CS 171: Discussion Section 3 (Feb 5)

1. Pseudorandom Generators

Let $F, G : \{0,1\}^n \to \{0,1\}^{3n}$ be pseudorandom generators. For each of the functions below, prove or disprove that H is necessarily a pseudorandom generator.

(a) $H(s_0 s_1 \ldots s_{n-1}) := G(s_{n-1} s_{n-2} \ldots s_0)$.

(b) $H(s) := G(s)_{1,\ldots,2n}$ (i.e., the first $2n$ bits of $G(s)$).

(c) $H(s) = G(s) \| F(s)$.

2. Equivalence of Definitions

Consider the following variant of CPA secure definition.

1. A key k is generated by running $\mathsf{Gen}(1^n)$.
2. The adversary $\mathcal{A}$ on input 1^n and oracle access to $\mathsf{Enc}_k(\cdot)$ produces a tuple of messages $(m_{0,1}, \ldots, m_{0,r})$ and $(m_{1,1}, \ldots, m_{1,r})$ where $m_{0,i}$ and $m_{1,i}$ have the same length.
3. A uniform bit $b \in \{0,1\}$ is chosen and for each $i \in [r]$, c_i is generated as $\mathsf{Enc}_k(m_{b,i})$ and the tuple of ciphertexts $(c_1, \ldots, c_r)$ is given to the adversary.
4. The adversary $\mathcal{A}$ continues to have oracle access to $\mathsf{Enc}_k(\cdot)$ and outputs a bit b'.
5. The output of the experiment is defined to be 1 if and only if $b = b'$.

We say that an encryption scheme to be strong CPA secure if for every $\mathcal{A}$ there is a negligible function ν such that:

$$\Pr[PrivK^{S-CPA}_{\mathcal{A},\Pi}(n) = 1] \leq 1/2 + \nu(n)$$

Show that the strong CPA security is equivalent to CPA security.