Tutorial 2: Computational Secrecy and Pseudorandom Generators

Submission Guidelines All problems must be solved in class today. Searching on the internet for solutions is strictly discouraged.

1. Show that semantic security and security in the sense of indistinguishability of ciphertexts are equivalent.

2. Let G be a PRF that stretches n-bit strings to $2n$-bit strings. For $s \in \{0,1\}^n$, write $G(s) = G_0(s)\|G_1(s)$, so that $G_0(s)$ represents the first n-bits of $G(s)$ and $G_1(s)$ represents the last n bits of $G(s)$. Define a new PRG G_0 that stretches n-bit strings to $4n$-bit strings as:

$$G'(s) = G(G_0(s))\|G(G_1(s)).$$

   Prove that if G is a secure PRG, then so is G'.

3. Suppose that G_1 and G_2 are PRGs defined from $\{0,1\}^n$ to $\{0,1\}^\ell$. Define a new PRG $G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\ell$, where $G(s_1, s_2) = G_1(s_1) \oplus G_2(s_2)$. Show that if either G_1 or G_2 is secure (we may not know which one is secure), then G is a secure PRG.

4. Let $G : \{0,1\}^n \to \{0,1\}^\ell$ be a PRG and let $\eta = 1/2^{\ell-n}$. Call G secure against *seed recovery* or (ϵ, t)-SR secure if any t-time adversary $\mathscr{A}$ has advantage at most ϵ in the following game: $\mathscr{A}$ receives $G(s)$ and returns a guess s' of s. Here, advantage $\mathsf{Adv}^{\mathsf{SR}}_{G,\mathscr{A}}$ is defined as $|\Pr[s = s'] - 1/2^n|$. Show that if G is an (ϵ', t')-PRG then it is (ϵ, t)-SR secure with $\epsilon \leq \epsilon' + \eta + 1/2^n$ and $t = t' + O(1)$. This shows that for a secure PRG, it is computationally hard to recover the seed from the output provided that η is small.