CS 601.442/642 – Modern Cryptography Instructors: Aditya Hegde and Harry Eldridge

Homework 3

Deadline: February 12; 2026, 11:59pm ET

Instructions

- The solutions must be submitted via Canvas.
- You must typeset your solutions. We suggest using LaTeX or Typst.

Notation

Let $s = (s_1, \dots, s_n)$ be an n-bit string. For any $1 \leq i \leq j \leq n$, the notation $s[i, \dots, j]$ refers to the contiguous substring $(s_i, \dots, s_j)$. Let 0^n denote the n-bit string of all zeros.

Problems

1. (10 points) Let G_1 and G_2 be PRGs. Prove or disprove if $G(s) = G_1(s) \| G_2(s)$ is also a PRG.

2. (20 points) Discuss whether the functions G_i below are PRGs for all PRGs G with at least $\lambda + 1$ bits of stretch i.e., on input a uniformly random λ-bit seed, G outputs a $\ell(\lambda)$-bit pseudorandom string with $\ell(\lambda) > 2\lambda + 1$. When G_i is a PRG, prove it. When G_i is not a PRG, describe an efficient adversary that successfully attacks the PRG. In each case below, G_i takes a uniformly random λ-bit seed $s \in \{0,1\}^\lambda$.

   (a) $G_1(s) \coloneqq G(s[1, \dots, \lambda - 1]) \| s[\lambda]$.

   (b) $G_2(s) \coloneqq G(s) \oplus (0^{\ell(\lambda) - \lambda} \| s)$.

   Remark. Recall that λ is a security parameter, not a fixed constant. Thus, when G is applied to an input of length $\lambda - 1$, it should be interpreted as running G with that input length as its security parameter.

3. (20 points) Let G_1 and G_2 be PRGs with at least $\lambda + 1$ bits of stretch. Define

   $$G(s) = G_1(s[1, \dots, \lambda]) \oplus G_2(s[\lambda + 1, \dots, 2\lambda]).$$

   Show that if either G_1 or G_2 is a PRG (we may not know which one is secure), then G is a PRG.

4. (20 points) Let G be a PRG with λ bits of stretch. Define $H(s)$ as follows: (1) Compute $r \coloneqq G(s)$, and (2) Output $G(r[1, \dots, \lambda]) \| G(r[\lambda + 1, \dots, 2\lambda])$. Prove or disprove if H is a PRG.

5. (30 points) Let G be an efficiently computable function that on input a λ-bit string outputs an $\ell(\lambda)$-bit string, where $\ell(\lambda) > \lambda$. Let $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be the following encryption scheme for $\ell(\lambda)$-bit messages:

   - $\mathsf{KeyGen}(1^\lambda) : k \leftarrow \{0,1\}^\lambda$.
   - $\mathsf{Enc}(k, m) : \mathsf{ct} \coloneqq G(k) \oplus m$.
   - $\mathsf{Dec}(k, \mathsf{ct}) : m \coloneqq G(k) \oplus \mathsf{ct}$.

   In class, we showed that if G is a PRG then Π is one-time computationally secure. **Now prove the converse:** If Π is one-time computationally secure, then G is a PRG.