CS 442
Introduction to Cryptography

Lecture 9: Example Problems on PRGs

Instructor: Aarushi Goel

Spring 2026

Pseudorandom Generators (PRG)

Definition: A deterministic algorithm G is called a pseudorandom generator if:

* G can be computed in polynomial time.
* $|G(x)| > |x|$
* For every PPT adversary, $Pr[b = b'] = \frac{1}{2} + negl(|x|)$ in the following game

Adv

Ch

$\xleftarrow{\quad r \quad}$

$\xrightarrow{\quad b' \quad}$

$b \xleftarrow{\$} \{0,1\}$

if $b = 0$: $\quad r \xleftarrow{\$} \{0,1\}^{\ell(n)}$

if $b = 1$: $\quad s \xleftarrow{\$} \{0,1\}^n$

$r = G(s)$

Example #1

Q Let $G_1: \{0,1\}^n \to \{0,1\}^{2n}$ and $G_2: \{0,1\}^n \to \{0,1\}^{2n}$ be PRGs.

Is $G(s) = G_1(s) \| G_2(s)$ also a PRG?

A No!

Counter example: What if G_1 and G_2 are the same PRG.

$\Rightarrow$ $G_1(s) = G_2(s)$, the first $2n$-bits of the output of $G(s)$ are identical to the last $2n$-bits of the output of $G(s)$.

- This is highly unlikely to happen in a randomly sampled string.
- More formally,

$$\Pr\left[s_1 = s_2 \;\middle|\; s \xleftarrow{\$} \{0,1\}^n,\ s_1 \| s_2 = G_1(s) \| G_2(s) \right] = 1$$

$$\Pr\left[s_1 = s_2 \;\middle|\; s_1 \| s_2 \xleftarrow{\$} \{0,1\}^{4n} \right] = 1/2^{2n}$$

- Here the output of G and a random string are trivially distinguishable.

Example # 2

Q Let $G_1 : \{0,1\}^n \to \{0,1\}^{2n}$ and $G_2 : \{0,1\}^n \to \{0,1\}^{2n}$ be distinct PRGs.

Is $G(s) = \begin{cases} G_1(s) & \text{if } s \text{ is odd} \\ G_2(s) & \text{if } s \text{ is even} \end{cases}$ also a PRG?

A No!

Counter example: Let $F : \{0,1\}^{n-1} \to \{0,1\}^{2n-1}$ be a PRG. We define

complement

We define $G_1(s_1, \ldots, s_n) = F(s_1, \ldots, s_{n-1}) \| s_n$ and $G_2(s_1, \ldots, s_n) = F(s_1, \ldots, s_{n-1}) \| \bar{s}_n$

Now, by definition of G_1 if s is odd, last bit of $G_1(s)$ is 1.

If s is even, last bit of $G_2(s)$ is $\bar{0} = 1$.

$\Rightarrow$ The last bit of $G(s)$ is always 1. But this only happens with probability $1/2$ in a randomly sampled string.

Distinguisher / Adversary:

$\xleftarrow{\;r\;}$

$b \xleftarrow{\$} \{0,1\}$

if $b=0$: $\quad r \xleftarrow{\$} \{0,1\}^{2n}$

if $b=1$: $\quad s \xleftarrow{\$} \{0,1\}^{n}$

$r = G(s)$

Checks if the last bit of r is 1.

If so, set $b' = 1$

else, set $b' = 0$

$\xrightarrow{\;b'\;}$

$$\Pr[b=b'] = \Pr[b=b'=0] + \Pr[b=b'=1]$$

$$= \frac{1}{2} \times \Pr[b'=0 \mid b=0] + \frac{1}{2} \times \Pr[b'=1 \mid b=1]$$

$$= \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times 1 = \frac{1}{2} + \frac{1}{4}$$

non-negligible advantage.

Example #3

Q Let $G_1 : \{0,1\}^n \to \{0,1\}^{2n}$ and $G_2 : \{0,1\}^{2n} \longrightarrow \{0,1\}^{4n}$ be PRGs. Prove that the following function is also a PRG: $F : \{0,1\}^n \to \{0,1\}^{4n}$, $F(x) = G_2(G_1(x))$

A. We need to show that the following two distributions are computationally indistinguishable:

$$\{ G_2(G_1(x)) \; ; \; x \xleftarrow{\$} \{0,1\}^n \}$$

$$\{ s \xleftarrow{\$} \{0,1\}^{4n} \}$$

Consider the following hybrids:

H_1: $\{ G_2(G_1(x)) \; ; \; x \xleftarrow{\$} \{0,1\}^n \}$

H_2: $\{ G_2(r) \; ; \; r \xleftarrow{\$} \{0,1\}^{2n} \}$

H_3: $\{ s \xleftarrow{\$} \{0,1\}^{4n} \}$

Following the hybrid lemma, it suffices for us to show that $H_1 \approx_c H_2$ and $H_2 \approx_c H_3$.

* $H_2 \approx_c H_3$ follows directly from pseudorandomness of G_2.
* Let us focus on proving $H_1 \approx_c H_2$ using a proof by reduction.

Proof by Reduction

$H_1 : \{ G_2(G_1(x))\ ;\ x \xleftarrow{\$} \{0,1\}^n \}$ $\quad$ $H_2 : \{ G_2(r)\ ;\ r \xleftarrow{\$} \{0,1\}^{2n} \}$

* To prove that $H_1 \approx_c H_2$, we will use the following line of reasoning:

1. Let us assume for the sake of contradiction that $\exists$ a non-uniform PPT adversary A, can distinguish between H_1 and H_2 with some non-negligible probability.
2. We will use A to construct another non-uniform PPT adversary B who can break pseudorandomness of G with non-negligible advantage.
3. But we know that G is a PRG. Therefore no such adversary B can exist. Hence we arrive at a contradiction implying that our assumption was incorrect.

Proof by Reduction: How to construct B using A?

$H_1 : \{ G_2(G_1(x)) \; ; \; x \xleftarrow{\$} \{0,1\}^n \}$ $\qquad$ $H_2 : \{ G_2(r) \; ; \; r \xleftarrow{\$} \{0,1\}^{2n} \}$

Recall the game-based definition of PRG.

Adv

Ch

$\xleftarrow{\quad r \quad}$

$\xrightarrow{\quad b' \quad}$

$b \xleftarrow{\$} \{0,1\}$

if $b = 0$: $\quad r \xleftarrow{\$} \{0,1\}^{\ell(n)}$

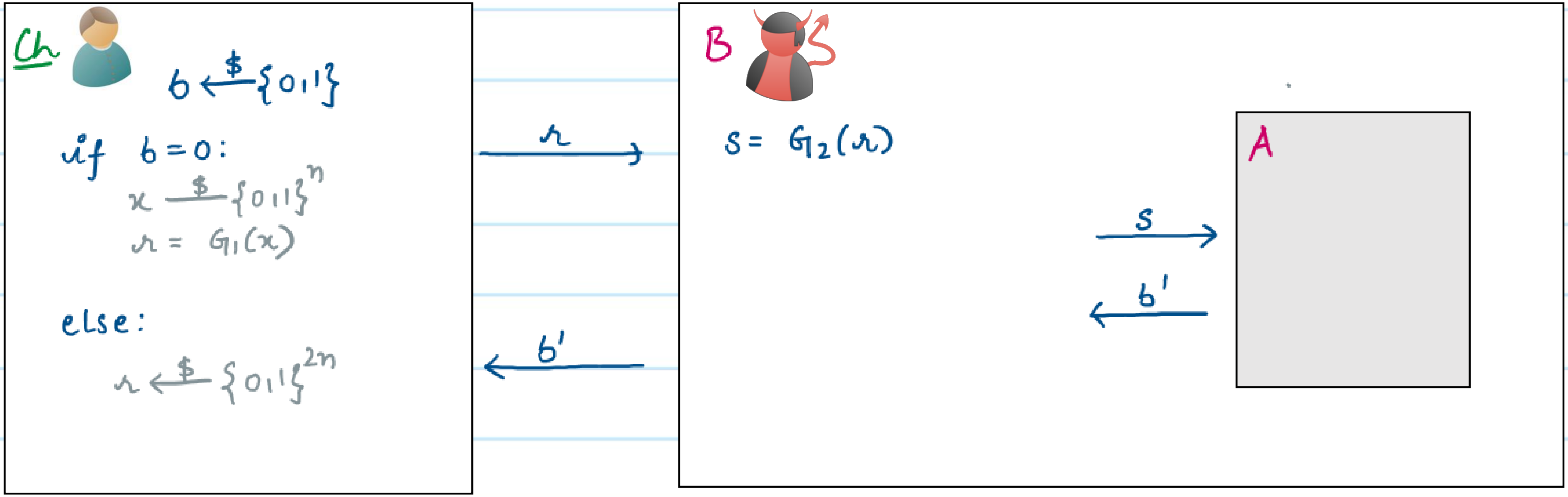
if $b = 1$: $\quad s \xleftarrow{\$} \{0,1\}^n$

$\qquad r = G(s)$

$$\Pr[b = b'] = \frac{1}{2} + negl(|x|)$$

To prove: $H_1 \approx_c H_2$

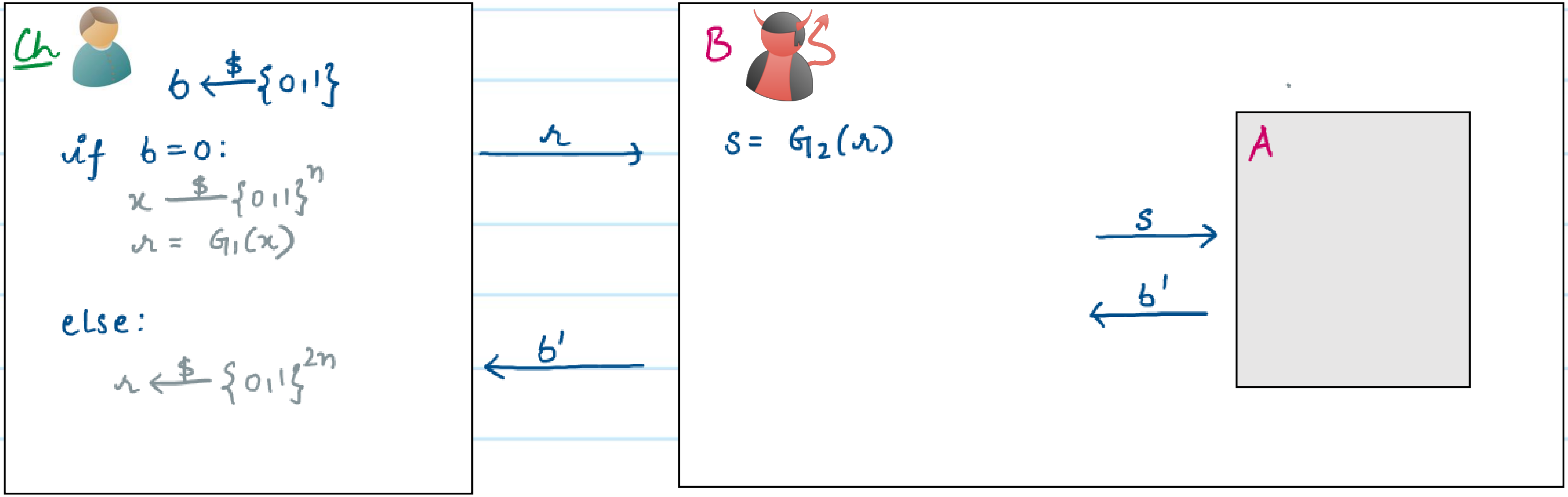
$H_1 : \{ G_2(G_1(x)) ; x \xleftarrow{\$} \{0,1\}^n \}$ $\quad$ $H : \{ G_2(r) ; r \xleftarrow{\$} \{0,1\}^{2n} \}$



If s is pseudorandom, then input to A is distributed identically to a sample from H_1, else it is identically distributed to a sample from H_2.

To prove: $H_1 \approx_c H_2$

$H_1 : \{ G_2(G_1(x)) \; ; \; x \xleftarrow{\$} \{0,1\}^n \}$ $\qquad$ $H : \{ G_2(r) \; ; \; r \xleftarrow{\$} \{0,1\}^{2n} \}$



$\Rightarrow$ If A succeeds with non-negligible advantage $\mu(n)$, then B also succeeds with the same non-negligible advantage $\mu(n)$.

This is a contradiction!

Proofs by Reduction : Key Points

* Here are 4 important things that must keep in mind for a valid reduction:

1. Input Mapping: How to map the input that the outer advesary B receives from the challenger to an input for the inner advesary A.

2. Input Distribution: Does the above input mapping provide the right distribution of inputs that A expects.

3. Output Mapping: How do we map the output that A provides to an output for B.

4. Win Probability: When we assume existence of A, we also assume that A wins with some non-negligible advantage $\mu(n)$. What is the probability or advantage with which B wins in terms of $\mu(n)$, given the above input / output mappings?