CS 435: Introduction to Cryptography	**Spring 2020**
Homework 3	
Professor Somesh Jha	**Due:** March 11

1. Let G and F be PRGs. Prove that $F \circ G$ (where $\circ$ is function composition) is also a PRG.

   Solution:

   Let us complete the proof sent by email.

   Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ and $F : \{0,1\}^{2n} \to \{0,1\}^{4n}$ be PRGs, and let D be a PPTA distinguisher.

   World 0: generate an n-bit random seed s and give $F(G(s))$ to D (note that $F(G(s))$ has length $4n$, which is the length of the string r in world 1.)

   World 1: generate a uniform bit string r of length $4n$ and give it to D.

   World I: generate a $2n$-bit random string z and provide $F(z)$ to the distinguisher D ($F(z)$ is a $4n$-bit string).

   Step 1 (difference between world 1 and I): Since F is a PRG, by definition (Definition 3.14) we have that there exists a negligible function $negl_1$ such that

   $$|\Pr[D(r) = 1] - \Pr[D(F(z)) = 1]| \leq negl_1(n).$$

   Step 2 (difference between world I and 0): Consider $D_1 = D \circ F$. Since F is polynomial time, then D_1 is a PPT algorithm. In particular, D_1 is a distinguisher. Now, since G is a PRG, by definition we have that that there exists a negligible function $negl_2$ such that

   $$|\Pr[D_1(z) = 1] - \Pr[D_1(G(s)) = 1]| \leq negl_2(n)$$

   which is the same as

   $$|\Pr[D(F(z)) = 1] - \Pr[D(F(G(s))) = 1]| \leq negl_2(n).$$

   Step 3: It follows from the triangle inequality ($|a-c| + |c-b| \geq |a-b|$) that

   $$|\Pr[D(r) = 1] - \Pr[D(F(G(s))) = 1]| \leq$$
   $$\leq |\Pr[D(r) = 1] - \Pr[D(F(z)) = 1]| + |\Pr[D(F(z)) - \Pr[D(F(G(s))) = 1]|.$$

   It follows from what we proved in Step 1 and 2 that

   $$|\Pr[D(r) = 1] - \Pr[D(F(z)) = 1]| + |\Pr[D(F(z)) - \Pr[D(F(G(s))) = 1]| \leq$$
   $$\leq negl_1(n) + negl_2(n).$$

Therefore $|\Pr[D(r)=1]-\Pr[D(F(G(s)))=1]| \le negl_1(n)+negl_2(n)$. Since the sum of two negligible functions is negligible (Proposition 3.6), we have just proved that there exist a negligible function $negl$ such that

$$|\Pr[D(r)=1]-\Pr[D(F(G(s)))=1]| \le negl(n).$$

That is, $F \circ G$ is a PRG.

2. Let G and F be PRGs. Is (F,G) a PRG? Note that $(F,G)(s)$ is $(F(s),G(s))$. Please justify your answer.

   Solution:

   No. In general, (F,G) is not a PRG.

   Consider the case when $F,G : \{0,1\}^n \to \{0,1\}^{2n}$ and $F=G$. An efficient distinguisher can be defined in the following way: on input a string $w=(w_1,w_2)$ from $\{0,1\}^{2n}\times\{0,1\}^{2n}$, D outputs 1 if and only if $w_1=w_2$. Since this property holds for all the strings output by (F,G), we have

   $$\Pr[D((F,G)(s)))=1]=\Pr[D(F(s),G(s))=1]=1.$$

   On the other hand, if w is uniform, the probability of $w_1=w_2$ is $1/2^{2n}$ (2^{2n} strings out of 2^{4n} possible strings). That is, $\Pr[D(w)=1]=1/2^{2n}$. Therefore

   $$|\Pr[D(F(s),G(s))=1]-\Pr[D(w_1,w_2)=1]=1-1/2^{2n}$$

   which is not a negligible function.

3. **Exercise 3.6**

   Let G be a pseudorandon generator with expansion factor $\ell(n)>2n$. In each of the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

   (a) Define $G'(s) \stackrel{\text{def}}{=} G(s_1\cdots s_{\lfloor n/2\rfloor})$, where $s=s_1\cdots s_n$.

   (b) Define $G'(s) \stackrel{\text{def}}{=} G(0^{|s|}\|s)$.

   (c) Define $G'(s) \stackrel{\text{def}}{=} G(s)\,\|\,G(s+1)$.

   (Note that given a real number x, the floor function $\lfloor x\rfloor$ gives the largest integer less than or equal to x.)

   Solution:

   (a) No, G' is not necessarily a PRG. To see this, assume that $n=2m+1$ (odd integer) and $\ell(n)=2n+1$ then we have $|G'(s)|=2m+1=n$. In other words, the expansion factor of $G' : \{0,1\}^n \to \{0,1\}^n$ does not satisfy Condition 1 in Definition 3.14.

   (b) No, G' is not necessarily a PRG. To see this, let $H : \{0,1\}^n \to \{0,1\}^{3n}$ be a PRG and define $G(s_1||s_2)=H(s_1)$. It can be proven that G is a PRG, $G : \{0,1\}^{2n} \to \{0,1\}^{3n}$. But then $G'(s)=G(0^n||s)=H(0^n)$, and clearly G' is not a pseudorandom generator. On input a string w, an efficient distinguisher D outputs 1 if and only if $w = H(0^n)$. Then

$$|\Pr[D(G'(s)) = 1] - \Pr[D(w) = 1]| = 1 - 1/2^{3n}.$$

Fundamentally, the problem here is that G' runs G on an input that is not uniformly distributed.

(c) No, G' is not necessarily a PRG. To see this, let $H : \{0,1\}^{n-1} \to \{0,1\}^{2n}$ be a PRG and define $G(s) = H(s_1, \ldots, s_{n-1})$. It can be proven that G is a PRG. But then if the last bit of s is 0, we have

$$G'(s) = G(s)||G(s+1) = H(s_1, \ldots, s_{n-1})||H(s_1, \ldots, s_{n-1})$$

because then s and $s+1$ differ only in their final bit. So, with probability $1/2$ the two halves of the output of G' are the same. This is clearly not a pseudorandom generator. On input $w = (w_1, w_2)$, an efficient distinguisher D outputs 1 if and only if $w_1 = w_2$. Then

$$|\Pr[D(G'(s)) = 1] - \Pr[D(w) = 1]| = 1/2 - 1/2^n.$$

Fundamentally, the problem here is that G' runs G on two correlated (rather than independent) inputs.

4. **Exercise 3.13**

Consider the following keyed function F: For security parameter n, the key is an $n \times n$ boolean matrix A and an n-bit boolean vector b. Define $F_{A,b} = \{0,1\}^n \to \{0,1\}^n$ by $F_{A,b}(x) \stackrel{\text{def}}{=} Ax + b$, where all operations are done modulo 2. Show that F is not a pseudorandom function.

Solution:

Let e_i denote the n-bit string with a 1 in position i (and 0s elsewhere). First of all, observe that $F_{A,b}(0^n) = b$ and $F_{A,b}(e_i) = a_i + b$, where a_i is the ith column of the matrix A.

Now consider the following distinguisher D:

1) D queries the oracle $\mathcal{O}$ on the $n+1$ strings $0^n, e_1, \ldots, e_n$ ($n+1$ queries) and then constructs the matrix A and the vector b as $b = \mathcal{O}(0^n)$ and $a_i = \mathcal{O}(e_i) - b$, where a_i is the ith column of the matrix A.

2) D queries the oracle $\mathcal{O}$ on a new string x, let $y = \mathcal{O}(x)$. If $y = Ax + b$, then D outputs 1. Otherwise, D outputs 0.

D is PPTA since it performs only $n+2$ queries. Moreover, if $\mathcal{O} = F_{A,b}$, then for any key (A, b), D outputs 1. On the other hand, if $\mathcal{O} = f$ for f chosen uniformly from $\texttt{Func}_n$, then the probability that $f(x) = Ax + b$ is $\frac{(2^n)^{2^n-1}}{(2^n)^{2^n}} = \frac{1}{2^n}$. Therefore

$$|\Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] = 1 - 1/2^n$$

which is not a negligible function.