. To this end, solve the following two sub-tasks.

a) [3 points] Find $(x_1, x_2, x_3) \neq (x_1', x_2', x_3')$ such that

$$\mathsf{H}(K_1 \| K_2, x_1 \| x_2 \| x_3) = \mathsf{H}(K_1 \| K_2, x_1' \| x_2' \| x_3')$$

for all $K_1, K_2 \in \{0,1\}^k$.

b) [5 points] Use **a)** to devise a distinguisher D such that $\mathsf{Adv}^{\mathsf{prf}}_{\mathsf{H}}(D)$ is large.