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 $\leq \varepsilon$.

- Asymptotic Approach:

  Introduce a security parameter n

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

Computationally Secure Encryption

- **Syntax:**

  A symmetric-key encryption scheme is defined by PPT algorithms $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$:

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

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

$$m/\bot := \mathrm{Dec}_k(c)$$

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

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

Computationally Secure Encryption

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

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

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

computationally indistinguishable

$C(1^n)$		$\mathcal{A}(1^n)$
	$\xleftarrow[|m_0| = |m_1|]{m_0, m_1 \in \{0,1\}^*}$
$k \leftarrow Gen(1^n)$	
$b \xleftarrow{\$} \{0,1\}$	
$c \leftarrow Enc_k(m_b)$	
	$\xrightarrow{c}$
		output b'

Computationally Secure Encryption

$\exists$ PPT $\mathcal{A}$, let $Y(n)$ be $\left| \Pr[b'=1 \mid b=0] - \Pr[b'=1 \mid b=1] \right|$, then $Y(n)$ must be non-negligible.

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

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

$C(1^n, b)$ $\qquad\qquad\qquad$ $\mathcal{A}(1^n)$

$$\xleftarrow[|m_0| = |m_1|]{m_0, m_1 \in \{0,1\}^*}$$

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

$c \leftarrow \mathrm{Enc}_k(m_b)$

$$\xrightarrow{\quad c \quad}$$

output b'

Computationally Secure Encryption

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

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

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

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

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

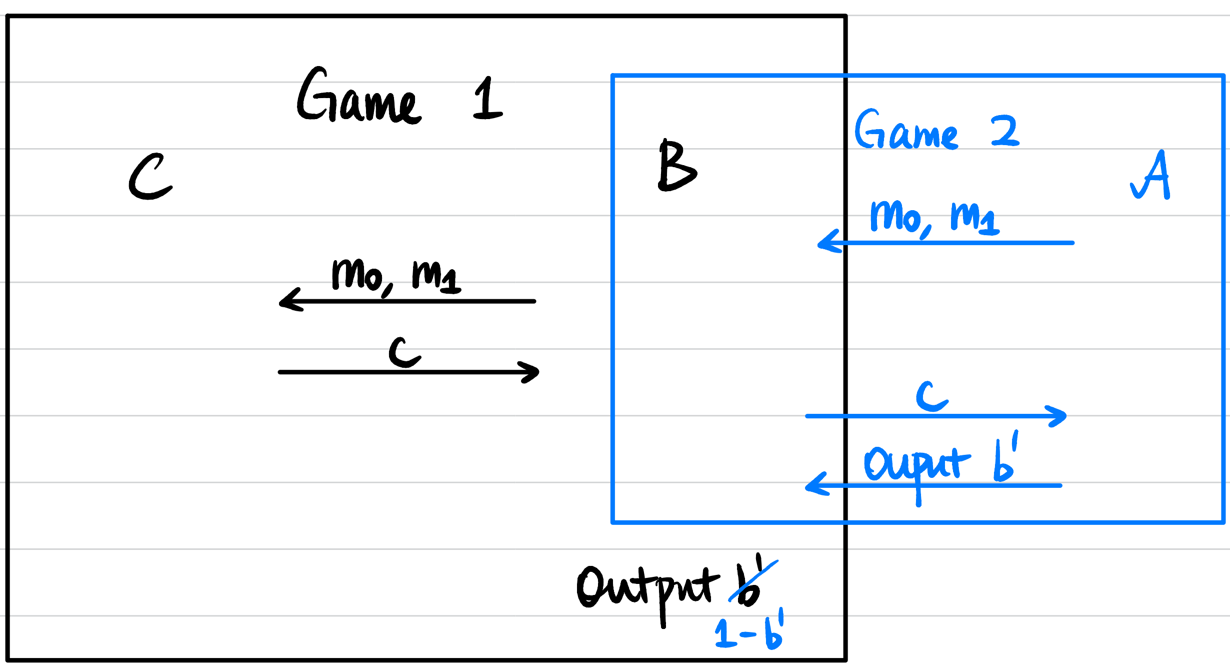
Proof: Assume Π is not secure under Def 2, then $\exists$ PPT $\mathcal{A}$, non-negligible function $\gamma(\cdot)$ s.t.

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

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

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

We construct a PPT $\mathcal{B}$ to break Def 1



Proof (Continued):

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

$$= \Pr[b=0]\cdot\Pr[b'=\cancel{0}^{\,1} \mid b=0] + \Pr[b=1]\cdot\Pr[b'=\cancel{1}^{\,0} \mid b=1]$$

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

$$= \frac{1}{2} + \frac{\beta-\alpha}{2} \qquad = \frac{1}{2} + \underbrace{\frac{\alpha-\beta}{2}}_{\text{non-negligible}}$$

$$\geq \frac{1}{2} + \underbrace{\frac{\gamma(n)}{2}}_{\text{non-negligible}}$$

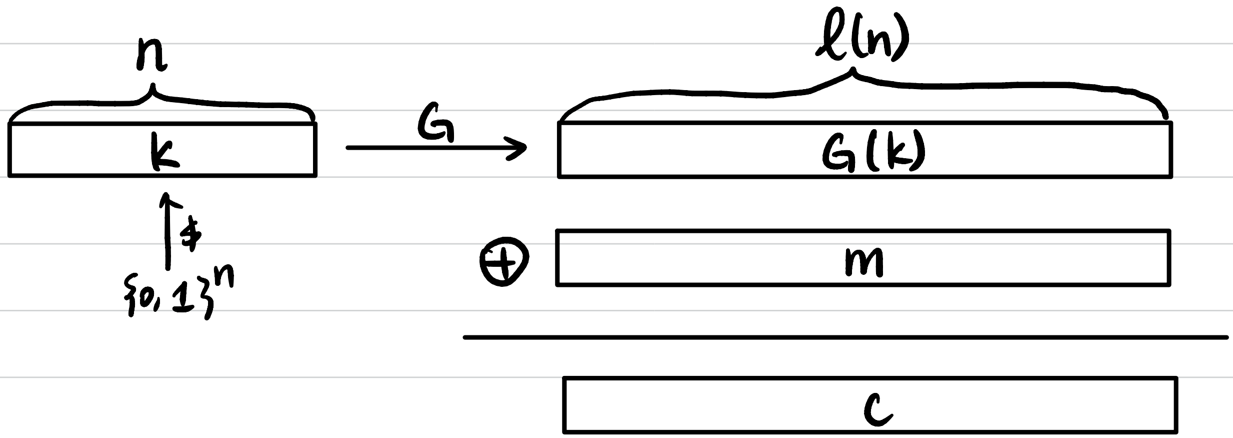
If $\alpha-\beta \geq \gamma(n)$: Construct B to output $1-b'$

Constructing Secure Encryption

Pseudorandom Generator (PRG)

$$\Downarrow$$

Semantically Secure Encryption



"pseudo OTP"

(Pseudo)randomness

What does it mean to be random?

Is this string random?

0110110101100001

0101010101010101

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 $\leq t$,

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

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

- Asymptotic Definition:

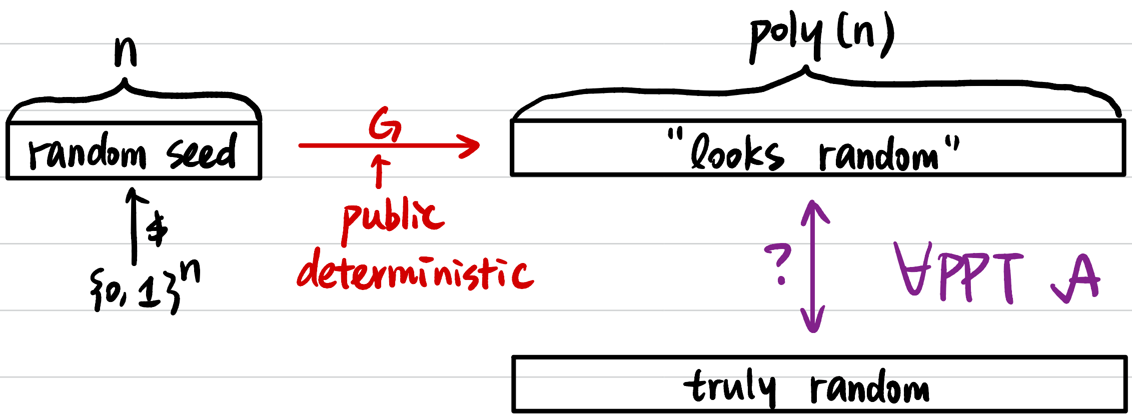
  $D = \{D_1, D_2, \cdots\}$ an ensemble of distributions,

  D_n: a distribution over n-bit string.

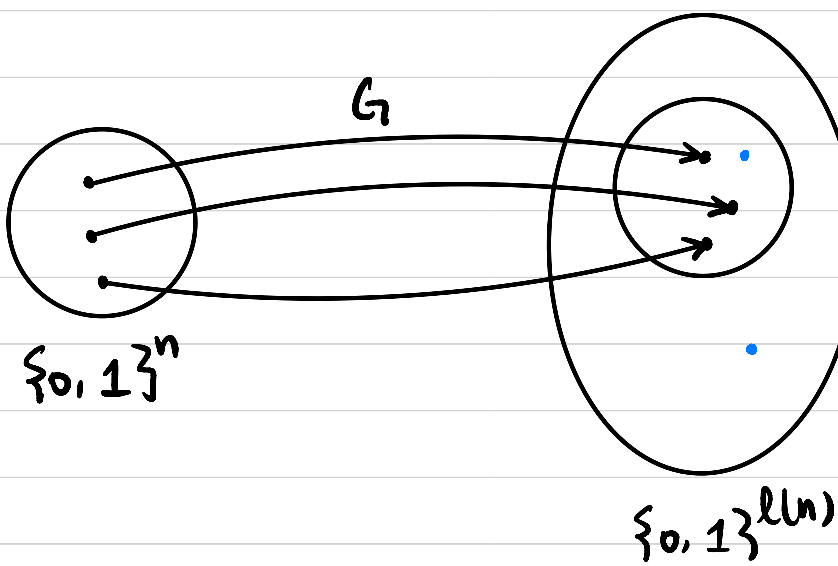
  D is pseudorandom if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

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

Pseudorandom Generator (PRG)



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



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

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

Pseudorandom Generator (PRG)

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

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

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

$C(1^n)$		$\mathcal{A}(1^n)$
$b \xleftarrow{\$} \{0,1\}$		
If $b=0$, then $s \leftarrow U_n$, $x := G(s)$		
If $b=1$, then $x \leftarrow U_{\ell(n)}$		
	$\xrightarrow{x}$	
		output b'

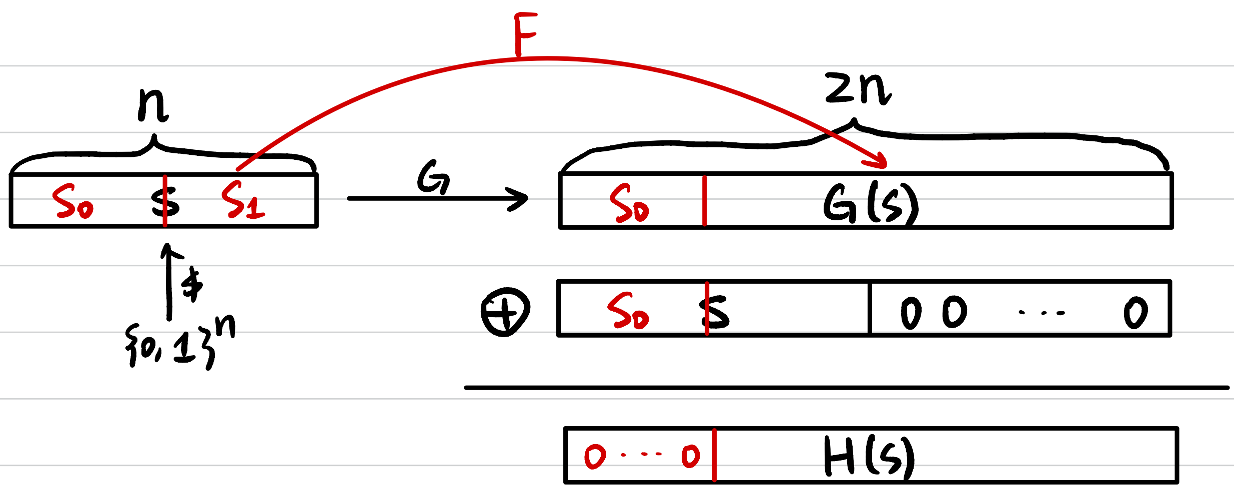
What if $\mathcal{A}$ is computationally unbounded?

Exercise

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

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

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

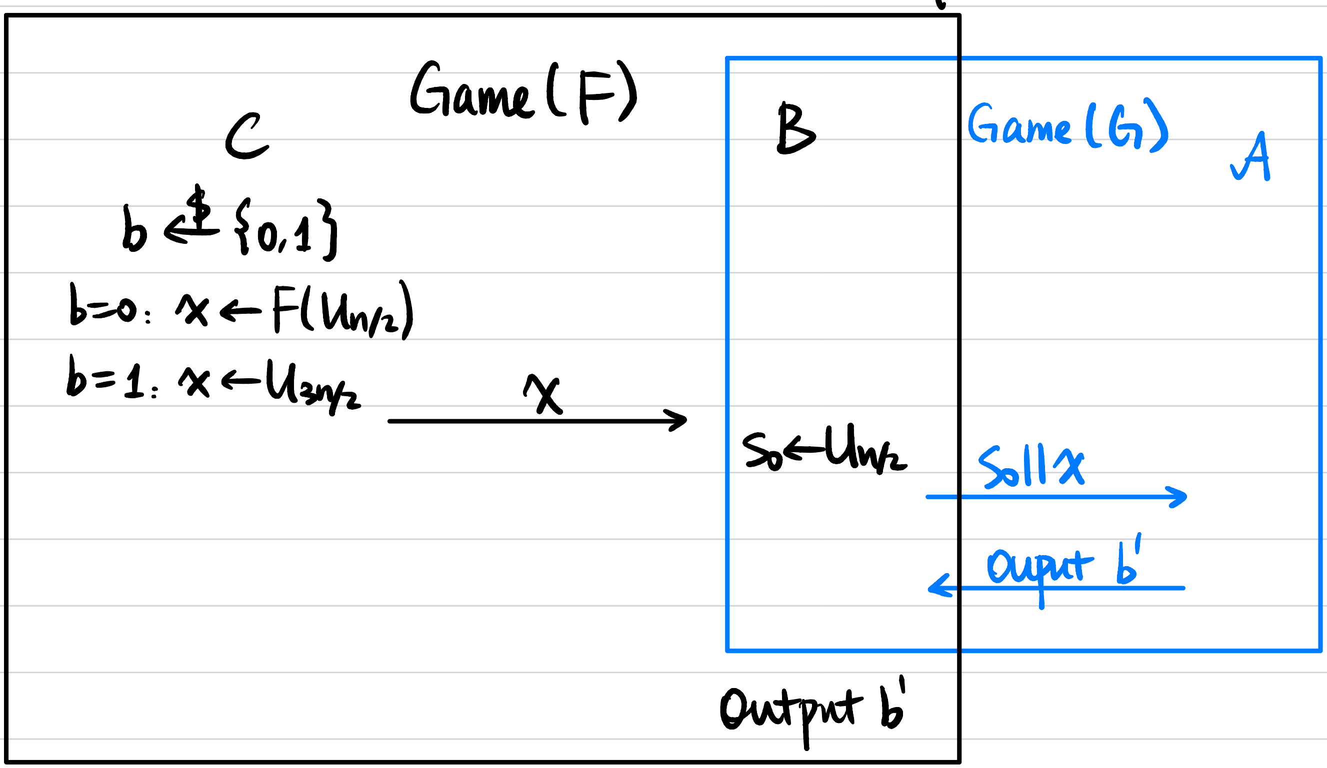
Construct G as $G(s_0 \| s_1) := s_0 \| F(s_1)$

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

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

$\Pr[b=b' \text{ in Game}(F) \text{ by } B] = \Pr[b=b' \text{ in Game}(G) \text{ by } \mathcal{A}] \geq \text{non-negl}(n)$.

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.

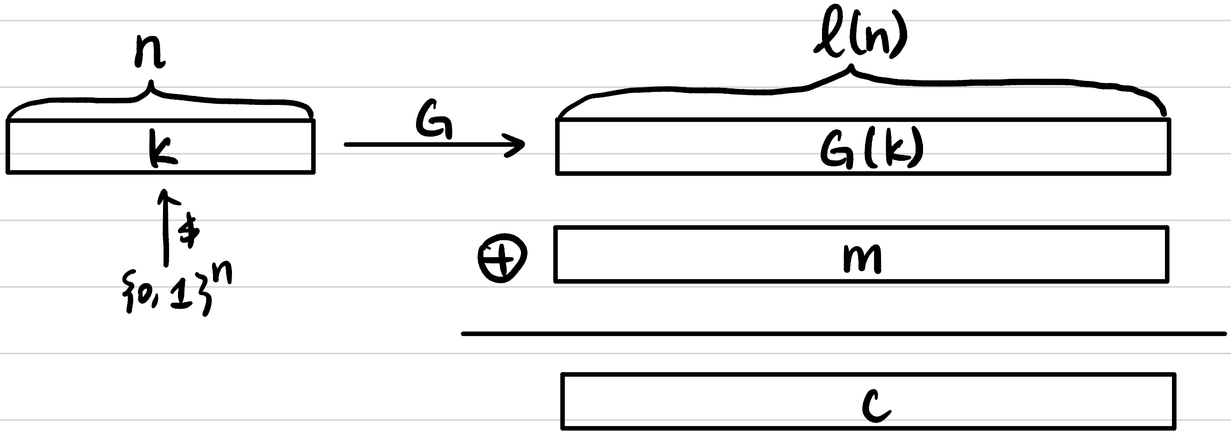
$$\left| \Pr_{s \leftarrow U_n} [\mathcal{A}(H(s)) = 1] - \Pr_{x \leftarrow U_{\ell(n)}} [\mathcal{A}(x) = 1] \right| = 1 - 2^{-n/2} \geq \text{non-negl}(n).$$

$$\Pr_{s \leftarrow U_n} [\mathcal{A}(H(s)) = 1] = 0, \qquad \Pr_{x \leftarrow U_{\ell(n)}} [\mathcal{A}(x) = 1] = 1 - 2^{-n/2}$$

Fixed-Length Encryption Scheme

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

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

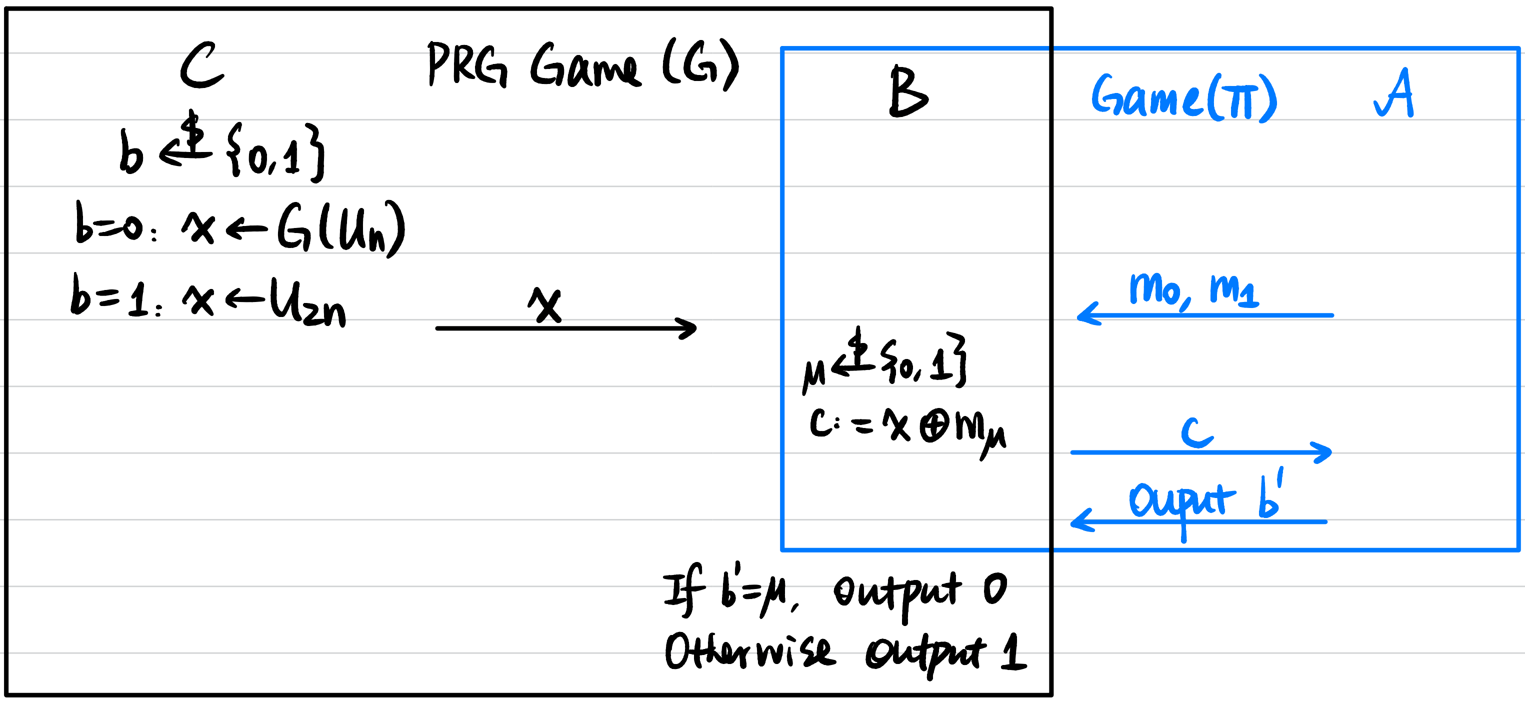


"pseudo OTP"

Proof of Security

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

Proof Assume Π is not semantically secure, then $\exists$ PPT $\mathcal{A}$ that breaks Π. We construct PPT B to break the pseudorandomness of G.



$$\Pr[B \text{ guesses Correctly}] = \Pr[b=0]\cdot\Pr[b'=\mu \mid b=0] + \Pr[b=1]\cdot\Pr[b'\neq\mu \mid b=1]$$

$$= \frac{1}{2}\cdot\Pr[\mathcal{A} \text{ guesses correctly in the security game of } \Pi] + \frac{1}{2}\cdot\frac{1}{2}$$

$$\geq \frac{1}{2}\cdot\left(\frac{1}{2} + \text{non-negl}(n)\right) + \frac{1}{4} = \frac{1}{2} + \frac{1}{2}\cdot\text{non-negl}(n).$$

Does Pseudo OTP allow encryption of multiple messages?

$$\left.\begin{array}{l} c_1 = G(k) \oplus m_1 \\ c_2 = G(k) \oplus m_2 \end{array}\right\rangle \oplus \rightarrow m_1 \oplus m_2$$