CS 601.442/642 – Modern Cryptography Instructors: Aditya Hegde and Harry Eldridge

Homework 2 Solutions

Problems

1. (50 points) For each function $g(\lambda)$ below, prove or disprove if $g(\lambda)$ is negligible.

   (a) (25 points) Let $f(\lambda) \in \omega(\log \lambda)$ and $g(\lambda) = 2^{-f(\lambda)}$.

   Solution By the definition of ω, we have that for all $c \in \mathbb{N}$ there exists $n_0 \in \mathbb{N}$ such that $\forall \lambda > n_0$, $\log(\lambda) < c \cdot f(\lambda)$. We then have that $\forall c$ and $\forall \lambda > n_0$:

$$\begin{aligned} g(\lambda) &= 2^{-f(\lambda)} \\ &< 2^{-c \cdot \log(\lambda)} \\ &= \frac{1}{\lambda^c} \end{aligned}$$

   which is the definition of negligible, and so $g(\lambda)$ is negligible.

   (b) (25 points)

$$g(\lambda) = \begin{cases} \lambda^{-100} & \text{if } \lambda \text{ is even} \\ 2^{-\lambda} & \text{otherwise} \end{cases}.$$

   Solution By the definition of a negligible function, it must be the case that $\forall c$ and $\forall \lambda > \Lambda$, $g(\lambda) \leq \frac{1}{\lambda^c}$. Let $c = 101$, and consider some value Λ. If Λ is even, we have that $g(\Lambda+2) = \lambda^{-100} > \frac{1}{\lambda^c}$. If Λ is odd, we have that $g(\Lambda+1) = \lambda^{-100} > \frac{1}{\lambda^c}$.
   Therefore, there exists a c such that there does *not* exist a value Λ for which all $\lambda > \Lambda$, $g(\lambda) \leq \frac{1}{\lambda^c}$, and so $g(\lambda)$ is not negligible.

2. (50 points) Recall that two ensembles $X = \{X_i\}_{i \in \mathbb{N}}$ and $Y = \{Y_i\}_{i \in \mathbb{N}}$ are computationally indistinguishable, denoted by $X \overset{c}{\approx} Y$, if for all non-uniform PPT adversaries $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that for all $\lambda \in \mathbb{N}$,

$$\left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 1\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 1\right]\right| \leq \nu(\lambda),$$

   where the probability is over the choice of x, y and randomness of $\mathcal{A}$.

   (a) (25 points) Show that if $X \overset{c}{\approx} Y$ then for all non-uniform PPT adversaries $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that for all $\lambda \in \mathbb{N}$,

$$\left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 0\right]\right| \leq \nu(\lambda),$$

   where the probability is over the choice of x, y and randomness of $\mathcal{A}$.

   Solution
   As we are given that $X \overset{c}{\approx} Y$, we have that:

$$\begin{aligned} \left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 1\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 1\right]\right| &\leq \nu(\lambda) \\ \left|\left(1 - \Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right]\right) - \left(1 - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 0\right]\right)\right| &\leq \nu(\lambda) \\ \left|- \Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right] + \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 0\right]\right| &\leq \nu(\lambda) \\ \left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 0\right]\right| &\leq \nu(\lambda) \end{aligned}$$

   Where $\nu(\lambda)$ is a negligible function.

(b) (25 points) Let $X \overset{c}{\approx} Y$. What is the maximum value of

$$\left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 1\right]\right|$$

for any non-uniform PPT adversary $\mathcal{A}$?

Solution

We fist consider the maximum value of the expression for *any* adversary. As the two quantities are probabilities, they each have a maximum value of 1. Therefore, the maximum value of the expression is also 1.

Consider the adversary $\mathcal{A}(1^\lambda, v)$ that always outputs 0. $\mathcal{A}$ is clearly NUPPT (in fact it runs in constant time).

As $\mathcal{A}$ always outputs 0, we have that $\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right] = 1$, and that $\Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 1\right] = 0$. We therefore have that for $\mathcal{A}$:

$$\begin{aligned} \left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 1\right]\right| &= \\ |1 - 0| &= \\ 1 & \end{aligned}$$

As we previously determined that 1 is the maximum value of the expression, and we have shown that there exists an NUPPT adversary $\mathcal{A}$ such that the expression takes the value 1, we can conclude that the answer is 1.