Homework 12

Problem 1. Let G be a pseudorandom generator of stretch ℓ such that $\ell(n) \geq 2n$.

(a) Define G' as $G'(s) = G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?

(b) Define G'' as $G''(s) = G(s_1 \cdots s_{n/2})$ for $s = s_1 s_2 \cdots s_n$. Is G'' necessarily a pseudorandom generator?

Solution. (a) Not necessarily. Assume we have a PRG $H\colon \{0,1\}^{n/2} \to \ell(n)$, we construct $G(s) = H(s_1 \dots s_{n/2}) s_{n/2+1} \dots s_n$. Easy to see that $G(s)$ is also a PRG. However $G'(s) = H(s)0^n$ is clearly not a PRG.

(a) Yes. By the security of G, we have that for any PPT adversary $\mathcal{A}$(poly in $n/2$, which is also poly in n), we have

$$|\Pr_s[\mathcal{A}(G(s_1 \dots s_{n/2})) = 1] - \Pr_s[\mathcal{A}(R_{\ell(n/2)}) = 1]| \leq \text{negl}(n/2) = \text{negl}(n).$$

Since $G''(s) = G(s_1 \dots s_{n/2})$, the beyond result also applies.

Problem 2. A keyed family of functions F_k is a pseudorandom random permutation (PRP) if (a) $F_k(\cdot)$ and $F_k^{-1}(\cdot)$ are efficiently computable given the key k and (b) for any polynomial-time algorithm $\mathcal{A}$,

$$\left|\Pr\left(\mathcal{A}^{F_k(\cdot),F_k^{-1}(\cdot)}(1^n) = 1\right) - \Pr\left(\mathcal{A}^{f_n(\cdot),f_n^{-1}(\cdot)}(1^n) = 1\right)\right| \leq \text{negl}(n).$$

Consider the following encryption scheme

1. Sample key k uniformly at random.
2. On input plaintext $x \in \{0,1\}^{n/2}$, algorithm Enc_k samples randomness $r \in \{0,1\}^{n/2}$ and outputs ciphertext $F_k(r\|x)$.

Solve the following problems assuming that F_k is a PRP.

(a) Show how the decryption Dec_k works.

(b) Prove that the encryption scheme is CPA-secure.

Solution. (a) The decryption algorithm runs $F_j^{-1}(\cdot)$ on the ciphertext, and output the second half as the plaintext. (b) The proof is similar to the proof in class. If there is an adversary $\mathcal{A}^{\text{Enc}_k(\cdot)}$ that breaks the IND-CPA security of the encryption protocol, we will also construct an adversary $\mathcal{D}$ that breaks the security of PRP.

The adversary $\mathcal{D}^{F_k(\cdot),F_k^{-1}(\cdot)}$ works as follows:

- It first calls $\mathcal{A}^{\mathrm{Enc}_k(\cdot)}$ and generates two plaintext x_0,x_1. Since we have access to $F_k(\cdot)$, we can simulate $\mathrm{Enc}_k(\cdot) = F_k(r\|\cdot)$.
- It samples $r \leftarrow \{0,1\}^{n/2}, b \leftarrow \{0,1\}$, and sends $F_k(r\|x_b)$ to $\mathcal{A}$.
- $\mathcal{A}$ returns b', $\mathcal{D}$ outputs 1 if $b' = b$.

We note that $\Pr[\mathcal{D}^{F_k(\cdot),F_k^{-1}(\cdot)}(1^n) = 1] = \Pr[\mathcal{A} \text{ succ}] \geq \frac{1}{2} + \frac{1}{\mathrm{poly}(n)}$.

Now we prove that if we replace $F_k(\cdot)$ in $\mathcal{D}$ with a random function f, $\Pr[\mathcal{D}^{f_k(\cdot),f_k^{-1}(\cdot)}(1^n) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$. Assuming $\mathcal{A}$ makes $q(n)$ queries to the oracle f, we can see that if it queries the challenge point $r\|x_b$, it will success with probability 1, otherwise it cannot success better than the random guessing b strategy. Since r is random, it has probability at most $q(n)/2^{n/2}$ to query the challenge point. Thus we have

$$\Pr[\mathcal{D}^{f_k(\cdot),f_k^{-1}(\cdot)}(1^n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^{n/2}}$$

Comparing the two cases, we can see that $\mathcal{D}$ breaks the security of PRP.