CS 442
Introduction to Cryptography

Lecture 8: Proofs by Reduction

Instructor: Aarushi Goel

Spring 2026

Agenda

* Computational Indistinguishability
* Non-uniform adversaries
* Examples of proofs by reduction.

HW2 will be released today. Will be due on Feb 22.

Computational Indistinguishability

* Let $\{A_n\}$, $\{B_n\}$ be distribution ensembles parameterized by n
* $\{A_n\}, \{B_n\}$ are computationally indistinguishable, if $\forall n \in \mathbb{N}$

$$\xleftarrow{\quad x \quad}$$

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

$$\text{if } b=0: \quad x \xleftarrow{\$} A_n$$

$$\text{if } b=1: \quad y \xleftarrow{\$} B_n$$

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

$$\Pr[b' = b] = \frac{1}{2} + \nu(n)$$

↳ negligible function.

$$\boxed{\{A_n\} \approx_c \{B_n\}}$$

Non-Uniform Adversaries

* **Non-uniform PPT adversaries/distinguishers:** A family of randomized adversaries/programs/ distinguishers $\{T_n\}$ (one for each value of the security parameter $n \in \mathbb{N}$), such that there is a polynomial $p(.)$ and each T_n runs in time at most $p(n)$.

* **Uniform PPT adversaries/distinguishers:** where T is a single program that takes n as an additional input.

By default, we will consider non-uniform PPT algorithms/ adversaries/tests/distinguishers.

Computationally Secure Encryption.

Definition: An encryption scheme (KeyGen, Enc, Dec) with message space $\mathcal{M}$ is computationally secure if it satisfies correctness (as defined previously) and if for every $m_1, m_2 \in \mathcal{M}$, it holds that

$$\left\{ \mathrm{Enc}(K, m_1) \,;\, K \xleftarrow{\$} \{0,1\}^n \right\} \approx_c \left\{ \mathrm{Enc}(K, m_2) \,;\, K \xleftarrow{\$} \{0,1\}^n \right\}$$

Pseudorandom Generators (PRG)

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

* G can be computed in polynomial time.
* $|G(x)| > |x|$
* $\{G(x) ; x \xleftarrow{\$} \{0,1\}^n\} \approx_c \{U_{\ell(n)}\}$, where $\ell(n) = |G(x)|$

uniform distribution.

Hybrid Lemma

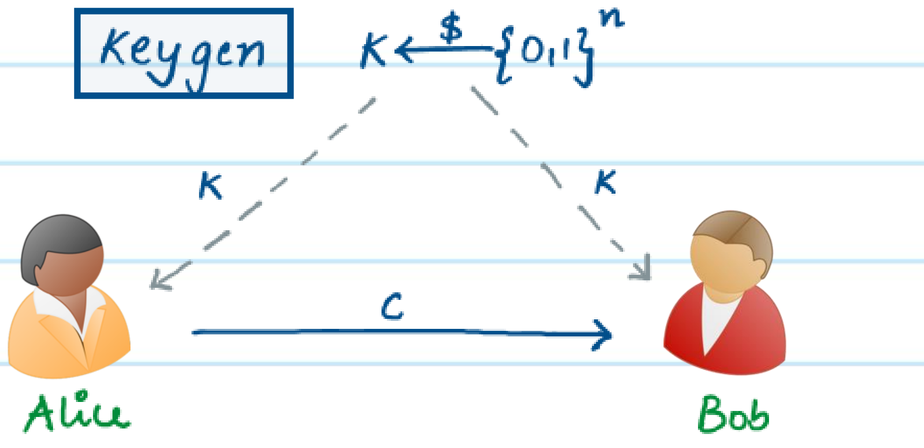
Lemma: Let $\{A_n^1\}, \ldots, \{A_n^m\}$ be distribution ensembles, where $m = poly(n)$. If $\forall i \in [m-1]$, $\{A_n^i\}, \{A_n^{i+1}\}$ are computationally indistinguishable, then $\{A_n^1\}, \{A_n^m\}$ are computationally indistinguishable.

This lemma is used in most crypto proofs.

Why:

Pseudorandom OTP Encryption Scheme

* Recall the candidate computationally secure encryption scheme from last class.



$c = m \oplus G(K)$ $\qquad$ $m = c \oplus G(K)$

PRG

We want to show that this is indeed a computationally secure encryption

* correctness : easy to verify
* security : we need to prove that $\forall\, m_1, m_2$, the following distributions are computationally indistinguishable:

$$\{c = m_1 \oplus G(K) \;;\; K \xleftarrow{\$} \{0,1\}^n\}$$
$$\{c = m_2 \oplus G(K) \;;\; K \xleftarrow{\$} \{0,1\}^n\}$$

Proof Using Hybrid Lemma

Consider the following hybrids:

H_1: $\{ c = m_1 \oplus G(K) \;;\; K \xleftarrow{\$} \{0,1\}^n \}$

H_2: $\{ c = m_1 \oplus s \;;\; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

H_3: $\{ c = m_2 \oplus s \;;\; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

H_4: $\{ c = m_2 \oplus G(K) \;;\; K \xleftarrow{\$} \{0,1\}^n \}$

Proof Using Hybrid Lemma

Consider the following hybrids:

$H_1: \{ c = m_1 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$

$H_2: \{ c = m_1 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

$H_3: \{ c = m_2 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

$H_4: \{ c = m_2 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$

Why is $H_1 \approx_c H_2$?

Since G is a PRG, we know that
$\{ G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \} \approx_c \{ s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$.

From closure property of computational indistinguishability, it then follows that $H_1 \approx_c H_2$.

Proof Using Hybrid Lemma

Consider the following hybrids:

$H_1: \{ c = m_1 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$

$H_2: \{ c = m_1 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

$H_3: \{ c = m_2 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

$H_4: \{ c = m_2 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$

Why is $H_2 \approx_c H_3$?

H_2 an H_3 are identically distributed, i.e., $H_2 \equiv H_3$.

Proof Using Hybrid Lemma

Consider the following hybrids:

$H_1: \{ c = m_1 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$

$H_2: \{ c = m_1 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

$H_3: \{ c = m_2 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

$H_4: \{ c = m_2 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$

Why is $H_3 \approx_c H_4$?

Same reason why H_1 and H_2 are computationally indistinguishable.

Proof Using Hybrid Lemma

Consider the following hybrids:

$H_1: \{ c = m_1 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$

$H_2: \{ c = m_1 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

$H_3: \{ c = m_2 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

$H_4: \{ c = m_2 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$

$H_1 \approx_c H_2 \equiv H_3 \approx_c H_4$

By hybrid lemma, it follows that $H_1 \approx_c H_4$.

Contrapositive Point of View

* What we just discussed was a proof in the "forward" direction.
* A more classical way is to prove security by arriving at a contradiction.
* Recall the following contrapositive variant of the hybrid lemma.

> **Lemma:** Let $\{A_n^1\}, \ldots, \{A_n^m\}$ be distribution ensembles, where $m = poly(n)$. Suppose there exists a PPT adversary A, who can distinguish between $\{A_n^1\}, \{A_n^m\}$ with probability μ. Then there must exist $i \in [m-1]$, such that A can distinguish between $\{A_n^i\}$ and $\{A_n^{i+1}\}$ with probability at least μ/m.

Contrapositive Point of View

* In the previous example, we proved a statement of the following form:

  If G is a PRG, then $H_1 \approx_c H_2$.

* What is the contrapositive of this?

  If $H_1 \not\approx_c H_2$, then G is not a PRG.

ie., if $H_1 \not\approx_c H_2$, then $\exists$ a non-uniform PPT Adversary A, who can distinguish between H_1 and H_2 with some non-negligible advantage.

Can we use this adversary A to break pseudorandomness of G?

Proof by Reduction

$H_1 : \{ c = m_1 \oplus G(K) \ ; \ K \xleftarrow{\$} \{0,1\}^n \}$ $\qquad$ $H_2 : \{ c = m \oplus s \ ; \ s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

* 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: $\{ c = m_1 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$ $\qquad$ H_2: $\{ c = m \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$

Recall the game-based definition of PRG.

Adv

Ch

$\xleftarrow{\quad r \quad}$

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

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

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

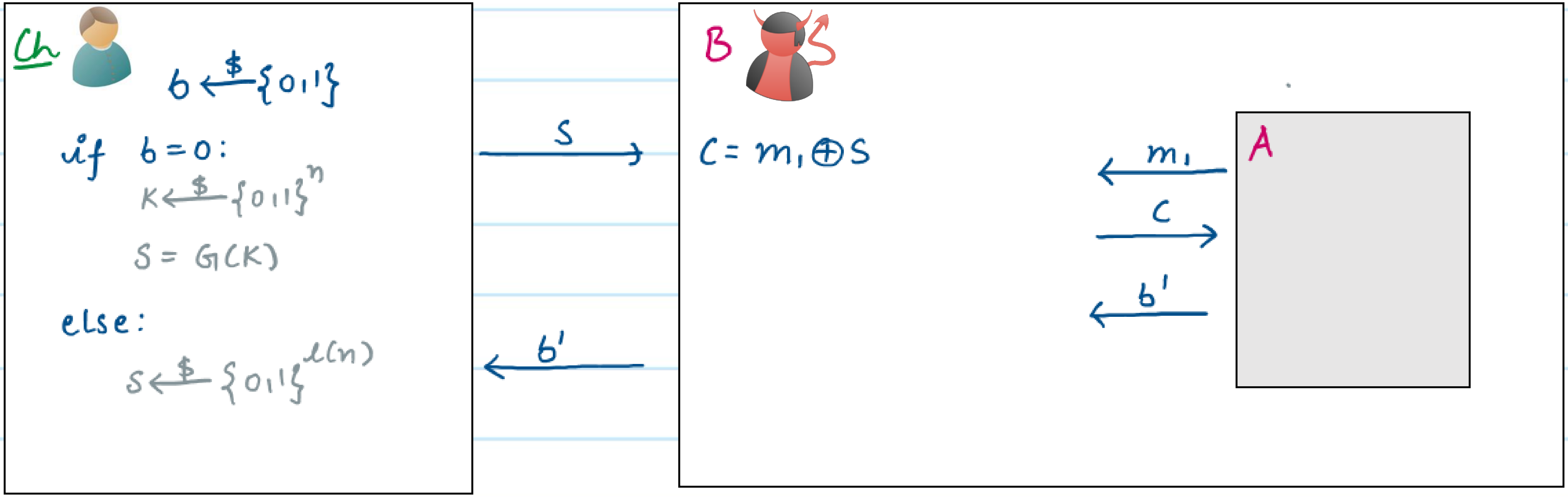
if $b = 1$: $\quad s \xleftarrow{\$} \{0,1\}^n$

$\qquad r = G(s)$

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

Proof by Reduction: How to construct B using A?

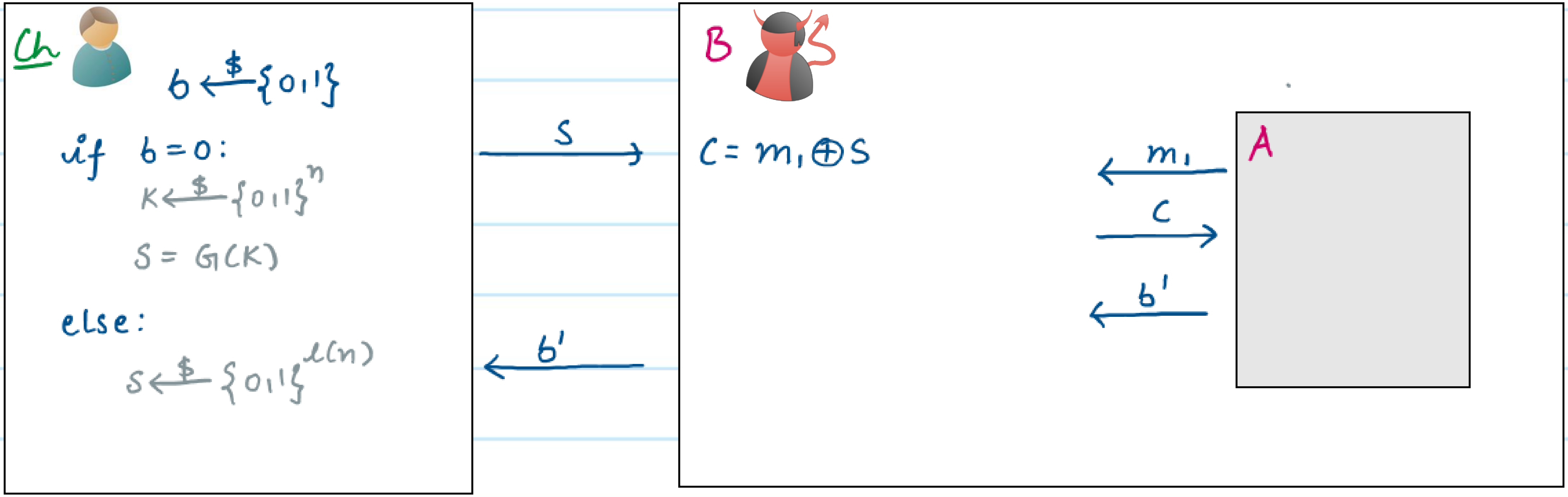
H_1: $\{ c = m_1 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$ $\qquad$ H_2: $\{ c = m \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$



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.

Proof by Reduction: How to construct B using A?

$H_1: \{ c = m_1 \oplus G(K) \; ; \; K \xleftarrow{\$} \{0,1\}^n \}$ $\qquad H_2: \{ c = m \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(n)} \}$



$\Rightarrow$ 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 adversary B receives from the challenger to an input for the inner adversary 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?

Another Example of a Proof by Reduction

Q Let $G_1 : \{0,1\}^n \to \{0,1\}^{2n}$ and $G_2 : \{0,1\}^{2n} \to \{0,1\}^{4n}$ 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.

To prove: $H_1 \approx_c H_2$

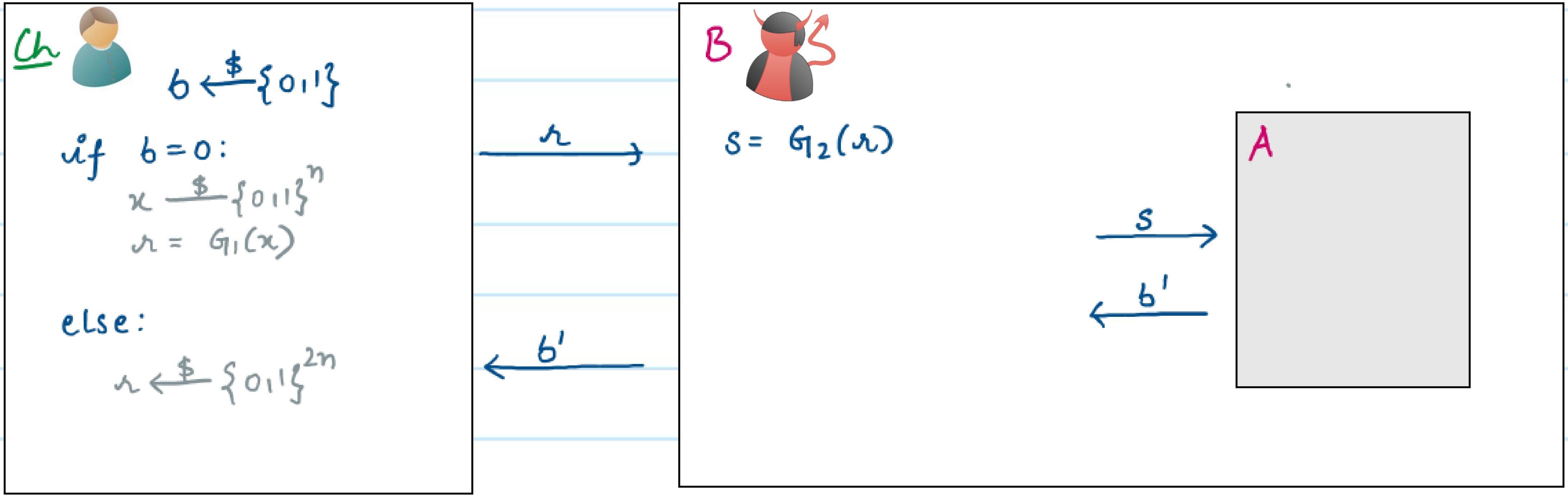
$H_1 : \{ G_2(G_1(x)) \,;\, x \xleftarrow{\$} \{0,1\}^n \}$ $\quad$ $H_2 : \{ G_2(r) \,;\, r \xleftarrow{\$} \{0,1\}^{2n} \}$

* Let us assume for the sake of contradiction that $H_1 \not\approx_c H_2$. In other words, we assume that there exists a non-uniform PPT adversary A, that can distinguish between H_1 and H_2 with non-negligible advantage $\mu(n)$.

* We will now use A to design another adversary B who can distinguish between H_1 and H_2 with non-negligible advantage.

To prove: $H_1 \approx_c H_2$

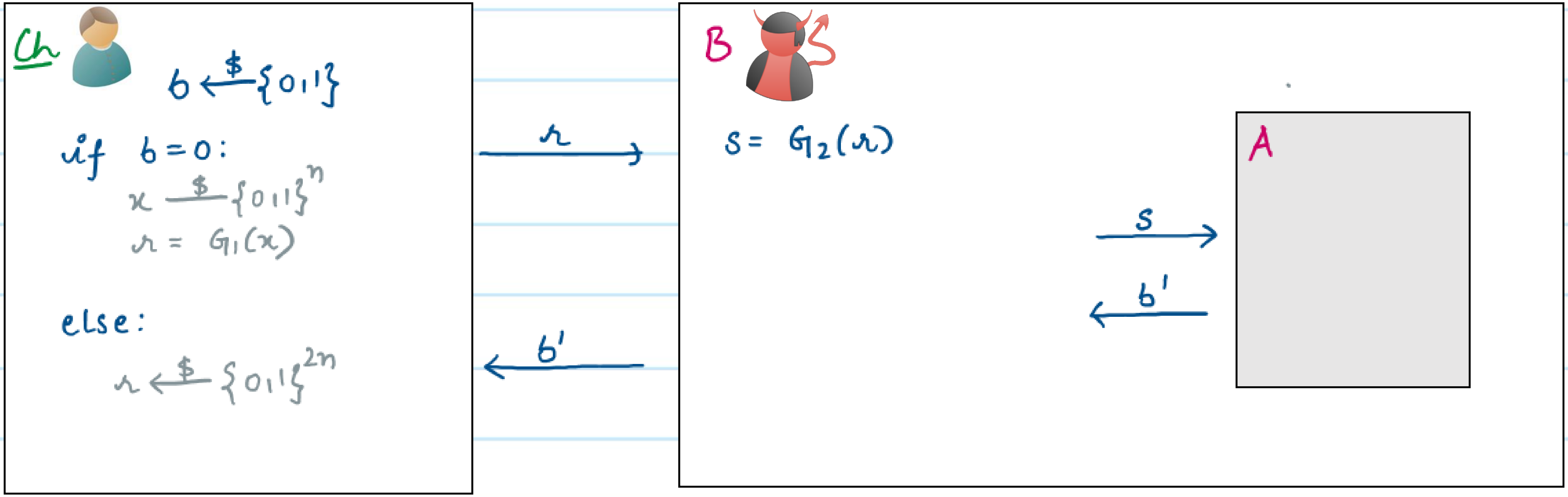
$H_1 : \{ G_2(G_1(x)) \; ; \; x \xleftarrow{\$} \{0,1\}^n \}$ $\quad$ $H : \{ G_2(r) \; ; \; r \xleftarrow{\$} \{0,1\}^{2n} \}$



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!