

CSCI 1510

This Lecture:

- 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 $\leq \epsilon$.

- 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 $(\text{Gen}, \text{Enc}, \text{Dec})$:

$$k \leftarrow \text{Gen}(1^n)$$

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

$$m/\perp := \text{Dec}_k(c)$$

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

$$\text{Dec}_k(\text{Enc}_k(m)) = m$$

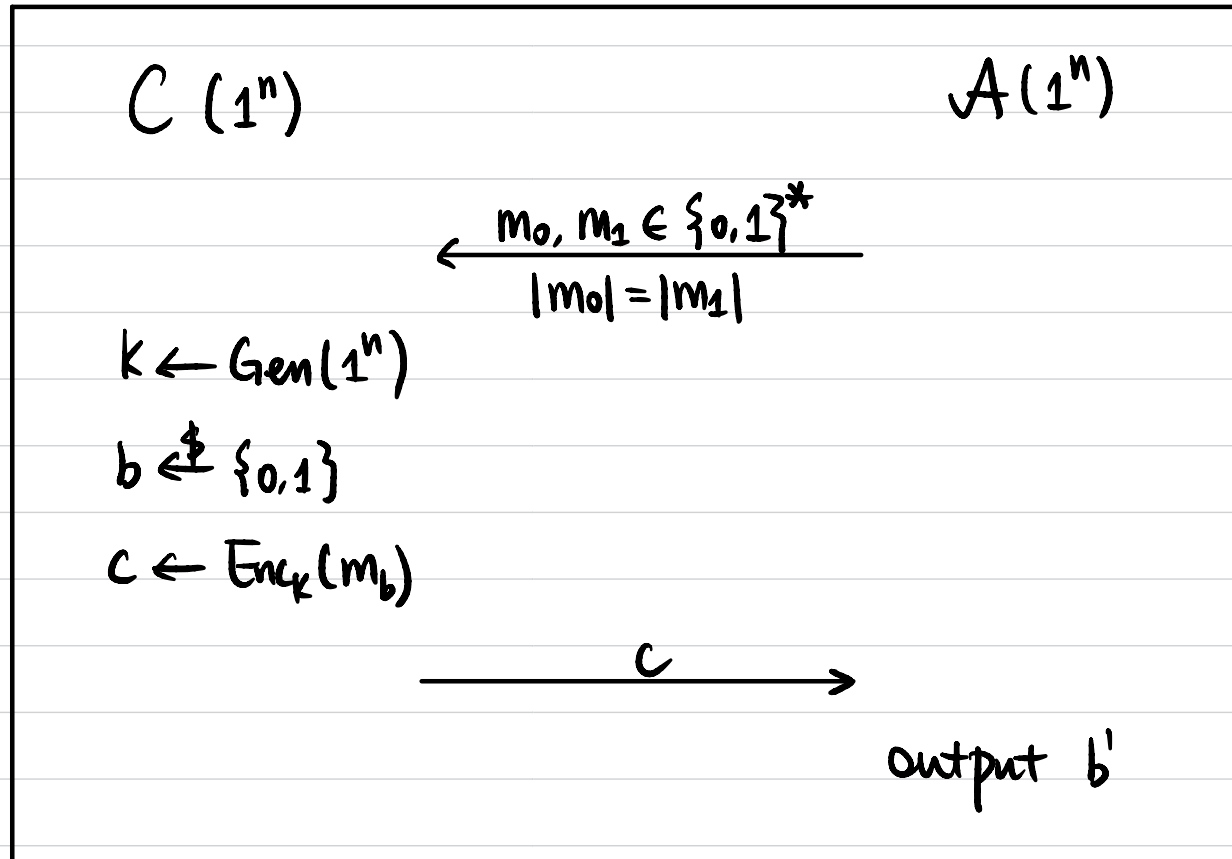
Computationally Secure Encryption

Def 1 A symmetric-key encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$

is **semantically secure** if $\forall \text{PPT } A, \exists \text{ negligible function } \epsilon(\cdot)$ s.t.

computationally
indistinguishable

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



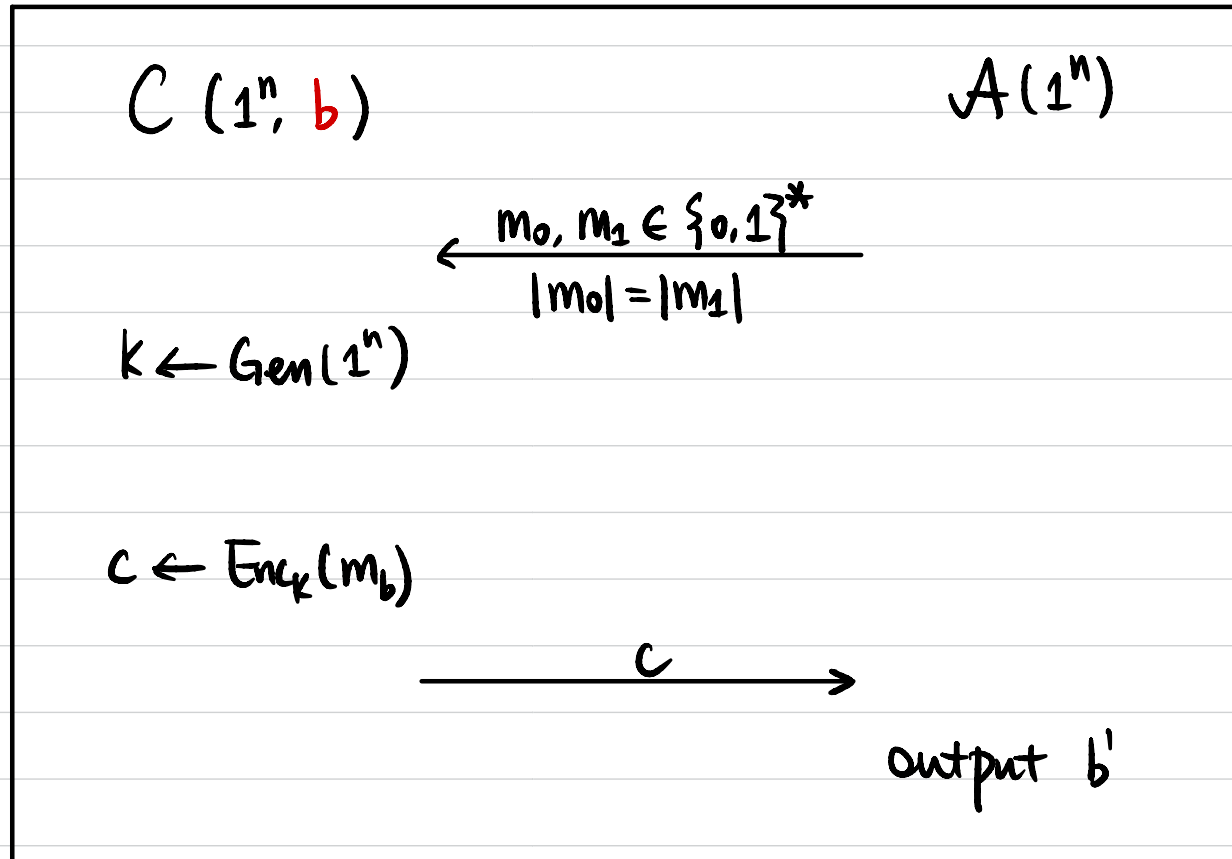
Computationally Secure Encryption

Def 2 A symmetric-key encryption scheme (Gen, Enc, Dec)

is **semantically secure** if $\forall$ PPT A , $\exists$ negligible function $\epsilon(\cdot)$ s.t.

computationally
indistinguishable

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



Computationally Secure Encryption

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

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



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

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 $\Rightarrow$ Def 2: If $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is secure under Def 1,
then Π is also secure under Def 2.

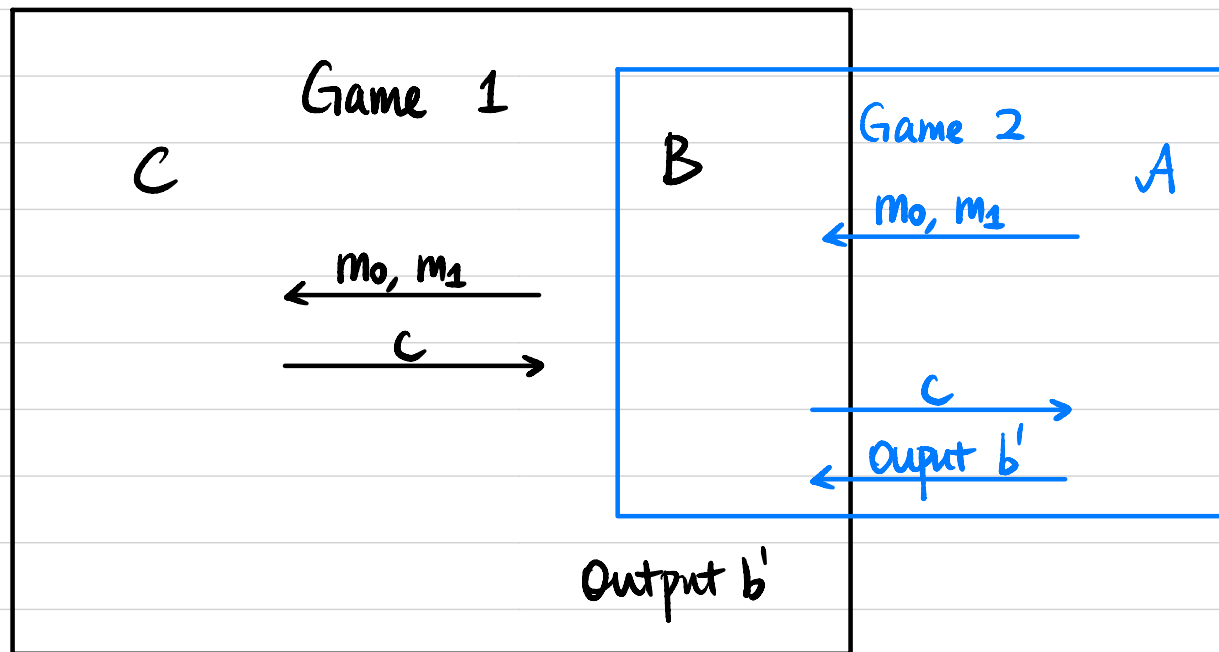
Proof: Assume Π is not secure under Def 2, then
 $\exists$ PPT A , non-negligible function $\gamma(\cdot)$ s.t.

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

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

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

We construct a PPT B to break Def 1



Proof (Continued):

$$\begin{aligned} & \Pr[b=b' \text{ in Game 1}] \\ &= \Pr[b=0] \cdot \Pr[b'=0 | b=0] + \Pr[b=1] \cdot \Pr[b'=1 | b=1] \\ &= \frac{1}{2} \cdot (1-\alpha) + \frac{1}{2} \cdot \beta \\ &= \frac{1}{2} + \frac{\beta-\alpha}{2} \\ &\geq \frac{1}{2} + \frac{\gamma(n)}{2} \\ & \quad \uparrow \\ & \quad \text{non-negligible} \end{aligned}$$

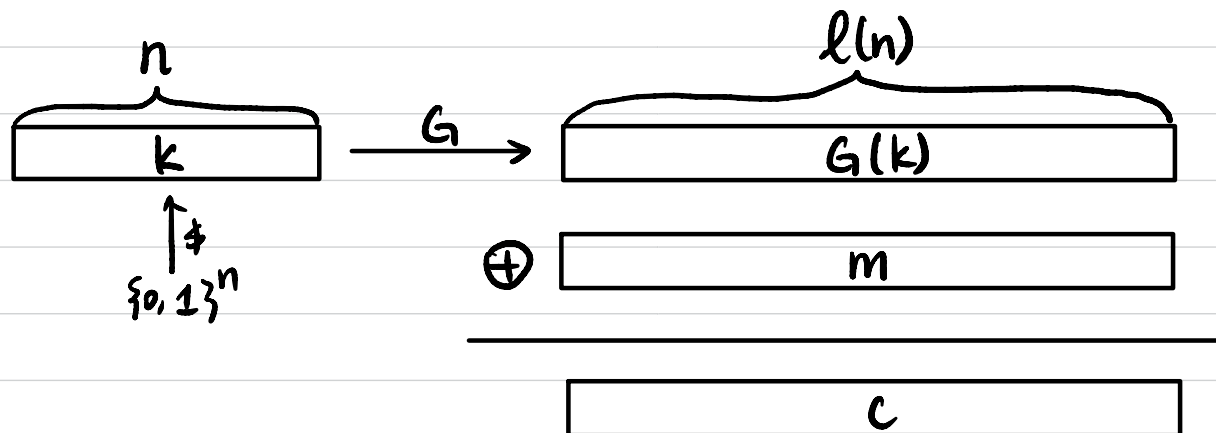
If $\alpha - \beta \geq \gamma(n)$: Construct B to output $1-b'$

Constructing Secure Encryption

Pseudorandom Generator (PRG)



Semantically Secure Encryption



"pseudo OTP"

(Pseudo)randomness

What does it mean to be random?

Is this string random?

011011010110001
010101010101010

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 $\leq t$,

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

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

- Asymptotic Definition:

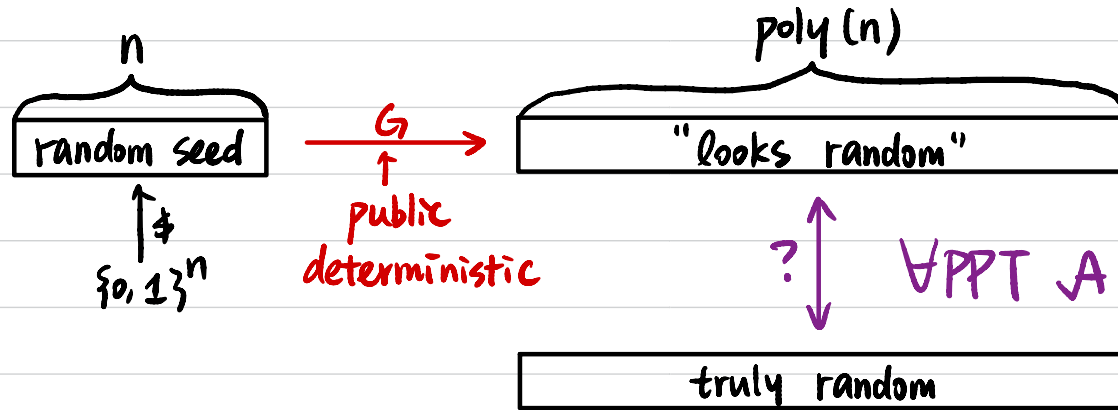
$D = \{D_1, D_2, \dots\}$ an ensemble of distributions,

D_n : a distribution over n -bit string.

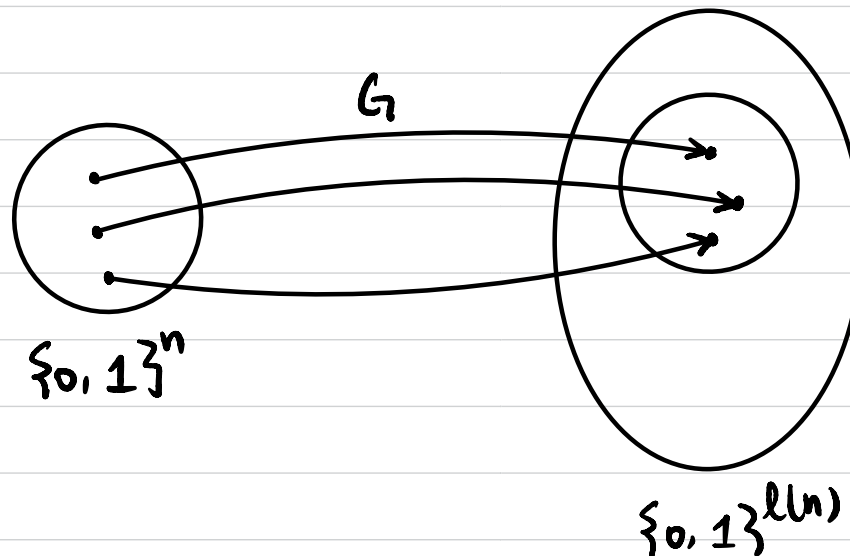
D is pseudorandom if $\forall$ PPT A , $\exists$ negligible function $\epsilon(\cdot)$ s.t.

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

Pseudorandom Generator (PRG)



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



Pseudorandom Generator (PRG)

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

Def 1 G is a pseudorandom generator (PRG) if

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

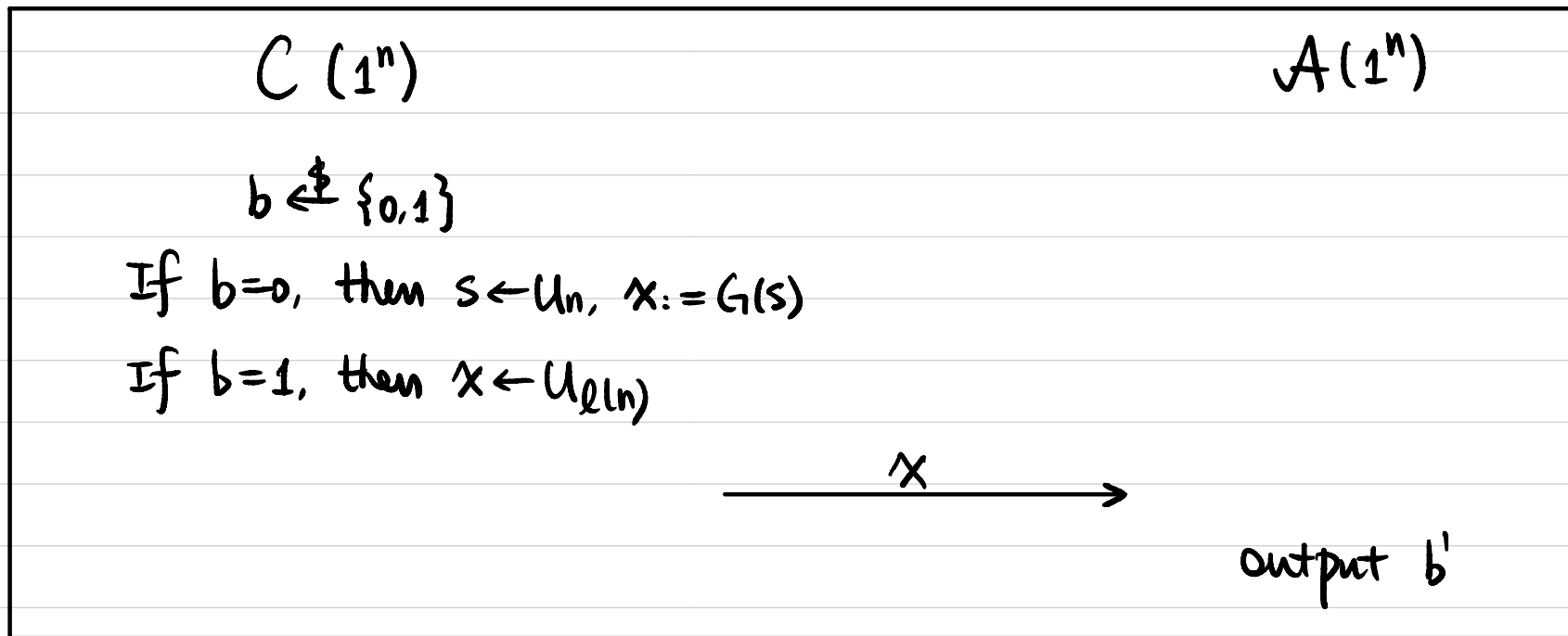
$$\left| \Pr_{s \leftarrow U_n} [A(G(s)) = 1] - \Pr_{x \leftarrow U_{\ell(n)}} [A(x) = 1] \right| \leq \text{negl}(n)$$

Pseudorandom Generator (PRG)

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

Def 2 G is a pseudorandom generator (PRG) if
 $\forall$ PPT A , $\exists$ negligible function $\text{negl}(\cdot)$ s.t.

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



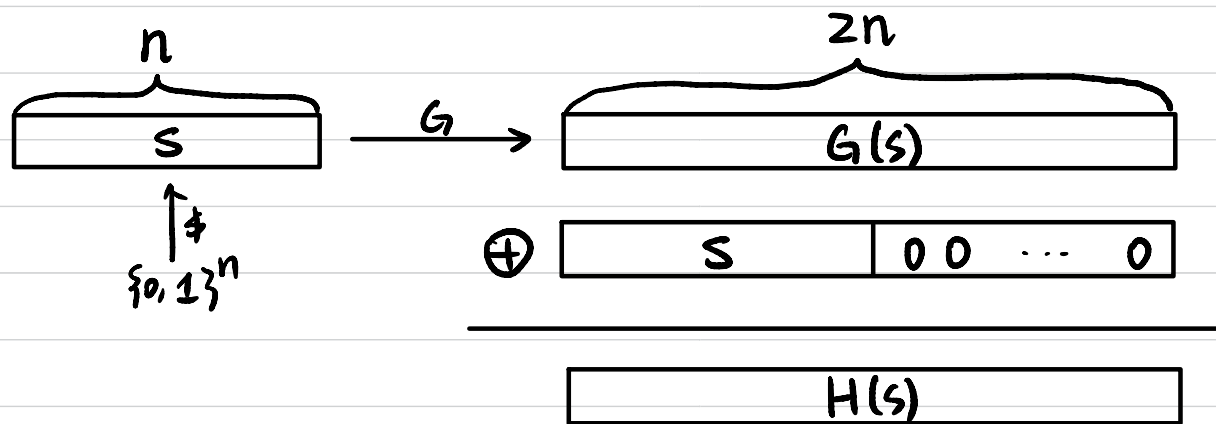
What if A is computationally unbounded?

Exercise

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

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

Is H necessarily a PRG?



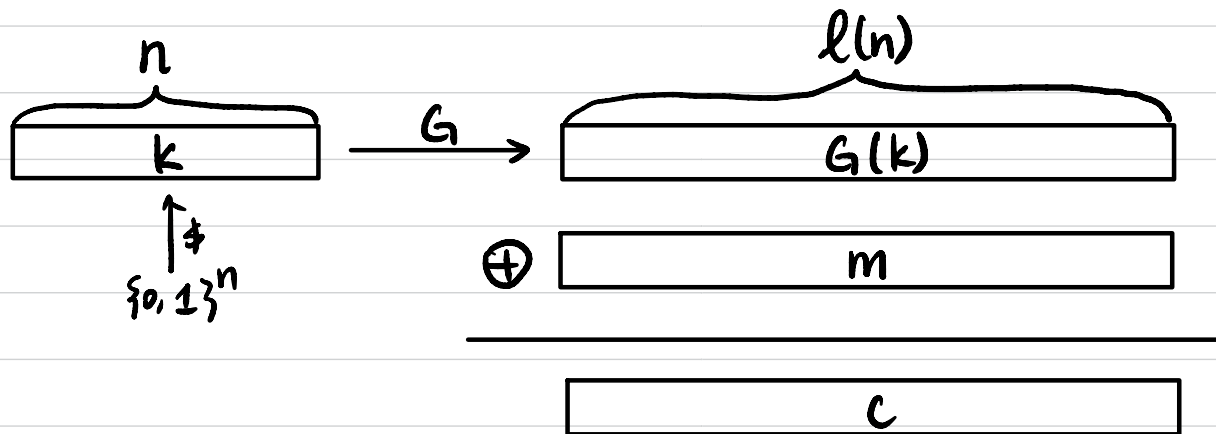
If yes $\Rightarrow$ prove: $\forall$ PRG G , H is also a PRG

If no $\Rightarrow$ show counterexample $\exists$ PRG G , H is not a PRG.

Fixed-Length Encryption Scheme

Let $G: \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$ 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 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ 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 .