CSA E0 235: Cryptography 27/08/2019

Tutorial 3

Instructor: Arpita Patra *Question Set*

1. We define a PRG $G_c(s) = G_a(s)||G_b(s)$ where $||$ is the concatenation operator. Let G_a, G_b are two different pseudorandom generators i.e., their outputs aren't necessarily the same on all inputs s. Is G_c a pseudorandom generator? Prove or disprove.

2. Suppose $G(s)$ is a secure PRG that outputs bit-strings in $\{0,1\}^n$. Which of are the following derived generators are secure?

   (a) $G_1(s_1||s_2) := G(s_1) \wedge G(s_2)$ where $\wedge$ denotes bit-wise AND.

   (b) $G_2(s_1||s_2) := G(s_1) \oplus G(s_2)$.

   (c) $G_3(s) := G(s) \oplus 1^n$.

3. Let G be a pseudorandom generator where $|G(s)| > 2|s|$. Is G_0 necessarily a pseudorandom generator?

   (a) $G_0(s) = G(s_1, \ldots, s_{n/2}), wheres = s_1, \ldots, s_n$.

   (b) $G_0(s) = G(s||0^{|s|})$.

   (c) $G_0(s) = G(s_1, \ldots, s_{|s|-1})||s_{|s|}$.

   (d) $G_0(s) = G(s)||0$.

   (e) $G_0(s) = G(s||0)$.