# CS 171: Discussion Section 4 (2/12)

## 1 Pseudorandom Functions

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. For each of the candidates below prove whether it is pseudorandom or not.

1. $f'_k(x) = f_k(x) \parallel f_k(\overline{x})$ where $\overline{x}$ flips all the bits of $x$.
2. $f'_{(k_1,k_2)}(x) = f_{k_1}(x) \parallel f_{k_2}(x)$.

**Solution**

1. No. Query the oracle on $x$ and $\overline{x}$ and when the oracle is the function $f'$, the answers will be $y_1 \parallel y_2$ and $y_2 \parallel y_1$ respectively. On the other hand, on a random function the answers will not be of this form except with probability $1/2^{2n}$.
2. Yes. We will show this via a hybrid argument.
   - $\mathsf{Hyb}_0(x) := f_{k_1}(x) \parallel f_{k_2}(x)$.
   - $\mathsf{Hyb}_1(x) := R_1(x) \parallel f_{k_2}(x)$ where $R_1$ is a random function.
   - $\mathsf{Hyb}_2(x) := R_1(x) \parallel R_2(x)$ where $R_1, R_2$ are random functions.

   **Claim 1.1.** *For any polynomial time distinguisher $D$,*

   $$|\Pr[D^{\mathsf{Hyb}_0(\cdot)}(1^n) = 1] - \Pr[D^{\mathsf{Hyb}_1(\cdot)}(1^n) = 1]| \leq \mathsf{negl}(n)$$

   *Proof.* Assume for the sake of contradiction that there exists an adversary $D$ that distinguishes between oracle access to the functions in $\mathsf{Hyb}_1$ and $\mathsf{Hyb}_0$ with non-negligible advantage. We will construct an adversary $D'$ against the pseudorandomness property of $f_{k_1}$. $D'$ samples $k_2$ randomly. $D'$ runs $D$ and on any oracle query $x$ made by $D$, $D'$ queries its own oracle on $x$ to get $y$. $D'$ returns $y \parallel f_{k_2}(x)$. It is easy to see that $D'$ runs in polynomial time since $D$ runs in poly time.

   If $D'$ has been given access to the $f_{k_1}$ oracle then its oracle responses are identically distributed to $\mathsf{Hyb}_0(\cdot)$. Otherwise the responses are distributed identically to $\mathsf{Hyb}_1(\cdot)$. Hence the advantage of $D'$ distinguishing oracle access to $f_{k_1}()$ and the random oracle is same as the advantage of $D'$ in distinguishing between oracle access to $\mathsf{Hyb}_0$ from $\mathsf{Hyb}_1$, and this is assumed to be non-negligible. A contradiction. □

   **Claim 1.2.** *For any polynomial time distinguisher $D$,*

   $$|\Pr[D^{\mathsf{Hyb}_1(\cdot)}(1^n) = 1] - \Pr[D^{\mathsf{Hyb}_2(\cdot)}(1^n) = 1]| \leq \mathsf{negl}(n)$$

   *Proof.* Assume for the sake of contradiction that there exists an adversary $D$ that distinguishes between oracle access to the functions in $\mathsf{Hyb}_1$ and $\mathsf{Hyb}_2$ with non-negligible advantage. We will construct an adversary $D'$ against the pseudorandomness property of $f_{k_2}$. $D'$ runs $D$ and on any oracle query $x$ made by $D$, $D'$ queries its own oracle on $x$ to get $y$. $D'$ returns $r \parallel y$ where $r$ is an uniformly chosen random string. It stores

$(x, r)$ and the next time $D$ queries $x$, it uses the stored value to answer this query. It is easy to see that $D'$ runs in polynomial time since $D$ runs in poly time.

If $D'$ has been given access to the $f_{k_2}$ oracle then its oracle responses are identically distributed to $\mathsf{Hyb}_1(\cdot)$. Otherwise the responses are distributed identically to $\mathsf{Hyb}_2(\cdot)$. Hence the advantage of $D'$ distinguishing oracle access to $f_{k_2}()$ and the random oracle is same as the advantage of $D'$ in distinguishing between oracle access to $\mathsf{Hyb}_1$ from $\mathsf{Hyb}_2$, and this is assumed to be non-negligible. A contradiction. □

□

## 2 Psuedorandom Permutations

Assume that pseudorandom permutations exist. Show that there exists a function that is a pseudorandom permutation but not a *strong* pseudorandom permutation.

**Solution** Let $F$ be a pseudorandom permutation. We now define another permutation $F'$ such that

$$F'_k(x) := \left\{ \begin{array}{ll} 0^n, & \text{for } x = k \\ F_k(k), & \text{for } x = F^{-1}(0^n) \\ F_k(x), & \text{otherwise} \end{array} \right\}$$

**Claim 2.1.** *$F'$ is a pseudorandom permutation.*

*Proof.* Assume for the sake of contradiction that $F'$ is a not a pseudorandom permutation. That is, there exists an attacker $\mathcal{A}$ such that for all negligible functions $\mathsf{negl}(n)$,

$$|\Pr[\mathcal{A}^{F'_k(\cdot)}(1^n) = 1] - \Pr[\mathcal{A}^{R(\cdot)}(1^n) = 1]| \geq \mathsf{negl}(n)$$

where $R$ is a random permutation. We will show that such an attacker can be used to contradict the pseudorandomness of $F$.

Let $\mathcal{B}$ be an attacker against the pseudorandomness of $F$. $\mathcal{B}$ runs $\mathcal{A}$ internally and then uses its oracle $F(\cdot)$ to answer all of $\mathcal{A}$'s queries. Finally, $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs. We now arugue that the probability that $\mathcal{A}$ outputs when 1 when given access to $F'$ is the same as the probability that $\mathcal{B}$ outputs 1 when given access to $F$. Notice that the only difference between $F$ and $F'$ is on two inputs, $k$ and $F_k^{-1}(0^n)$. As long as $\mathcal{A}$ does not make a query on these two points, it follows that $\mathcal{B}$'s responses to $\mathcal{A}$'s queries are consistent with $F'$. But if $\mathcal{A}$ makes any of these two queries, then $\mathcal{B}$ can use these two queries to distinguish between $F$ and the random permutation. Thus, $\mathcal{B}$ contradicts the pseudorandomness of $F$. □

It can be easily seen that $F'$ is not a strong pseudorandom permutation as we can query that inversion oracle on $0^n$ to learn the key $k$.

□