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 $\forall \mathcal{A}$ 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 $\forall \mathcal{A}$ 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 $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$:

  $\underbrace{11\cdots 1}_{n}$

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

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

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

- **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.

computationally indistinguishable

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

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

Computationally Secure Encryption

Def 2 A symmetric-key encryption scheme $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$

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

computationally indistinguishable

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

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

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

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

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

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

output b'

Computationally Secure Encryption

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

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

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

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

Def 1 $\Rightarrow$ Def 2: If Π is secure under Def 1, then it's also secure under Def 2.

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

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

use $\mathcal{A}$ to break Def 1

Computationally Secure Encryption

Def 1 A symmetric-key encryption scheme (Gen, Enc, Dec) is semantically secure if $\forall$ PPT $\mathcal{A}$:

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

$\Updownarrow$

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

Def 2 $\Rightarrow$ Def 1: If Π is secure under Def 2, then it's also secure under Def 1.

Assume Π is not secure under Def 1, then $\exists$ PPT $\mathcal{A}$, non-negligible function $\varepsilon(\cdot)$ s.t.

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

use $\mathcal{A}$ to break Def 2.

Constructing Secure Encryption

Pseudorandom Generator (PRG)

$\Downarrow$

Semantically Secure Encryption

(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 $\forall \mathcal{A}$ running in time $\le t$,

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

- Asymptotic Definition:

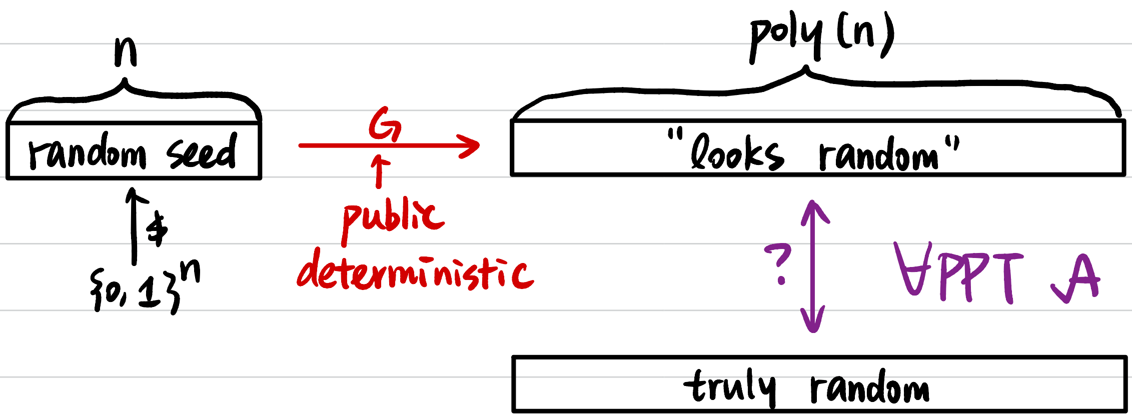
  $D = \{D_1, D_2, \cdots\}$ an ensemble of distributions,

  D_n: a distribution over n-bit string.

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

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

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 $\text{negl}(\cdot)$ s.t.

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

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

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

If $b=0$, then $s \leftarrow U_n$, $x := G(s)$

If $b=1$, then $x \leftarrow U_{\ell(n)}$

$\xrightarrow{\quad x \quad}$

output b'

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

Exercises

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

Concatenation

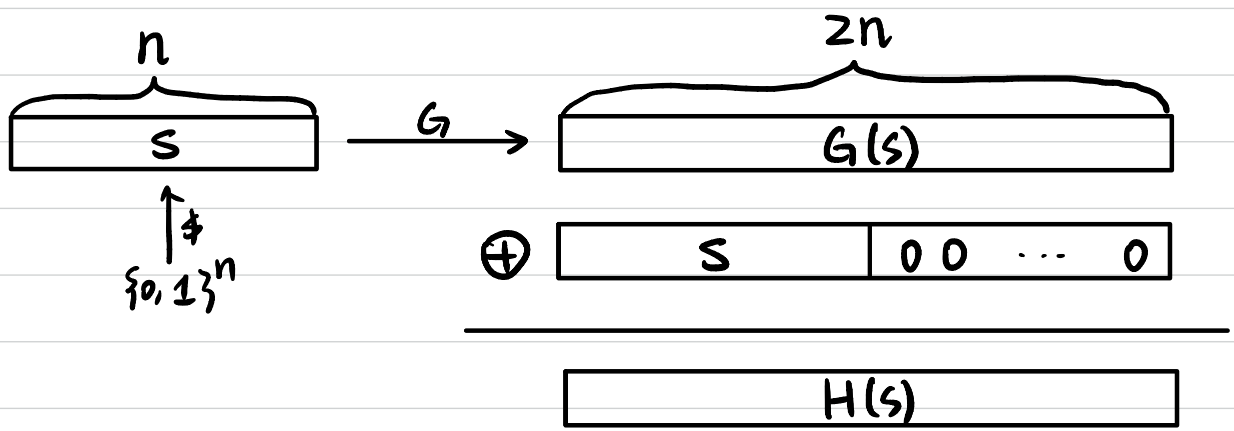
Is G a secure PRG?

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?



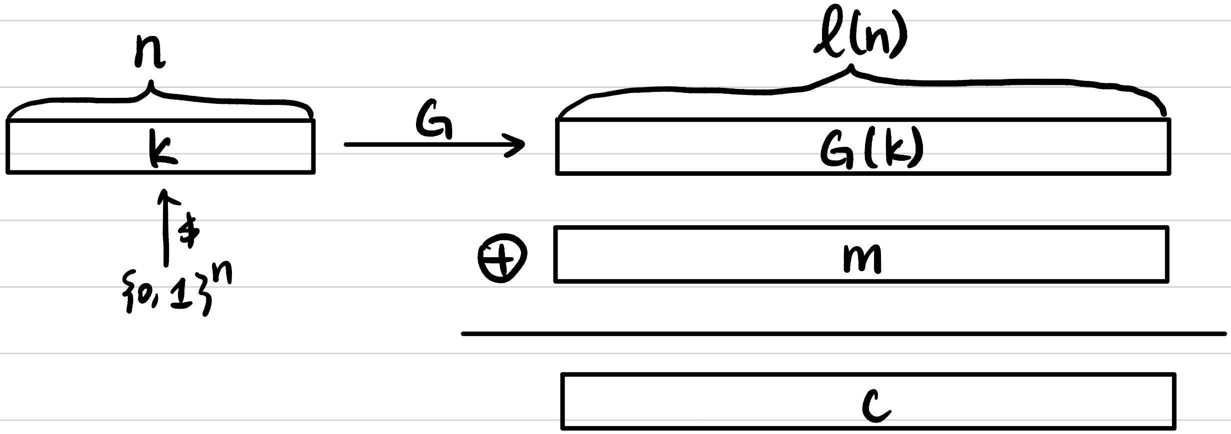
If yes $\Rightarrow$ prove: $\forall$ PRG G, H is also a PRG

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

Fixed-Length Encryption Scheme

Let $G: \{0,1\}^n \to \{0,1\}^{\ell(n)}$ 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 $\Pi = (Gen, Enc, Dec)$ is semantically secure for fixed-length messages.

Assume Π is not semantically secure, then

$\exists$ PPT $\mathcal{A}$ that breaks Π

↳ Construct PPT B to break G.