CS 65500
Advanced Cryptography

Lecture 2: Basics of Provable Security

Instructor: Aarushi Goel

Spring 2025

Recap

→ Indistinguishability — Perfect
— Statistical
— Computational

→ Negligible Functions

→ Non-Uniform Adversaries

Reminder: HW1 out today. Due Jan 30!

Perfect Indistinguishability

Definition: Distribution ensembles $\{A_K\}$ and $\{B_K\}$ are perfectly indistinguishable if $\forall K$,

$$\Pr_{x \leftarrow A}[T(x) = 0] = \Pr_{x \leftarrow B}[T(x) = 0]$$

$$A \equiv B$$

Statistical Indistinguishability

Definition: Distribution ensembles $\{A_K\}$, $\{B_K\}$ are statistically indistinguishable if

$\exists$ negligible $\nu(\cdot)$, s.t., $\forall K$, $\Delta(A_K, B_K) \leq \nu(K)$

$$\{A_K\} \approx_s \{B_K\}$$

Computational Indistinguishability

Definition: Distribution ensembles $\{A_K\}, \{B_K\}$ are computationally indistinguishable if $\forall$ efficient tests T, $\exists$ negligible $\nu(.)$. s.t. $\forall K$,

$$\left| \Pr_{x \leftarrow A_K} [T_K(x) = 0] - \Pr_{x \leftarrow B_K} [T_K(x) = 0] \right| \leq \nu(K)$$

$$\{A_K\} \approx_c \{B_K\}$$

Agenda

→ Security Games

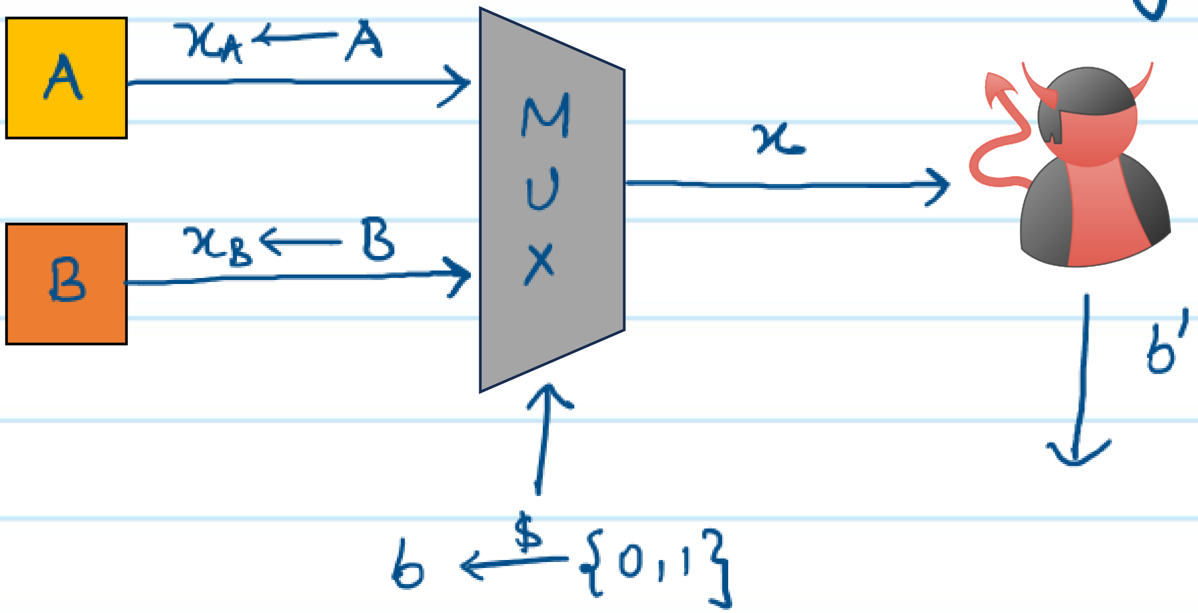
→ Properties of Computational Indistinguishability

→ Hybrid Lemma

→ Proofs by Reduction.

Security Games

Indistinguishability can be defined using a guessing game

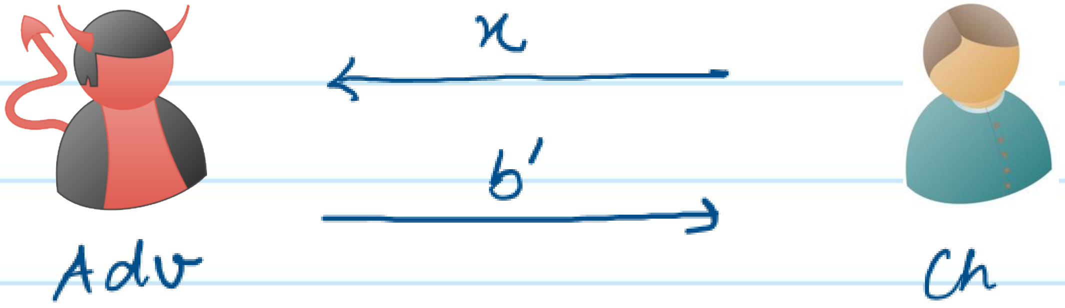


Adv wins if $b = b'$!

if b is chosen at random, what is $\Pr[b' = b] = ?$

Security Games

Equivalent to the following game between the adversary and a challenger.



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

if $b = 0$:

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

else:

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

Adv wins if $b = b'$!

if b is chosen at random, what is $\Pr[b' = b] = ?$

Security Games

$$\Pr[b' = b] = ?$$

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

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

$$= \frac{1}{2}\left(\Pr[b' = 0 \mid b = 0] + 1 - \Pr[b' = 0 \mid b = 1]\right)$$

$$= \frac{1}{2} + \frac{1}{2}\left(\Pr[b' = 0 \mid b = 0] - \Pr[b' = 0 \mid b = 1]\right)$$

$$= \frac{1}{2} + \frac{1}{2}\left(\Pr_{x \leftarrow A}[T(x) = 0] - \Pr_{x \leftarrow B}[T(x) = 0]\right)$$

$$= \frac{1}{2} + \frac{\Delta(A, B)}{2}$$

Security Games

Maximum $Pr[b' = b] = \frac{1}{2} + \frac{\Delta(A, B)}{2}$

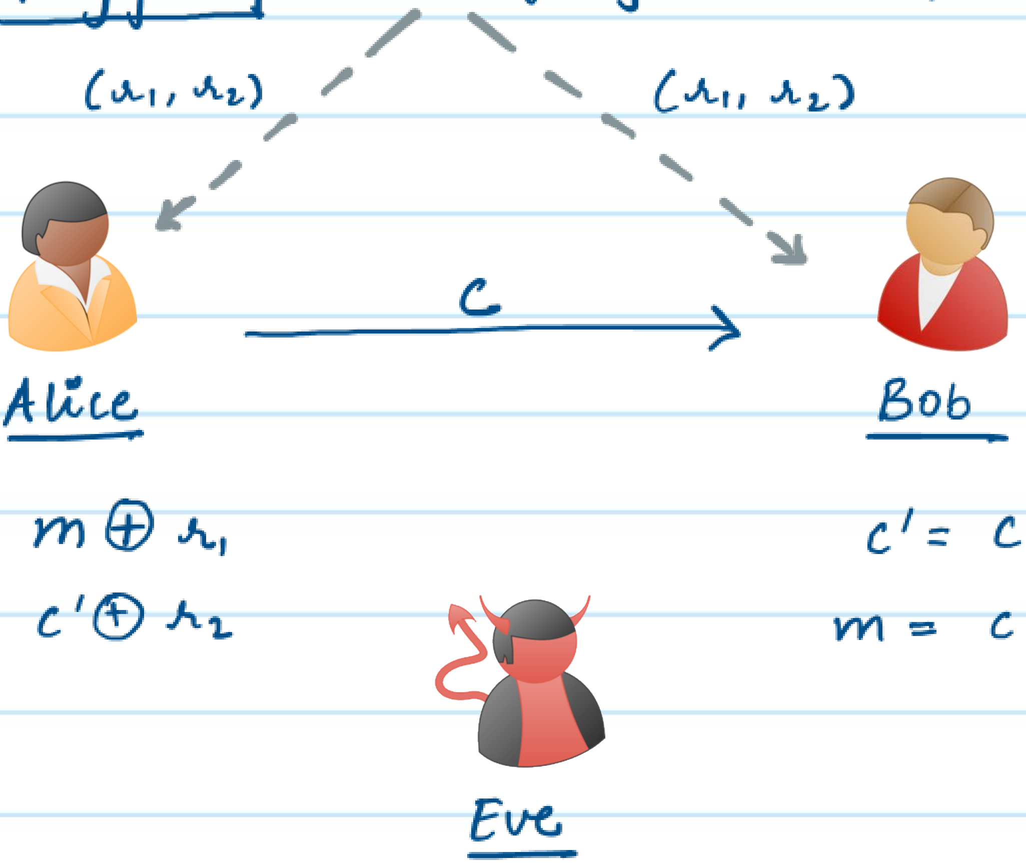
Definition: A, B are ~~statistically~~ computationally indistinguishable if for every PPT adversary in the above game, $\exists$ a negligible function $\nu(\cdot)$, s.t. $\forall K$,

$$\text{Advantage}(K) := Pr[b' = b] - \frac{1}{2} \leq \nu(K)$$

Proof by Hybrid Technique

Example (Double OTP): Prove that the following encryption scheme satisfies perfect secrecy.

$\boxed{\text{Keygen:}}$ $r_1 \xleftarrow{\$} \{0,1\}^k \quad r_2 \xleftarrow{\$} \{0,1\}^k$



Alice:

$c' = m \oplus r_1$

$c = c' \oplus r_2$

Bob:

$c' = c \oplus r_2$

$m = c' \oplus r_1$

Proof by Hybrid Technique

→ For perfect secrecy, we need to show that $\forall c$, $\forall m_1 \in \{0,1\}^k$, $m_2 \in \{0,1\}^k$ (we let the adv choose m_1 and m_2)

$$\Pr[\text{view} = c \mid \text{msg} = m_1] = \Pr[\text{view} = c \mid \text{msg} = m_2]$$

→ In other words, we need to show that $\forall m_1 \in \{0,1\}^k$, $\forall m_2 \in \{0,1\}^k$, the following distributions are identical:

1. $\{c = c' \oplus r_2 \, ; \, c' = r_1 \oplus m_1 \, , \, r_1 \xleftarrow{\$} \{0,1\}^k, \, r_2 \xleftarrow{\$} \{0,1\}^k\}$
2. $\{c = c' \oplus r_2 \, ; \, c' = r_1 \oplus m_2 \, , \, r_1 \xleftarrow{\$} \{0,1\}^k, \, r_2 \xleftarrow{\$} \{0,1\}^k\}$

Proof by Hybrid Technique

→ For this, we will consider the following set of distributions called hybrids

H_1 $\{c = c' \oplus r_2 \,;\; c' = r_1 \oplus m_1 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k,\; r_2 \xleftarrow{\$} \{0,1\}^k\}$

H_2 $\{c \xleftarrow{\$} \{0,1\}^k \,;\; c' = r_1 \oplus m_1 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k\}$

H_3 $\{c \xleftarrow{\$} \{0,1\}^k \,;\; c' = r_1 \oplus m_2 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k\}$

called intermediate hybrids

H_4 $\{c = c' \oplus r_2 \,;\; c' = r_1 \oplus m_2 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k,\; r_2 \xleftarrow{\$} \{0,1\}^k\}$

Proof by Hybrid Technique

H_1 $\left\{ c = c' \oplus r_2 \, ; \, c' = r_1 \oplus m_1 \, , \quad r_1 \xleftarrow{\$} \{0,1\}^k , \; r_2 \xleftarrow{\$} \{0,1\}^k \right\}$

H_2 $\left\{ c \xleftarrow{\$} \{0,1\}^k \, ; \, c' = r_1 \oplus m_1 \, , \quad r_1 \xleftarrow{\$} \{0,1\}^k \right\}$

H_3 $\left\{ c \xleftarrow{\$} \{0,1\}^k \, ; \, c' = r_1 \oplus m_2 \, , \quad r_1 \xleftarrow{\$} \{0,1\}^k \right\}$

H_4 $\left\{ c = c' \oplus r_2 \, ; \, c' = r_1 \oplus m_2 \, , \quad r_1 \xleftarrow{\$} \{0,1\}^k , \; r_2 \xleftarrow{\$} \{0,1\}^k \right\}$

Our goal is to show that H_1 is identical to H_4

for this, we will show

$H_1 \equiv H_2$, $H_2 \equiv H_3$ and $H_3 \equiv H_4$

Proof by Hybrid Technique

H_1 $\{c = c' \oplus r_2 \,;\, c' = r_1 \oplus m_1 \,,\quad r_1 \xleftarrow{\$} \{0,1\}^k,\ r_2 \xleftarrow{\$} \{0,1\}^k\}$

H_2 $\{c \xleftarrow{\$} \{0,1\}^k \,;\, c' = r_1 \oplus m_1 \,,\quad r_1 \xleftarrow{\$} \{0,1\}^k\}$

H_3 $\{c \xleftarrow{\$} \{0,1\}^k \,;\, c' = r_1 \oplus m_2 \,,\quad r_1 \xleftarrow{\$} \{0,1\}^k\}$

H_4 $\{c = c' \oplus r_2 \,;\, c' = r_1 \oplus m_2 \,,\quad r_1 \xleftarrow{\$} \{0,1\}^k,\ r_2 \xleftarrow{\$} \{0,1\}^k\}$

Why is $H_1 \equiv H_2$?

Proof by Hybrid Technique

H_1 $\{c = c' \oplus r_2 \,;\, c' = r_1 \oplus m_1 \,, \quad r_1 \xleftarrow{\$} \{0,1\}^k, \; r_2 \xleftarrow{\$} \{0,1\}^k\}$

H_2 $\{c \xleftarrow{\$} \{0,1\}^k \,;\, c' = r_1 \oplus m_1 \,, \quad r_1 \xleftarrow{\$} \{0,1\}^k\}$

H_3 $\{c \xleftarrow{\$} \{0,1\}^k \,;\, c' = r_1 \oplus m_2 \,, \quad r_1 \xleftarrow{\$} \{0,1\}^k\}$

H_4 $\{c = c' \oplus r_2 \,;\, c' = r_1 \oplus m_2 \,, \quad r_1 \xleftarrow{\$} \{0,1\}^k, \; r_2 \xleftarrow{\$} \{0,1\}^k\}$

Why is $H_2 \equiv H_3$? Trivially

Proof by Hybrid Technique

H_1 $\{c = c' \oplus r_2 \,;\, c' = r_1 \oplus m_1 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k, \; r_2 \xleftarrow{\$} \{0,1\}^k\}$

H_2 $\{c \xleftarrow{\$} \{0,1\}^k \,;\, c' = r_1 \oplus m_1 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k\}$

H_3 $\{c \xleftarrow{\$} \{0,1\}^k \,;\, c' = r_1 \oplus m_2 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k\}$

H_4 $\{c = c' \oplus r_2 \,;\, c' = r_1 \oplus m_2 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k, \; r_2 \xleftarrow{\$} \{0,1\}^k\}$

Why is $H_3 \equiv H_4$?

Proof by Hybrid Technique

$H_1 \quad \{ c = c' \oplus r_2 \,;\, c' = r_1 \oplus m_1 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k,\; r_2 \xleftarrow{\$} \{0,1\}^k \}$

$H_2 \quad \{ c \xleftarrow{\$} \{0,1\}^k \,;\, c' = r_1 \oplus m_1 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k \}$

$H_3 \quad \{ c \xleftarrow{\$} \{0,1\}^k \,;\, c' = r_1 \oplus m_2 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k \}$

$H_4 \quad \{ c = c' \oplus r_2 \,;\, c' = r_1 \oplus m_2 \,,\; r_1 \xleftarrow{\$} \{0,1\}^k,\; r_2 \xleftarrow{\$} \{0,1\}^k \}$

Since $H_1 \equiv H_2$, $H_2 \equiv H_3$ and $H_3 \equiv H_4$,
by transitivity, $\underline{H_1 \equiv H_4}$

Properties of Computational Indistinguishability

→ **Closure:** If we apply an efficient operation on A and B, they remain computationally indistinguishable. That is, $\forall$ non-uniform PPT M

$$\{A_k\} \approx_c \{B_k\} \Rightarrow \{M(A_k)\} \approx_c \{M(B_k)\}$$

Why?

→ **Transitivity:** If A, B are computationally indistinguishable and B, C are computationally indistinguishable, then A, C are also computationally indistinguishable

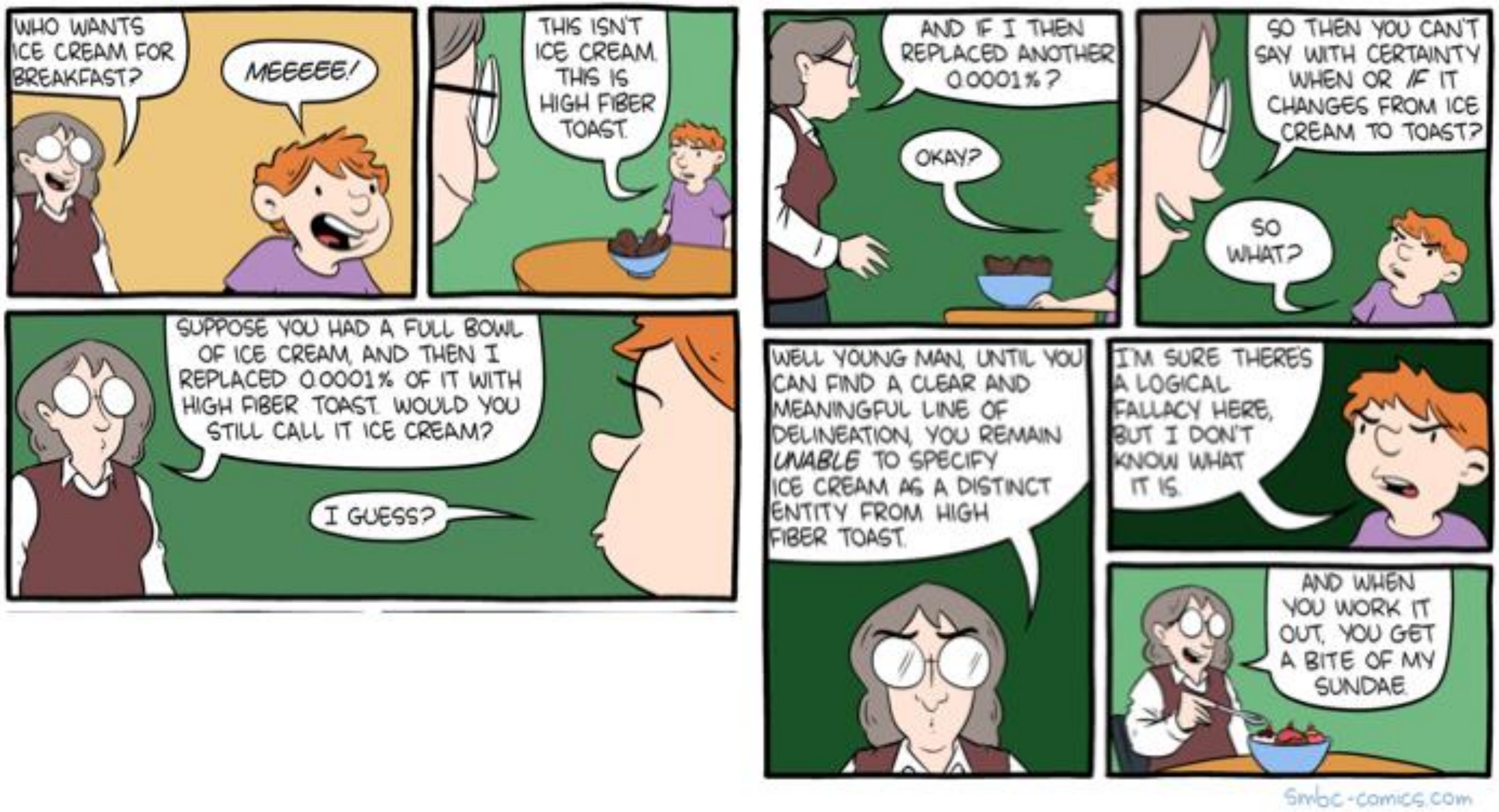
$$\{A_k\} \approx_c \{B_k\} \;\&\; \{B_k\} \approx_c \{C_k\} \Rightarrow \{A_k\} \approx_c \{C_k\}$$

Hybrid Lemma: Generalizing Transitivity

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

This hybrid technique is used in most crypto proofs.

Hybrid lemma



Pseudorandom Generator

Recall the following definition of a pseudorandom generator (PRG):

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

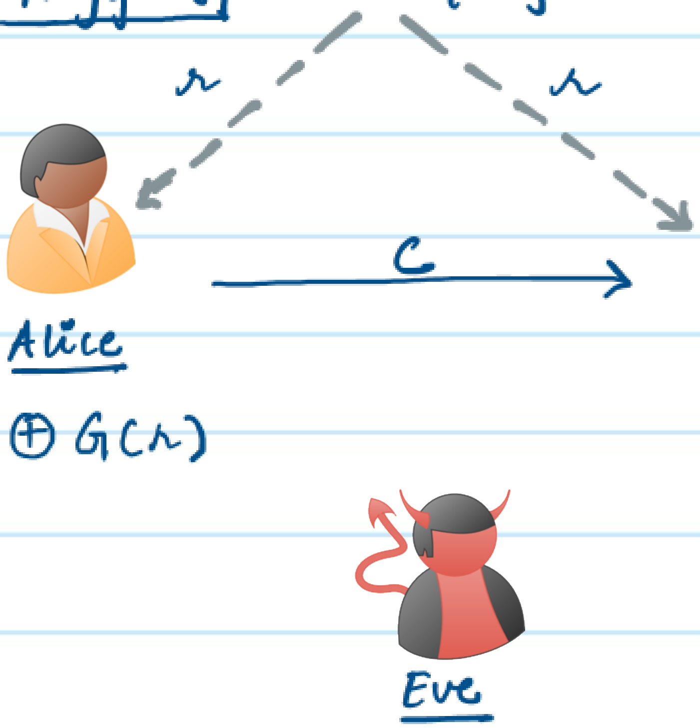
1. G can be computed in polynomial time
2. $|G(x)| > |x|$
3. $\{G(x); x \xleftarrow{\$} \{0,1\}^{\kappa}\} \approx_c \{\mathcal{U}_{\ell(\kappa)}\}$ where $\ell(\kappa) = |G(x)|$

uniform distribution

Proof by Hybrid Lemma

Example (Pseudorandom OTP): Consider the following encryption scheme

$\boxed{\text{Keygen:}}$ $r \xleftarrow{\$} \{0,1\}^k$



$c = m \oplus G(r)$

$m = c \oplus G(r)$

Prove that $\forall\, m_1, m_2$, the following distributions are computationally indistinguishable:

1. $\{ c = m_1 \oplus G(r) \,;\, r \xleftarrow{\$} \{0,1\}^k \}$

2. $\{ c = m_2 \oplus G(r) \,;\, r \xleftarrow{\$} \{0,1\}^k \}$

Proof by Hybrid Lemma

Consider the following hybrids:

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

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

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

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

Proof by Hybrid Lemma

H_1: $\left\{ c = m_1 \oplus G(r) \;;\; r \xleftarrow{\$} \{0,1\}^k \right\}$

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

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

H_4: $\left\{ c = m_2 \oplus G(r) \;;\; r \xleftarrow{\$} \{0,1\}^k \right\}$

why is $H_1 \approx_c H_2$?

Proof by Hybrid Lemma

H_1: $\left\{ c = m_1 \oplus G(r) \;;\; r \xleftarrow{\$} \{0,1\}^k \right\}$

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

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

H_4: $\left\{ c = m_2 \oplus G(r) \;;\; r \xleftarrow{\$} \{0,1\}^k \right\}$

why is $H_2 \equiv H_3$?

Proof by Hybrid Lemma

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

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

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

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

why is $H_3 \approx_c H_4$?

Proof by Hybrid Lemma

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

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

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

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

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

By hybrid lemma $H_1 \approx_c H_4$

Contrapositive Point of View

→ So far, we have only considered security proofs in the "forward" direction

→ A more classical way is to prove security by arriving at a contradiction.

Definition: A function $\nu(K)$ is non-negligible if $\exists c$, such that $\forall N$, $\exists K > N$,

$$\nu(K) \geq \frac{1}{n^c}$$

Contrapositive Point of View

Here is an alternate way to state the hybrid lemma:

Lemma: Let $\{X_K^1\}, \ldots \{X_K^m\}$ be distribution ensembles for $m = \text{poly}(K)$. Suppose there exists a distinguisher/adversary A that distinguishes between $\{X_K^1\}$ & $\{X_K^m\}$ with probability μ. Then $\exists i \in [m-1]$, such that A can distinguish between $\{X_K^i\}$ and $\{X_K^{i+1}\}$ 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.

If $H_1 \not\approx_c H_2$, then $\exists$ a n.u. PPT Adversary A, who can distinguish between H_1 and H_2 with some non-negligible advantage μ.

Can we use A to break security of G?

Proof by Reduction

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

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

→ Let us assume a n.u. PPT A can distinguish between H_1 and H_2 with non-negligible advantage

→ Can we use A to construct B who can break security of G with non-negligible advantage?

→ But G is a secure PRG. Therefore no such B should exist. Hence we will arrive at a contradiction implying that our assumption was wrong.

Proof by Reduction

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

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

Recall game based definition of PRG.

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

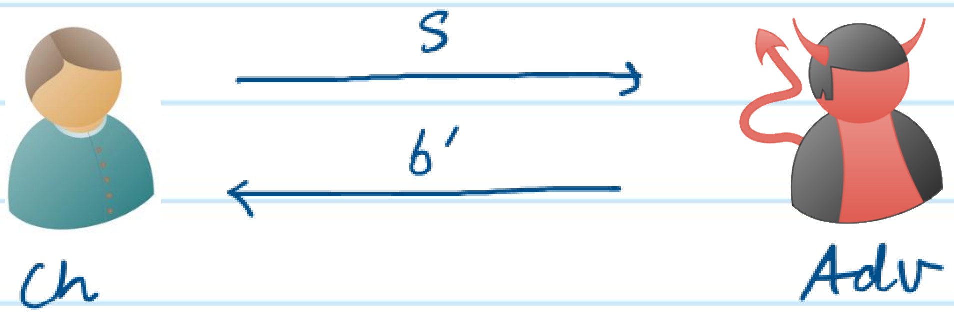
if $b = 0$:

$r \xleftarrow{\$} \{0,1\}^k$

$s = G(r)$

else:

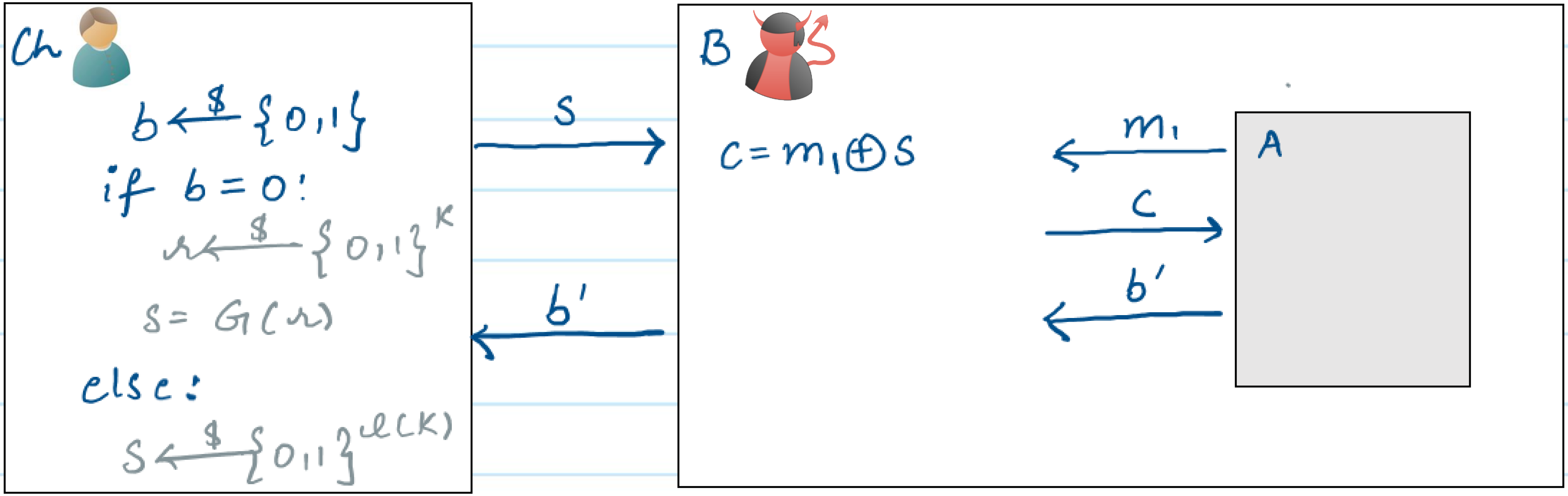
$s \xleftarrow{\$} \{0,1\}^{\ell(k)}$



Adv wins if $b = b'$

Proof by Reduction

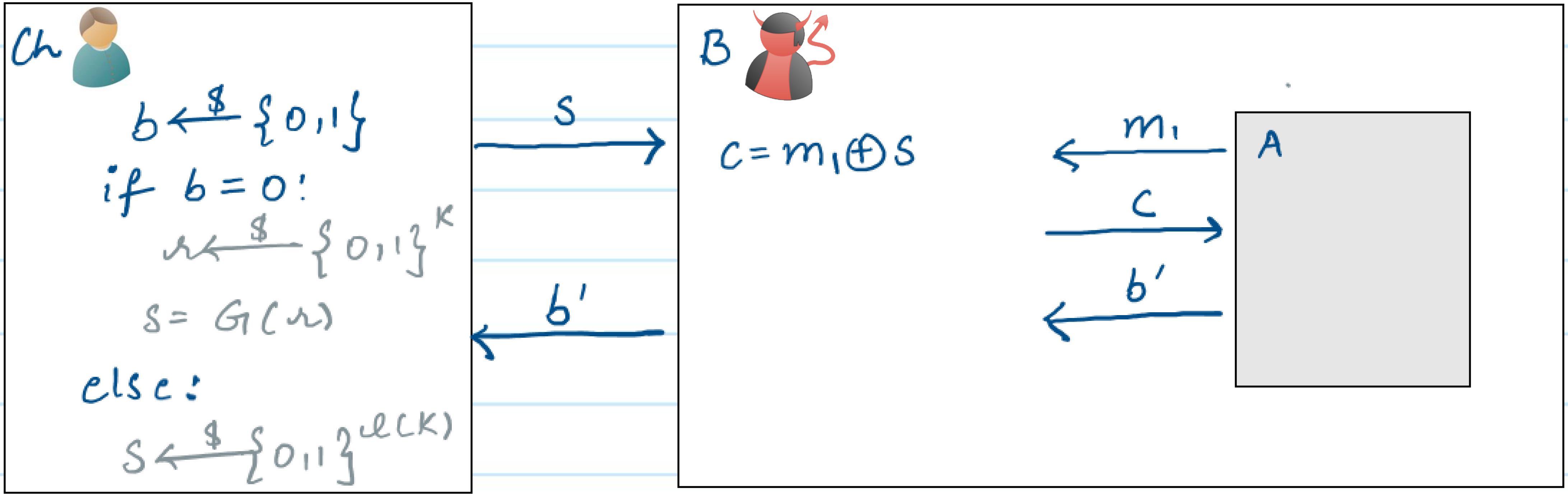
$H_1 : \{ c = m_1 \oplus G(r) \; ; \; r \xleftarrow{\$} \{0,1\}^K \}$ $\qquad$ $H_2 : \{ c = m_1 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(K)} \}$



if s is pseudorandom, then input to A is distributed identically to the output of H_1; else it is identically distributed to the output of H_2

Proof by Reduction

$H_1: \{ c = m_1 \oplus G(r) \; ; \; r \xleftarrow{\$} \{0,1\}^k \}$ $\quad$ $H_2: \{ c = m_1 \oplus s \; ; \; s \xleftarrow{\$} \{0,1\}^{\ell(k)} \}$



$\Rightarrow$ If A succeeds with non-negligible probability μ, the B also succeeds with probability μ.

This is a contradiction!

Proofs by Reduction: Key Points

Here are four important things you must work through for a valid reduction:

1. **Input Mapping:** How to map the input that outer adversary B receives from the challenger to an input to the inner adversary A?

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

Proofs by Reduction: Key Points

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

4. **Probability:** When we assume existence of A, we also assume that A wins with some non-negligible advantage μ. What is the probability / advantage that B wins in terms of μ, given the above mappings.