Problem Set 4

We will work on the following exercises together during the work sessions on Friday, 15 September 2017.

You are strongly encouraged to work together on the exercises, including the homework. You do not have to hand in solutions to these problem sets.

Problem 1: not PRGs

For all of the following constructions, explain why they are not PRGs. If necessary, give an explicit description of an efficient distinguisher.

(a) Let $G(s)$ output s.

(b) Let $G(s)$ output $s\|s$

(c) Let $G(s)$ output $s\| \bigoplus_{i=1}^{n} s_i$.

Problem 2: Basic properties of PRGs

Recall that the *image of a function* $f : A \to B$ is the subset $f(A)$ of B. Formally,

$$\mathsf{im}(f) := f(A) = \{b \in B \mid \exists a \in A \text{ such that } b = f(a)\}\,.$$

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG.

(a) Let us assume that G is injective. How many different $2n$-bit strings y are there in the image of G?

(b) What is the fraction of images of G among all $2n$-bit strings?

(c) For a given $y \in \{0,1\}^{2n}$, what is $\Pr_{s\leftarrow\{0,1\}^n}[G(s) = y]$? Express it in terms of $|\{s \in \{0,1\}^n \mid G(s) = y\}|$ and n.

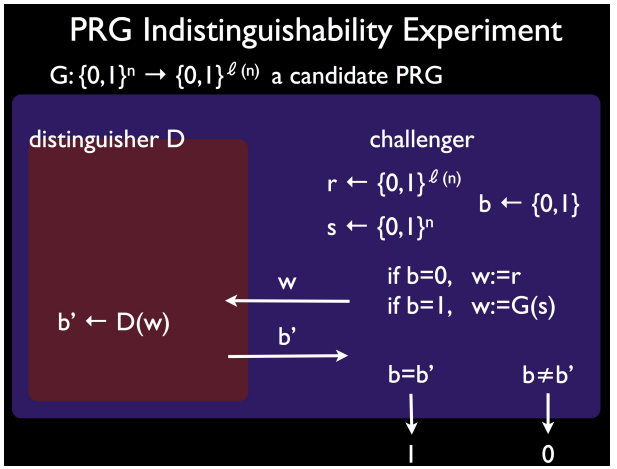

Figure 1: The $\mathsf{PRG}_{\mathcal{A},G}$ experiment

Problem 3: Exercise 3.5 from [KL]

Let $|G(s)| = \ell(|s|)$ for some ℓ. Consider the following experiment:

The PRG indistinguishability experiment $\mathsf{PRG}_{\mathcal{A},G}(n)$, see also Figure 1:

(a) A uniform bit $b \in \{0,1\}$ is chosen. If $b = 0$ then choose a uniform $r \leftarrow \{0,1\}^{\ell(n)}$ and set $w := r$; if $b = 1$ then choose a uniform $s \leftarrow \{0,1\}^n$ and set $w := G(s)$.

(b) The adversary $\mathcal{A}$ is given w, and outputs a bit b'.

(c) The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

Provide a definition of a pseudorandom generator based on this experiment, and prove that your definition is equivalent to Definition 3.14. (That is, show that G satisfies your definition if and only if it satisfies Definition 3.14.)

Problem 4: Brute-forcing a PRG

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Describe a *computationally unbounded* adversary $\mathcal{A}$ that distinguishes the output of G from a uniform $2n$-bit string with probability exponentially close 1. How does it work? Compute its exact distinguishing advantage. What is $\Pr[\mathsf{PRG}_{\mathcal{A},G}(n) = 1]$ for this adversary?

★ **Problem 5: Exercise 3.7 from [KL]**

Prove the converse of Theorem 3.18. Namely, show that if G is not a pseudorandom generator then Construction 3.17 does not have indistinguishable encryptions in the presence of an eavesdropper.