CSCI 1510

- Fixed-Length Encryption from PRG (continued)
- CPA Security
- Pseudorandom Function (PRF)

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.

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

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

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

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

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

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

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

output b'

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.

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

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

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

$k \leftarrow Gen(1^n)$

$c \leftarrow Enc_k(m_b)$

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

output b'

Pseudorandom Generator (PRG)

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

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)

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

Def 2 G is a pseudorandom generator (PRG) if

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

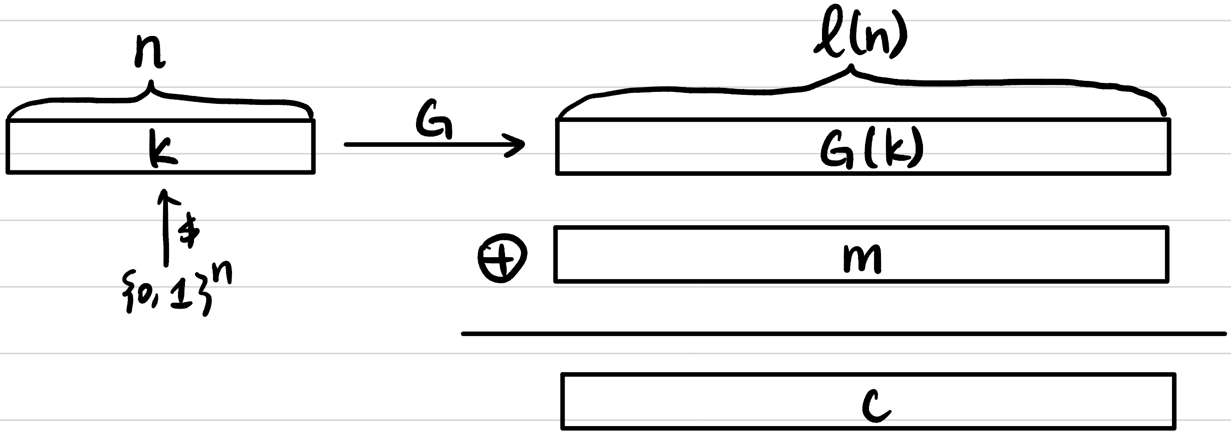
$$\Pr[b = b'] \le \frac{1}{2} + \mathrm{negl}(n)$$

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

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.

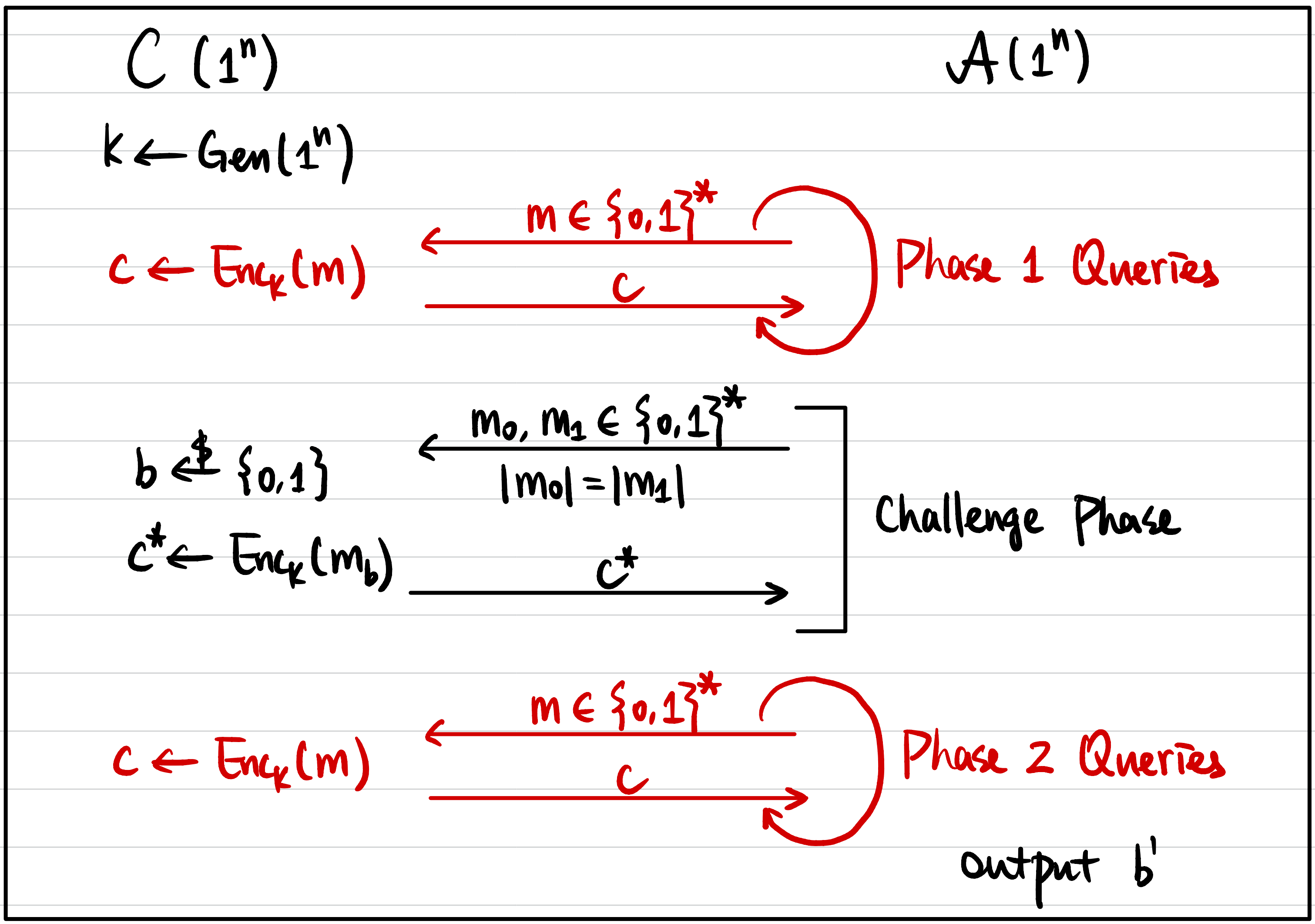
Assume Π is not semantically secure, then $\exists$ PPT $\mathcal{A}$ that breaks Π

↳ construct PPT B to break G.

Does Pseudo OTP allow encryption of multiple messages?

Chosen Plaintext Attack (CPA) Security

Def A symmetric-key encryption scheme (Gen, Enc, Dec) is secure against chosen plaintext attacks, or CPA-secure, if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b=b'] \le \frac{1}{2} + \varepsilon(n)$



Is Pseudo OTP CPA-secure?

<u>Thm</u> If the Enc algorithm is deterministic on the secret key k and message m, then the encryption scheme can't be CPA-secure.

Constructing CPA-Secure Encryption

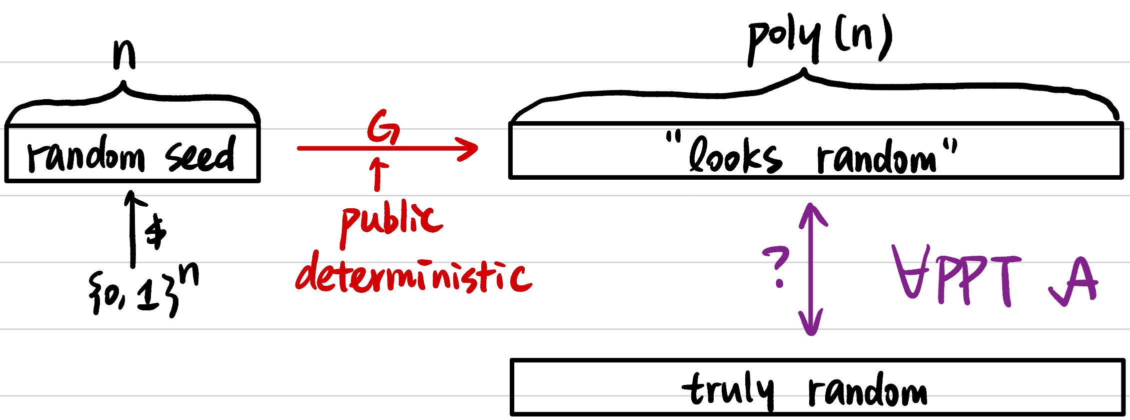
Pseudorandom Function (PRF)

$$\Downarrow$$

CPA-Secure Encryption

Pseudorandom Function (PRF)

Pseudorandom Generator (PRG)



"random-looking" string

Pseudorandom Function (PRF):

"random-looking" function

Pseudorandom Function (PRF)

Keyed Function $F: \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^m$

$$F(k, x) \to y$$

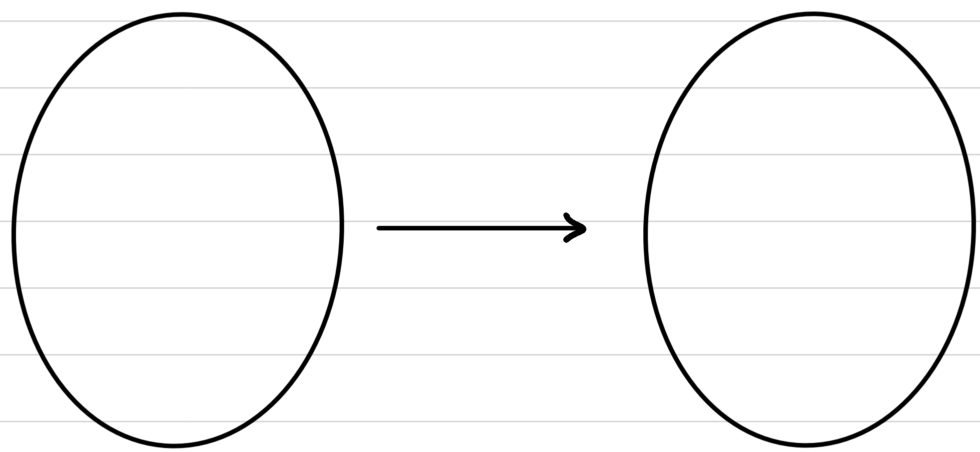
deterministic poly-time

key

input

output

$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad F_k:$



$\{0,1\}^n$ $\quad\quad\quad$ $\{0,1\}^m$

"looks like a random function"

Pseudorandom Function (PRF)

$k \xleftarrow{\$} \{0,1\}^\lambda \qquad F_k : \{0,1\}^n \longrightarrow \{0,1\}^m$

How many possible F_k's ?

$\Big\updownarrow$ $\forall$ PPT $\mathcal{A}$ (not knowing k)

$f \xleftarrow{\$} \{ F \mid F: \{0,1\}^n \to \{0,1\}^m \}$

$f : \{0,1\}^n \longrightarrow \{0,1\}^m$

How many possible f's ?

Pseudorandom Function (PRF)

Def 1 Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a deterministic, poly-time, keyed function. F is a pseudorandom function (PRF) if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \le \frac{1}{2} + \varepsilon(n)$

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

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

If $b=0$, then $k \xleftarrow{\$} \{0,1\}^n$ $\quad \{F \mid F: \{0,1\}^n \to \{0,1\}^n\}$

If $b=1$, then $f \xleftarrow{\$} \mathrm{Func}_n$

$\xleftarrow{\quad x \quad}$

If $b=0$, then $y := F_k(x)$

If $b=1$, then $y := f(x)$

$\xrightarrow{\quad y \quad}$

output b'

Pseudorandom Function (PRF)

Def 2 Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a deterministic, poly-time, keyed function. F is a pseudorandom function (PRF) if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\left| \Pr_{k \leftarrow U_n}\left[\mathcal{A}^{F_k(\cdot)}(1^n) = 1\right] - \Pr_{f \xleftarrow{\$} \mathrm{Func}_n}\left[\mathcal{A}^{f(\cdot)}(1^n) = 1\right] \right| \leq \varepsilon(n)$$

Exercises

$$F_k(x) := k \oplus x$$

Is F a secure PRF?

Exercises

Let $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF.

Define $F': \{0,1\}^n \times \{0,1\}^{n-1} \rightarrow \{0,1\}^{2n}$ as follows.

Is F' necessarily a PRF?

a) $F'_k(x) = F_k(0\|x) \| F_k(0\|x)$ $\quad F_k(0\,\boxed{\;x\;}) \,\|\, F_k(0\,\boxed{\;x\;})$

b) $F'_k(x) = F_k(0\|x) \| F_k(1\|x)$ $\quad F_k(0\,\boxed{\;x\;}) \,\|\, F_k(1\,\boxed{\;x\;})$

c) $F'_k(x) = F_k(0\|x) \| F_k(x\|0)$ $\quad F_k(0\,\boxed{\;x\;}) \,\|\, F_k(\boxed{\;x\;}\,0)$

d) $F'_k(x) = F_k(0\|x) \| F_k(x\|1)$ $\quad F_k(0\,\boxed{\;x\;}) \,\|\, F_k(\boxed{\;x\;}\,1)$

PRF $\Leftrightarrow$ PRG

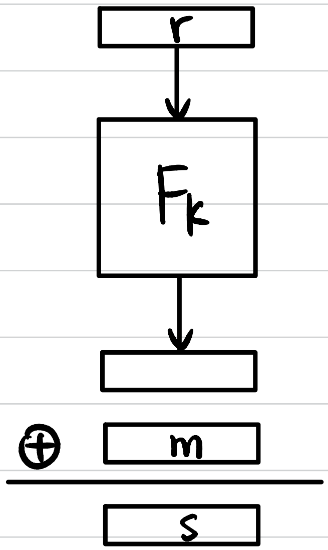
"$\Rightarrow$": Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF,
Construct $G: \{0,1\}^n \to \{0,1\}^{2n}$

"$\Leftarrow$": Let $G: \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG,
Construct $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

CPA-Secure Encryption Scheme

Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF,

- $Gen(1^n)$: sample $k \xleftarrow{\$} \{0,1\}^n$, output k.
- $Enc_k(m)$: $m \in \{0,1\}^n$
  $r \xleftarrow{\$} \{0,1\}^n$
  output $c := \langle r, F_k(r) \oplus m \rangle$
- $Dec_k(c)$: $c = \langle r, s \rangle$
  output $m := F_k(r) \oplus s$



Theorem If F is a PRF, then $\Pi = (Gen, Enc, Dec)$ is CPA-Secure.