Homework 3

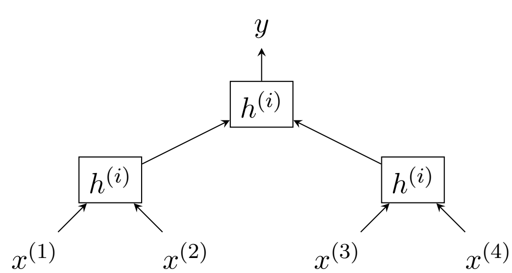
1. (10 + 10 points) Let DDH assumption hold over the multiplicative group $G = \{g^0, g, \dots, g^{|G|-1}\}$, where g is a generator for the group.

   (a) Prove that the distributions $(g, g^x, g^y, g^{xy}) \approx^{(c)} (g, g^x, g^y, g^z)$, where $x, y, z \xleftarrow{\$} \{1, \dots, |G|-1\}$.

   (b) Prove that the distributions $(g, g^x, g^y, g^{x/y}) \approx^{(c)} (g, g^x, g^y, g^z)$, where $x, y, z \xleftarrow{\$} \{1, \dots, |G|-1\}$. (Here x/y is computed over $\mathbb{Z}^*_{|G|}$)

2. (10 + 15 points) Let $\mathcal{H} = \{h^{(i)} : i \in I\}$ be a CRHF family, where I is the set of indices for the functions and $h^{(i)} : \{0,1\}^{2n} \to \{0,1\}^n$.

   (a) Define $h^{(2,i)} : \{0,1\}^{4n} \to \{0,1\}^n$, for $i \in I$, as follows. For an input $x \in \{0,1\}^{4n}$, interpret it as a concatenation of 4 blocks of n-bit strings $(x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)})$. The output $y = h^{(2,i)}(x)$ is defined by



   Prove that $\mathcal{H}^{(2)} = \{h^{(2,i)} : i \in I\}$ is a CRHF family.

   (b) Intuitively, the construction above interprets the input as blocks of length n. Then it embeds a balanced binary tree such that the leaves correspond to these input-blocks. At each interior node of the balanced binary tree, the construction applies $h^{(i)}$ to compresses the two incoming inputs. The output of the function is the output of the hash function at the root.

   Extend the above intuition to construct $h^{(t,i)} : \{0,1\}^{2^t \cdot n} \to \{0,1\}^n$. Prove that $\mathcal{H}^{(t)} = \{h^{(t,i)} : i \in I\}$ is a CRHF family. For this problem interpret t as an constant integer $\geqslant 2$.

3. (25 points) Let $\mathcal{H} = \{h^{(i)} \colon i \in I\}$ is a *universal one-way hash function* (UOWHF) family if $h^{(i)} \colon \{0,1\}^{2n} \to \{0,1\}^n$, for all $i \in I$, and the following definition holds.

For an arbitrary efficient adversary $\mathcal{A}$ the following is true:

(a) The adversary $\mathcal{A}$ sends $x \in \{0,1\}^{2n}$

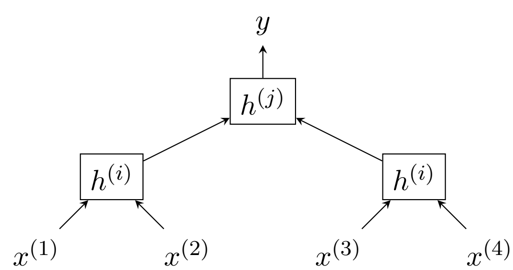
(b) The honest challenger $\mathcal{H}$ picks $i \in I$ and sends $h^{(i)}$ to the adversary $\mathcal{A}$

(c) The adversary $\mathcal{A}$ replies with $x' \in \{0,1\}^{2n}$

(d) The honest challenger outputs $z = 1$ if $h^{(i)}(x) = h^{(i)}(x')$

We have $\Pr[z = 1] \leqslant \mathsf{negl}(n)$ in the above experiment.

Define $h^{(2,i,j)} \colon \{0,1\}^{4n} \to \{0,1\}^n$, for $i, j \in I$, as follows. For an input $x \in \{0,1\}^{4n}$, interpret it as a concatenation of 4 blocks of n-bit strings $(x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)})$. The output $y = h^{(2,i,j)}(x)$ is defined by



Prove that $\mathcal{H}^{(2)} = \{h^{(2,i,j)} \colon i, j \in I\}$ is a UOWHF family.