

Homework #1

Due: Tuesday, April 28th, 2026, 11:59 PM

For the purpose of this assignment, we will allow the input length of a PRG to be a value other than exactly λ bits. (We still require that the input length depend on λ , and that the output be longer than the input.)

1. Suppose that $G_1: \{0, 1\}^\lambda \rightarrow \{0, 1\}^{3\lambda}$ is a PRG. Show that $H_1: \{0, 1\}^\lambda \rightarrow \{0, 1\}^{2\lambda}$, defined as follows, is *not* a PRG:

$H_1(S)$:
 $A \parallel B \parallel C := G_1(S)$
 $Z := B \wedge C$ // here " $\wedge$ " denotes bitwise and
 return $A \parallel Z$

You will want to give a distinguishing algorithm $\mathcal{A}$ in pseudocode, and to analyze the probability that it returns true when interacting with H and with a truly random string.

Hint: Recall Chernoff bounds. Let X be the number of heads from flipping n biased coins that each show heads with probability p . Then $\Pr[X \geq (1 + \delta)pn] \leq e^{-\delta^2 pn / (2 + \delta)}$.

2. Suppose that $G_2: \{0, 1\}^\lambda \rightarrow \{0, 1\}^{\lambda+\ell}$ is a PRG. Prove that $H_2: \{0, 1\}^{\lambda+1} \rightarrow \{0, 1\}^{\lambda+\ell+1}$, defined as follows, is also a PRG:

$H_2(S)$:
 $B := S[0 : 1]$ // first bit of S
 $X := S[1 : \lambda + 1]$ // last λ bits of S
 return $B \parallel G_2(X)$

The notation means that the first bit of H_2 's output is the first bit of H_2 's seed, and the rest of H_2 's output is whatever G_2 returns given the remaining λ bits of seed.

3. Suppose that $G_3: \{0, 1\}^\lambda \rightarrow \{0, 1\}^{\lambda+\ell}$ is a PRG. Show that $H_3: \{0, 1\}^{2\lambda} \rightarrow \{0, 1\}^{2\lambda+\ell}$, defined as follows, is not necessarily a secure PRG:

$H_3(S)$:
 $X \parallel Y := S$
 return $(X \oplus Y) \parallel (G_3(X) \oplus G_3(Y))$

Specifically, show that (assuming PRGs exist) you can pick a PRG G_3 such that H_3 is not a PRG.

Hint: Try $G_3 = H_2$.