CS 435: Introduction to Cryptography **Fall 2016-17**

Homework 3 Solutions

Professor Somesh Jha

1. We are given that G, F are pseudorandom generators. Let G be a P.R.G. that on inputs of length n returns a string of length $\ell_G(n)$, and F be a P.R.G. that returns strings of length $\ell_F(n)$ on inputs of length n. Let $\ell(n) = \ell_F(\ell_G(n))$. We need to prove that $F \circ G$ is a P.R.G., i.e. we need to show that for any PPT algorithm D,

$$| \Pr_{s \in \{0,1\}^n}[D(F(G(s))) = 1] - \Pr_{r \in \{0,1\}^{\ell(n)}}[D(r) = 1] | \leq \text{negl}(n).$$

Let D be an arbitrary PPT algorithm. Then,

$$\begin{aligned}
&| \Pr_{s \in \{0,1\}^n}[D(F(G(s))) = 1] - \Pr_{r \in \{0,1\}^{\ell(n)}}[D(r) = 1] | \\
=& | \Pr_{s \in \{0,1\}^n}[D(F(G(s))) = 1] - \Pr_{z \in \{0,1\}^{\ell_G(n)}}[D(F(z)) = 1] \\
+& \Pr_{z \in \{0,1\}^{\ell_G(n)}}[D(F(z)) = 1] - \Pr_{r \in \{0,1\}^{\ell(n)}}[D(r) = 1] | \\
\leq& | \Pr_{s \in \{0,1\}^n}[D(F(G(s))) = 1] - \Pr_{z \in \{0,1\}^{\ell_G(n)}}[D(F(z)) = 1] | \\
+& | \Pr_{z \in \{0,1\}^{\ell_G(n)}}[D(F(z)) = 1] - \Pr_{r \in \{0,1\}^{\ell(n)}}[D(r) = 1] |
\end{aligned}$$

The final inequality follows by the triangle inequality. Now, since F is a P.R.G. and D is a PPT algorithm, $| \Pr_{z \in \{0,1\}^{\ell_G(n)}}[D(F(z)) = 1] - \Pr_{r \in \{0,1\}^{\ell(n)}}[D(r) = 1] | \leq \text{negl}(n)$. All that is left to do is bound $| \Pr_{s \in \{0,1\}^n}[D(F(G(s))) = 1] - \Pr_{z \in \{0,1\}^{\ell_G(n)}}[D(F(z)) = 1] |$ by a negligible function. Recall that every P.R.G. is a deterministic polynomial time algorithm (See Definition 3.14 of the textbook). As a result, the output of $D(F(.))$ on any given input can be computed by PPT algorithm (on input z, first compute $F(z)$ and then feed $F(z)$ into D to get $D(F(z))$). Since G is a P.R.G., we have $| \Pr_{s \in \{0,1\}^n}[D(F(G(s))) = 1] - \Pr_{z \in \{0,1\}^{\ell_G(n)}}[D(F(z)) = 1] | \leq \text{negl}(n)$.

By the closure property of negligible functions,

$$| \Pr_{s \in \{0,1\}^n}[D(F(G(s))) = 1] - \Pr_{r \in \{0,1\}^{\ell(n)}}[D(r) = 1] | \leq \text{negl}(n).$$

Since D was an arbitrary PPT distinguisher, this proves that $F \circ G$ is indeed a P.R.G..

2. $(F, G)(s) = (F(s), G(s))$ is not necessarily a P.R.G. when F and G are P.R.G.s. To see this set $F = G$. In this case (F, G) always outputs a string with the same first and second half.

A PPT distinguisher can exploit this structure to distinguish the output of (F, G) from a truly random string. Take D to be the algorithm that returns 1 if the input is a string with the first and second halves equal, and 0 otherwise. Then, $\Pr[D((F, G)(s)) = 1]$ is 1, while $\Pr[D(r) = 1]$ is $2^{-n/2}$. This tells us that D succeeds in distinguishing the output of (F, G) from a truly random string. As a result (F, G) is not a P.R.G..

3. Consider the following distinguisher D:
   D is given input 1^n and access to oracle $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$.

   (a) Picks two distinct strings x_1 and x_2 from $\{0,1\}^n$.

   (b) Query the oracle on these strings to obtain $y_1 = \mathcal{O}(x_1)$ and $y_2 = \mathcal{O}(x_2)$.

   (c) If $y_1 \oplus y_2 = x_1 \oplus x_2$ output 1. Output 0 otherwise.

   We claim that D distinguishes F_k from a truly random function. If $\mathcal{O} = F_k$ then D outputs 1 with probability 1 . On the other hand if $\mathcal{O}$ is a truly random function f, then the probability that D outputs 1 is the same as the probability that two random strings $y_1, y_2 \in \{0,1\}^n$ satisfy $y_1 \oplus y_2 = x_1 \oplus x_2$ (why?).

$$
\begin{aligned}
&\Pr_{y_1,y_2}[y_1 \oplus y_2 = x_1 \oplus x_2] \\
&= \Pr_{y_1,y_2}[y_1 = x_1 \oplus x_2 \oplus y_2] \\
&= \sum_{z \in \{0,1\}^n} \Pr[y_1 = z \text{ and } x_1 \oplus x_2 \oplus y_2 = z] \\
&= \sum_{z \in \{0,1\}^n} \Pr[y_1 = z \text{ and } y_2 = x_1 \oplus x_2 \oplus z] \\
&= \sum_{z \in \{0,1\}^n} 1/2^{2n} = 1/2^n.
\end{aligned}
$$

   Therefore, the distinguisher succeeds with advantage $\mid 1 - 2^{-n} \mid$, which is not negligible.

4. We present a proof by contradiction. Assume that G is not a P.R.G., which means there is a distinguisher A and a polynomial $p(n)$ such that for every n,

$$
\mid \Pr_{\{0,1\}^n}[A(G(s)) = 1] - \Pr_{r \in \{0,1\}^{\ell n}}[A(r) = 1] \mid \geq 1/p(n).
$$

   We use A to construct a distinguisher D that distinguishes between F_s and a random function f. Consider the following distinguisher D:
   D is given input 1^n and access to oracle $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$.

   (a) D queries $\mathcal{O}$ on the inputs $1, 2, \ldots \ell$. To get $\mathcal{O}(1), \ldots \mathcal{O}(\ell)$.

   (b) Run A on the string $\mathcal{O}(1) \| \mathcal{O}(2) \| \ldots \| \mathcal{O}(\ell)$.

   Observe that if D is given F_s as the oracle, then D runs A on $G(s)$. Which implies $\Pr_s[D^{F_s(.)}(1^n) = 1] = \Pr[A(G(s)) = 1]$. On the other hand if D is given a random function f as the oracle, then $\Pr[D^f(1^n) = 1] = \Pr_{r \in \{0,1\}^{\ell n}}[A(r) = 1]$. (why?) Therefore, for all n,

$$
\begin{aligned}
&\left| \Pr_s[D^{F_s(\cdot)}(1^n) = 1] - \Pr[D^f(1^n) = 1] \right| \\
&= \left| \Pr_{\{0,1\}^n}[A(G(s)) = 1] - \Pr_{r \in \{0,1\}^{\ell n}}[A(r) = 1] \right| \geq 1/p(n)
\end{aligned}
$$

This contradicts the premise that F_s is a pseudorandom function. Therefore, if F_s is a pseudorandom function then G must be a pseudorandom generator with expansion $\ell \cdot n$.