CSCI 1510

- Definition of Semantic Security (Continued)
- Pseudorandom Generator (PRG)
- Fixed-Length Encryption from PRG
- Proof by Reduction

Last Lecture

Computational Security

- **Concrete Approach:**

  A scheme is (t, ε)-secure if $\forall A$ running in time $\leq t$ succeeds in breaking the scheme with probability $\leq \varepsilon$.

- **Asymptotic Approach:**

  Introduce a security parameter n

  A scheme is secure if $\forall A$ running in time $\text{poly}(n)$ succeeds in breaking the scheme with probability $\leq \text{negl}(n)$

Computationally Secure Encryption

- **Syntax:**

  A symmetric-key encryption scheme is defined by PPT algorithms (Gen, Enc, Dec):

  $k \leftarrow Gen(1^n)$ — 1^n = $\underbrace{11\cdots1}_{n}$

  $c \leftarrow Enc_k(m)$ $\quad m \in \{0,1\}^*$

  $m/\perp := Dec_k(c)$

- **Correctness:** $\forall n$, $\forall k$ output by $Gen(1^n)$, $\forall m \in \{0,1\}^*$

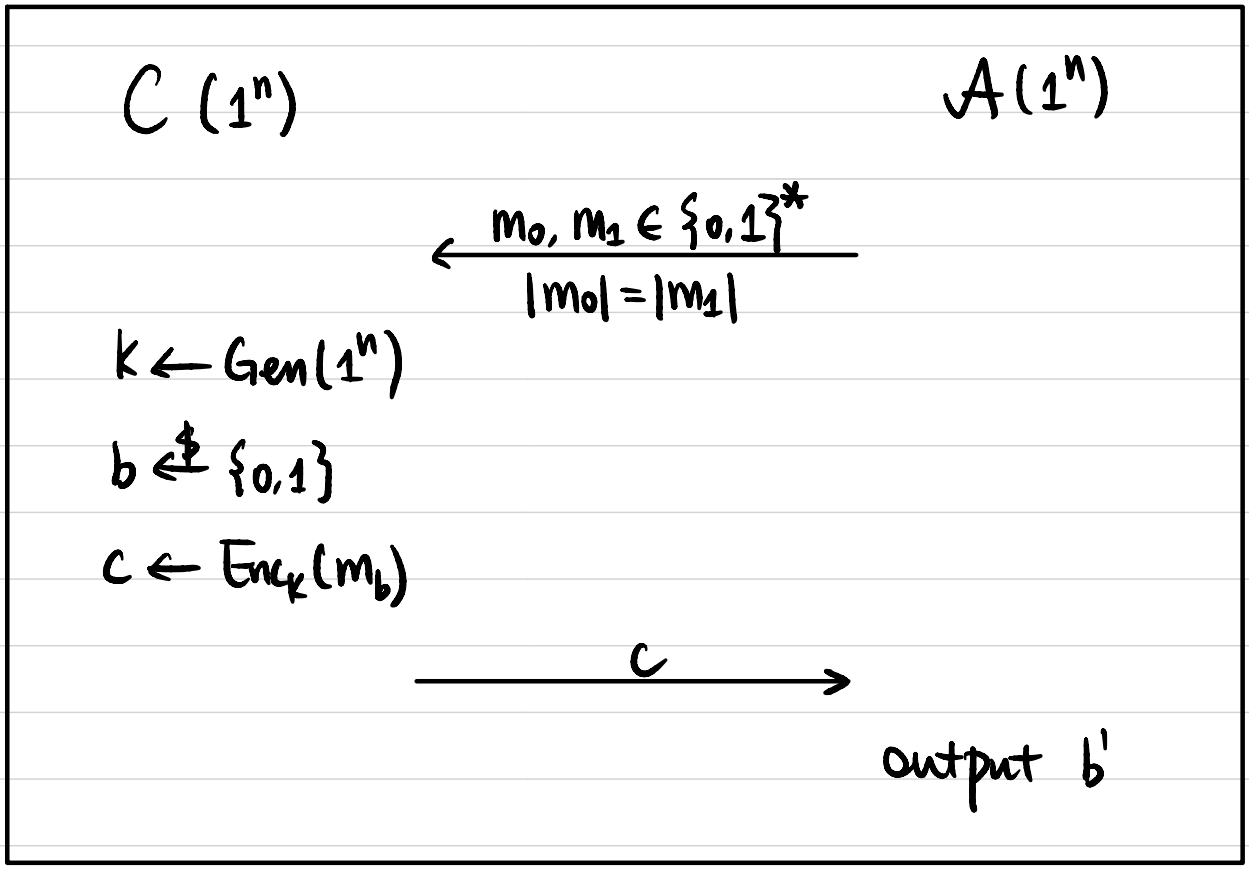
  $$Dec_k(Enc_k(m)) = m$$

Computationally Secure Encryption

Def 1 A symmetric-key encryption scheme (Gen, Enc, Dec) is **semantically secure** if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

computationally indistinguishable

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

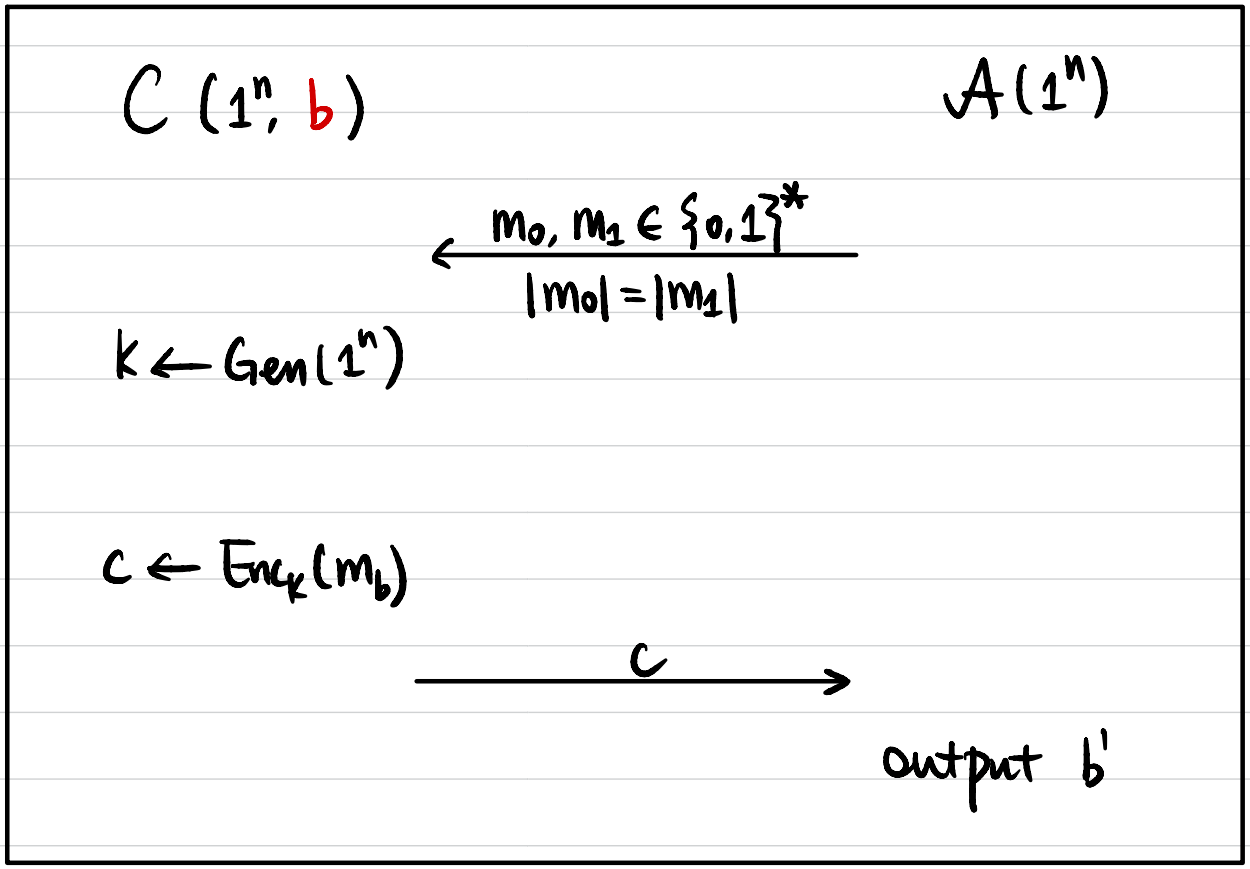


Computationally Secure Encryption

Def 2 A symmetric-key encryption scheme (Gen, Enc, Dec) is **semantically secure** if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

computationally indistinguishable

$$\left| \Pr[b' = 1 \mid b = 0] - \Pr[b' = 1 \mid b = 1] \right| \leq \varepsilon(n)$$



Computationally Secure Encryption

Def 1 A symmetric-key encryption scheme (Gen, Enc, Dec)

is semantically secure if $\forall$ PPT $\mathcal{A}$:

$$\Pr[b = b'] \leq \frac{1}{2} + \text{negl}(n)$$ in Game 1.

Def 2 $$\left|\Pr[b' = 1 \mid b = 0] - \Pr[b' = 1 \mid b = 1]\right| \leq \text{negl}(n)$$ in Game 2.

Def 1 ⇒ Def 2:

If Π is secure under Def 1, then it's also secure under Def 2.

Proof: Assume Π is not secure under Def 2, then

$\exists$ PPT A, non-negligible function $\varepsilon(\cdot)$ s.t.

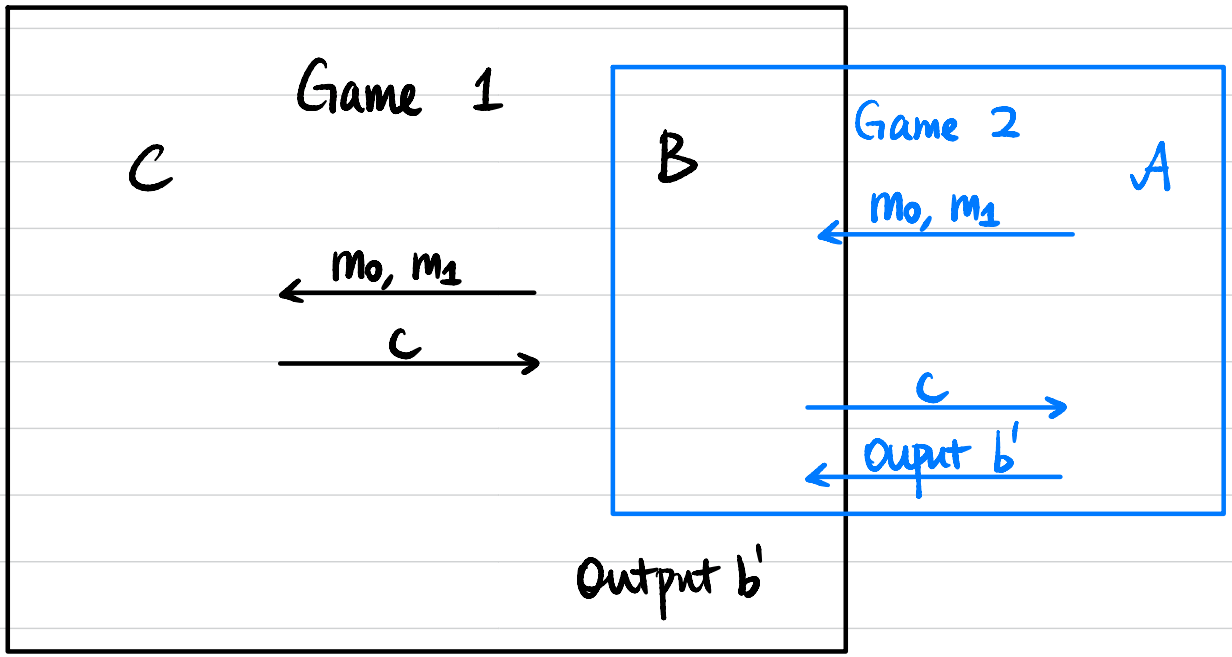
$$\left| \Pr[b'=1 \mid b=0] - \Pr[b'=1 \mid b=1] \right| \geq \varepsilon(n) \quad \text{in Game 2.}$$

$$\Pr[b'=1 \mid b=0] = \alpha \qquad \Pr[b'=1 \mid b=1] = \beta$$

$$|\alpha - \beta| \geq \varepsilon(n).$$

Assume $\beta - \alpha \geq \varepsilon(n)$:

We construct a PPT B to break Def 1



Proof (Continued):

$$\Pr[b=b' \text{ in Game 1}]$$

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

$$= \frac{1}{2} \cdot (1-\alpha) + \frac{1}{2} \cdot \beta$$

$$= \frac{1}{2} + \frac{\beta - \alpha}{2}$$

$$\geq \frac{1}{2} + \frac{\varepsilon(n)}{2}$$

↑ non-negligible

If $\alpha - \beta \geq \varepsilon(n)$: Construct B to output $1-b'$

Def 2 ⇒ Def 1 :

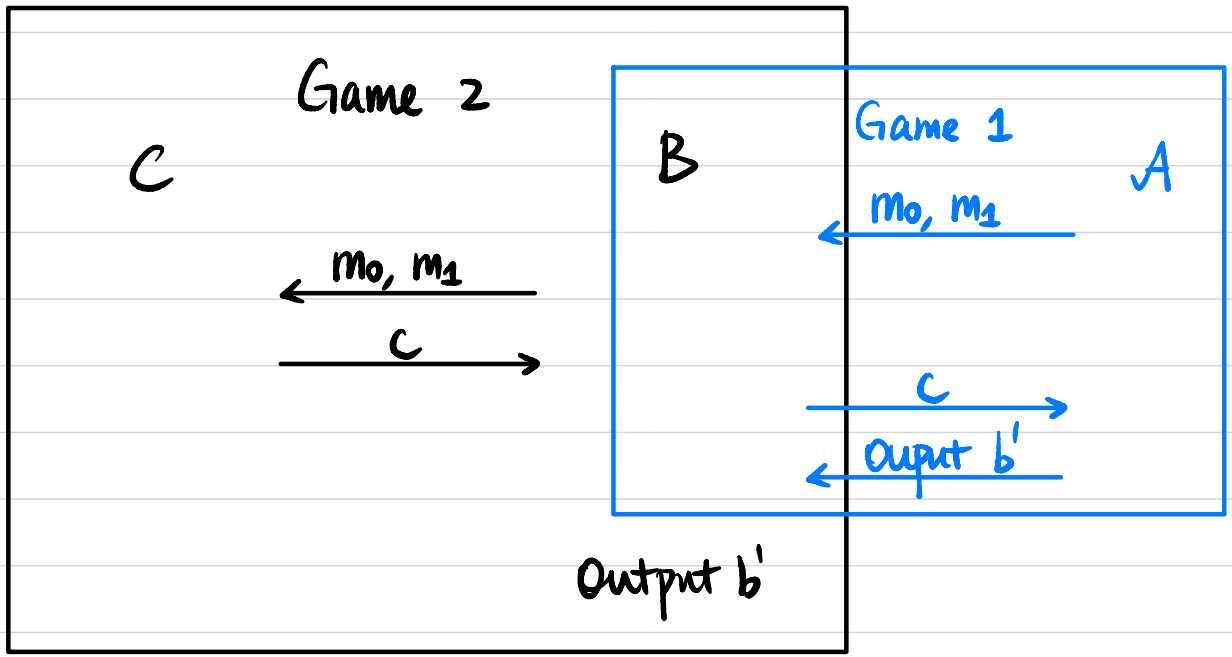
If Π is secure under Def 2, then it's also secure under Def 1.

Proof: Assume Π is not secure under Def 1, then

$\exists$ PPT A, non-negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr[b=b'] \geq \frac{1}{2} + \varepsilon(n) \quad \text{in Game 1.}$$

We construct a PPT B to break Def 2



We want to bound $\left| \Pr[b'=1 \mid b=0] - \Pr[b'=1 \mid b=1] \right|$

$\Pr[b'=1 \mid b=0] = \alpha$

$\Pr[b'=1 \mid b=1] = \beta$

Proof (Continued):

We know $\Pr[b=b' \text{ in Game 1 by } \mathcal{A}] \geq \frac{1}{2} + \varepsilon(n)$

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

$$= \frac{1}{2} \cdot (1-\alpha) + \frac{1}{2} \cdot \beta$$

$$= \frac{1}{2} + \frac{\beta - \alpha}{2}$$

$$\frac{1}{2} + \frac{\beta - \alpha}{2} \geq \frac{1}{2} + \varepsilon(n)$$

$$\Rightarrow \quad \beta - \alpha \geq 2 \cdot \varepsilon(n)$$

↑ non-negligible

$$\left| \Pr[b'=1 \mid b=0] - \Pr[b'=1 \mid b=1] \right| = |\alpha - \beta| \geq \text{non-negl}(n).$$

Constructing Secure Encryption

Pseudorandom Generator (PRG)

Semantically Secure Encryption

(Pseudo)randomness

What does it mean to be random?

Is this string random?

0 1 1 0 1 1 0 1 0 1 1 0 0 0 1

0 1 0 1 0 1 0 1 0 1 0 1 0 1 0

What does it mean to be pseudorandom?

Pseudorandomness

- Concrete Definition:

  D: a distribution over n-bit strings.

  D is (t, ε)-pseudorandom if $\forall A$ running in time $\leq t$,

$$\left| \Pr_{x \leftarrow D}[A(x) = 1] - \Pr_{x \leftarrow U_n}[A(x) = 1] \right| \leq \varepsilon$$

  U_n: uniform distribution over $\{0,1\}^n$

- Asymptotic Definition:

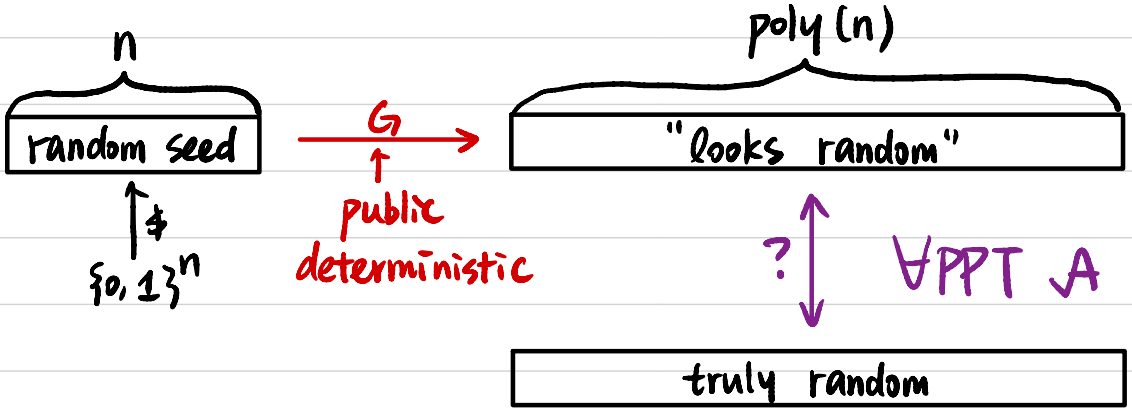
  $D = \{D_1, D_2, \cdots\}$ an ensemble of distributions,

  D_n: a distribution over n-bit string

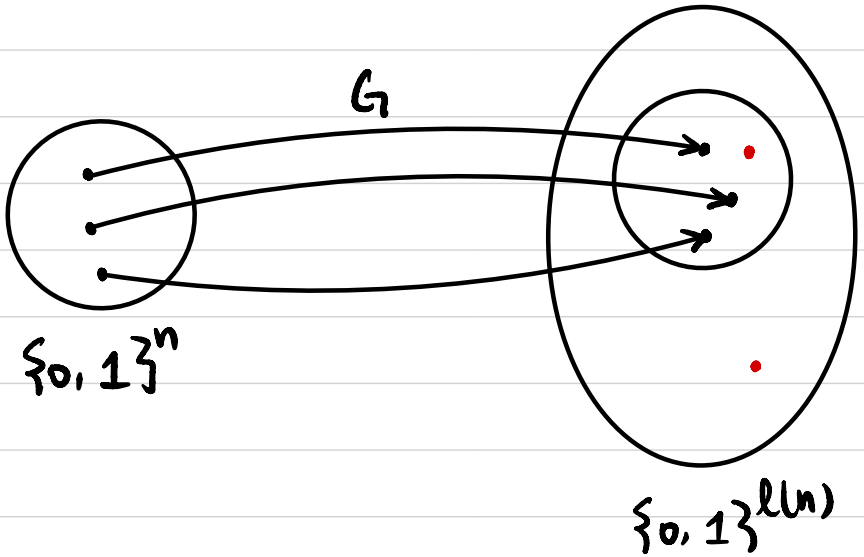
  D is pseudorandom if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\left| \Pr_{x \leftarrow D_n}[A(x) = 1] - \Pr_{x \leftarrow U_n}[A(x) = 1] \right| \leq \varepsilon(n).$$

Pseudorandom Generator (PRG)



$G: \{0,1\}^n \to \{0,1\}^{\ell(n)} \quad \ell(n) > n$



Pseudorandom Generator (PRG)

$G: \{0,1\}^n \to \{0,1\}^{\ell(n)} \quad \ell(n) > n$

Def 1 G is a pseudorandom generator (PRG) if

$\forall$ PPT A, $\exists$ negligible function $\text{negl}(\cdot)$ s.t.

$$\left| \Pr_{s \leftarrow U_n} [A(G(s)) = 1] - \Pr_{x \leftarrow U_{\ell(n)}} [A(x) = 1] \right| \leq \text{negl}(n)$$

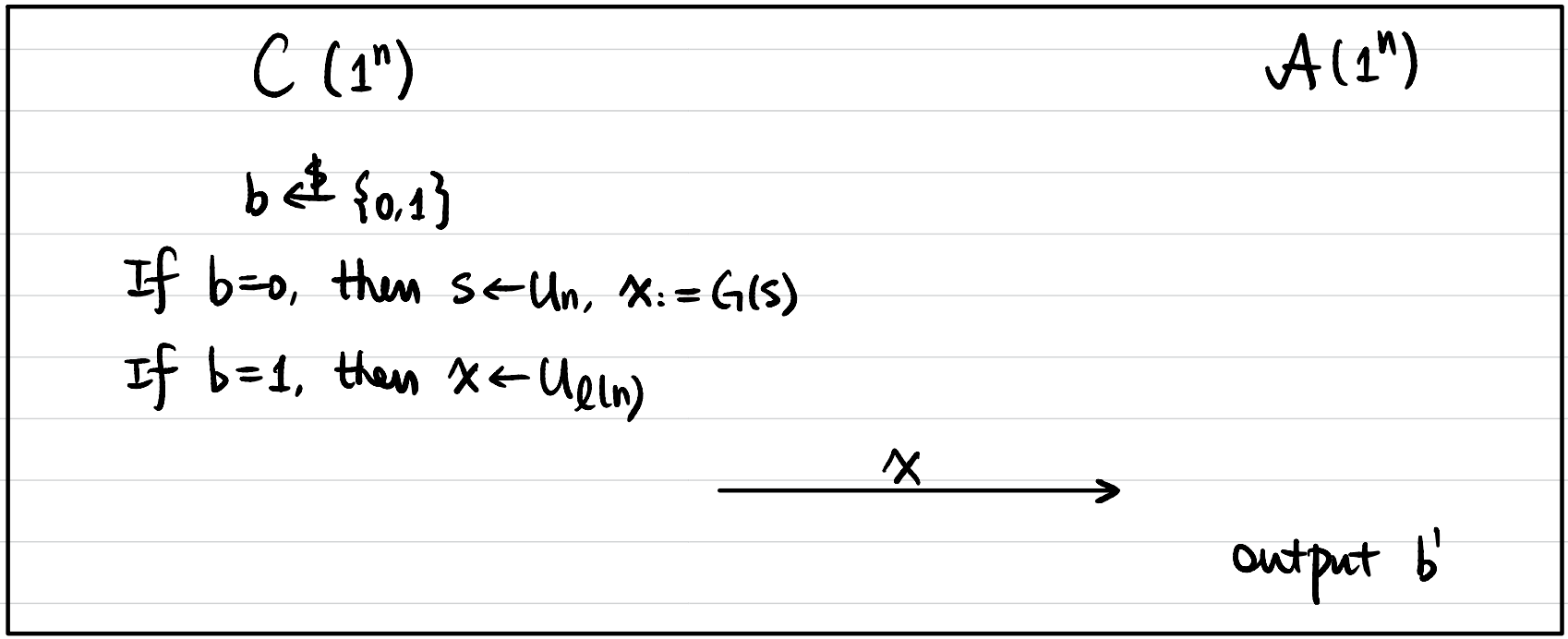
Pseudorandom Generator (PRG)

$G: \{0,1\}^n \to \{0,1\}^{\ell(n)} \quad \ell(n) > n$

Def 2 G is a pseudorandom generator (PRG) if

$\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\text{negl}(\cdot)$ s.t.

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



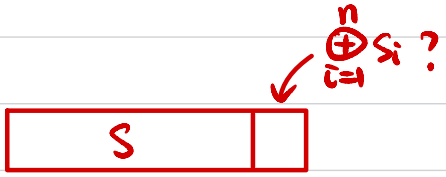
What if $\mathcal{A}$ is computationally unbounded?

Exercises

$$G(s) = s \,||\, \bigoplus_{i=1}^{n} s_i$$

↑ concatenation

Is G a secure PRG ? No !

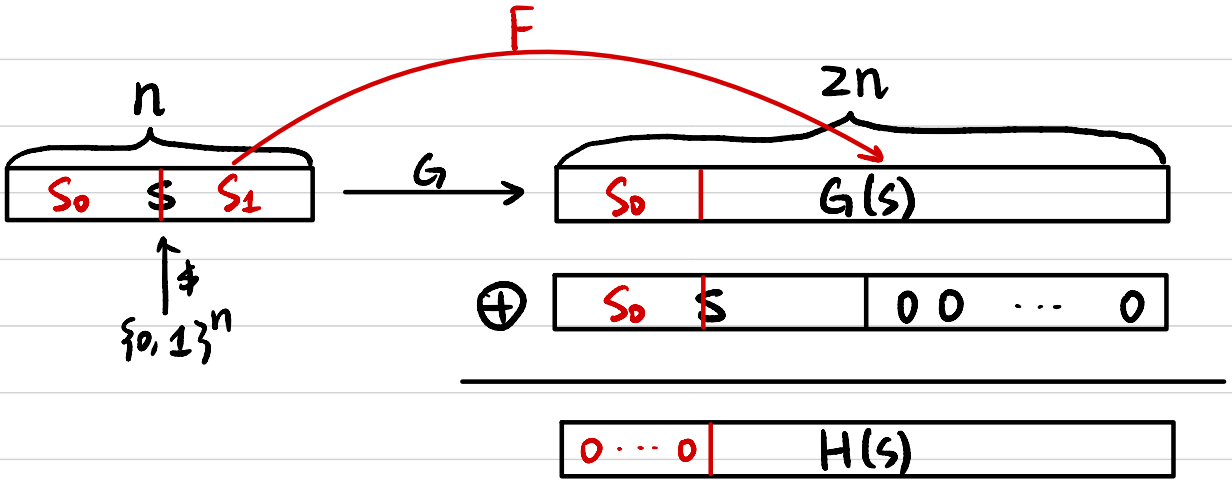


Exercises

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

Construct $H: \{0,1\}^n \to \{0,1\}^{2n}$ as $H(s) := G(s) \oplus (s \| 0^n)$.

Is H necessarily a PRG?



If yes ⇒ prove: ∀ PRG G, H is also a PRG

If no ⇒ show counterexample ∃ PRG G, H is not a PRG.

Assume $F: \{0,1\}^{n/2} \to \{0,1\}^{3n/2}$ is a PRG.

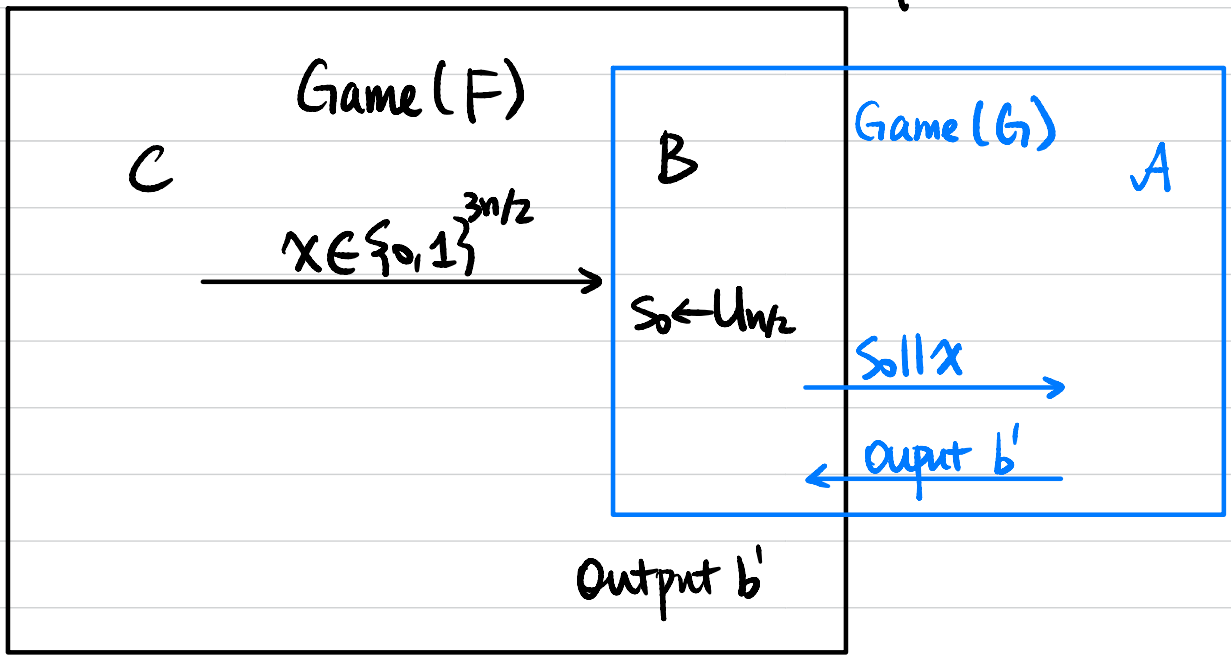
Construct G as $G(s_0 \| s_1) := s_0 \| F(s_1)$

$s_0, s_1 \in \{0,1\}^{n/2}$

① G is a PRG.

Assume not. Then $\exists$ PPT $\mathcal{A}$ that breaks the pseudorandomness of G.

We construct a PPT B to break the pseudorandomness of F.



If $b=0$, $s_0 \| x \leftarrow G(U_n)$

If $b=1$, $s_0 \| x \leftarrow U_{2n}$

$\Pr[b=b' \text{ in Game}(F) \text{ by } B]$

$= \Pr[b=b' \text{ in Game}(G) \text{ by } \mathcal{A}]$

$\geq$ non-negl(n).

② H is not a PRG.

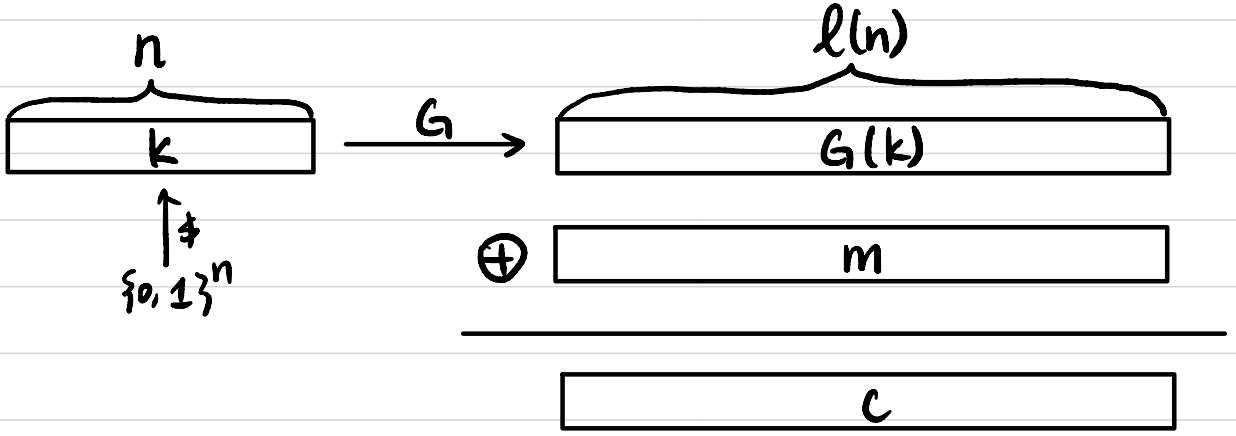
$\exists$ PPT $\mathcal{A}$: on input $x \in \{0,1\}^{2n}$, if first $n/2$ bits are all 0, then output 0;

otherwise output 1.

Fixed-Length Encryption Scheme

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

- $\text{Gen}(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $\text{Enc}_k(m)$: $m \in \{0,1\}^{\ell(n)}$.
  output $c := G(k) \oplus m$.
- $\text{Dec}_k(c)$: $c \in \{0,1\}^{\ell(n)}$,
  output $m := G(k) \oplus c$.



"pseudo OTP"

Proof of Security

Theorem If G is a PRG, then $\Pi = (Gen, Enc, Dec)$ is semantically secure for fixed-length messages.

Assume Π is not semantically secure, then

$\exists$ PPT A that breaks Π

↳ construct PPT B to break G.