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.

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

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

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

$k \leftarrow Gen(1^n)$

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

$c \leftarrow Enc_k(m_b)$

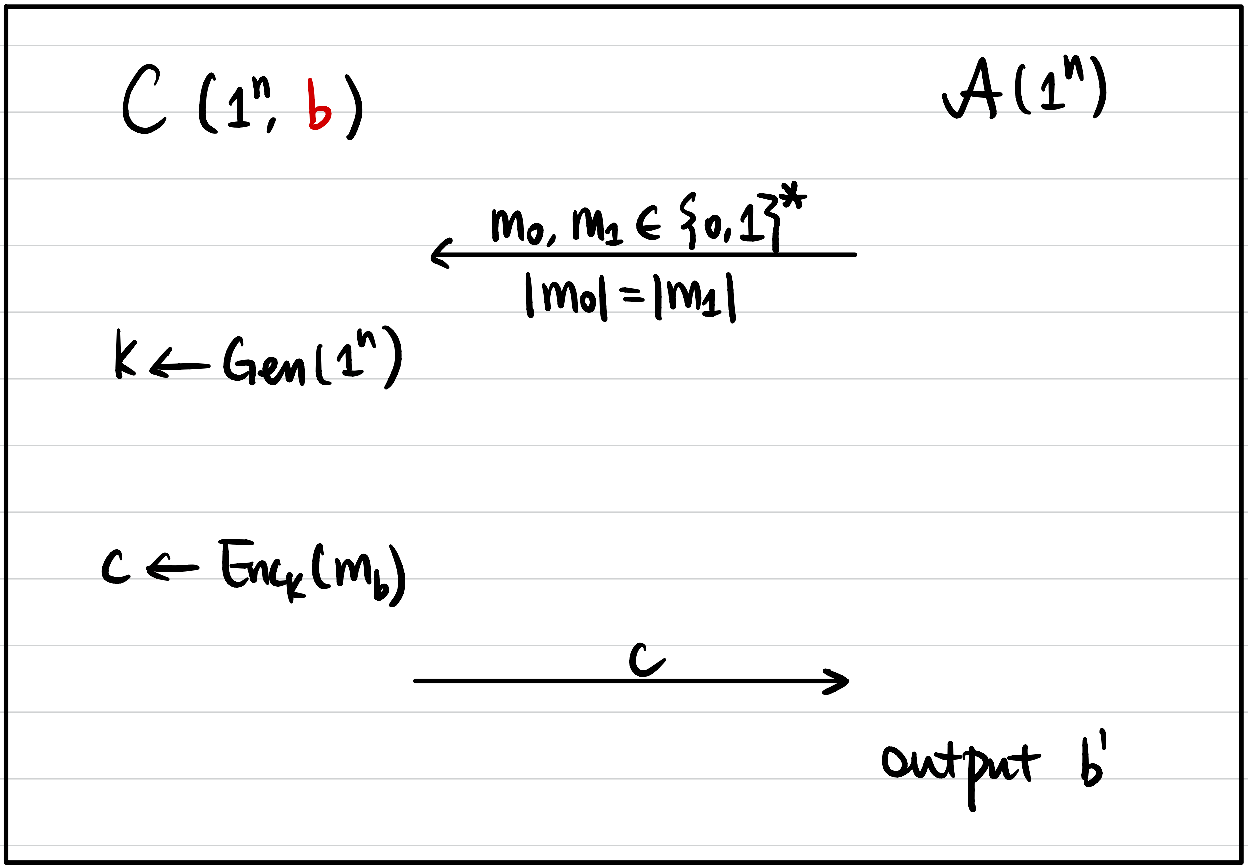
$$\xrightarrow{\quad c \quad}$$

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.

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



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 $negl(\cdot)$ s.t.

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

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'

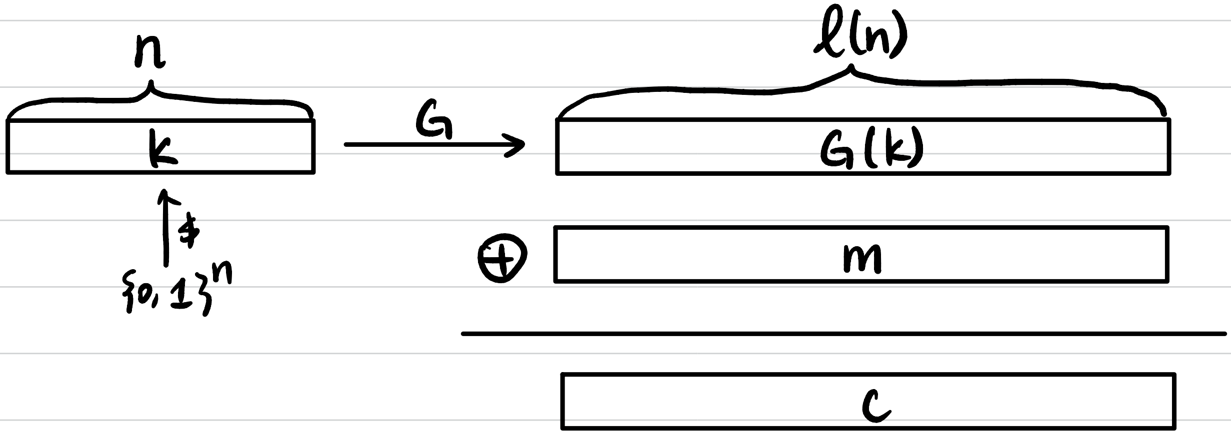
Fixed-Length Encryption Scheme

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 $m := G(k) \oplus c$.

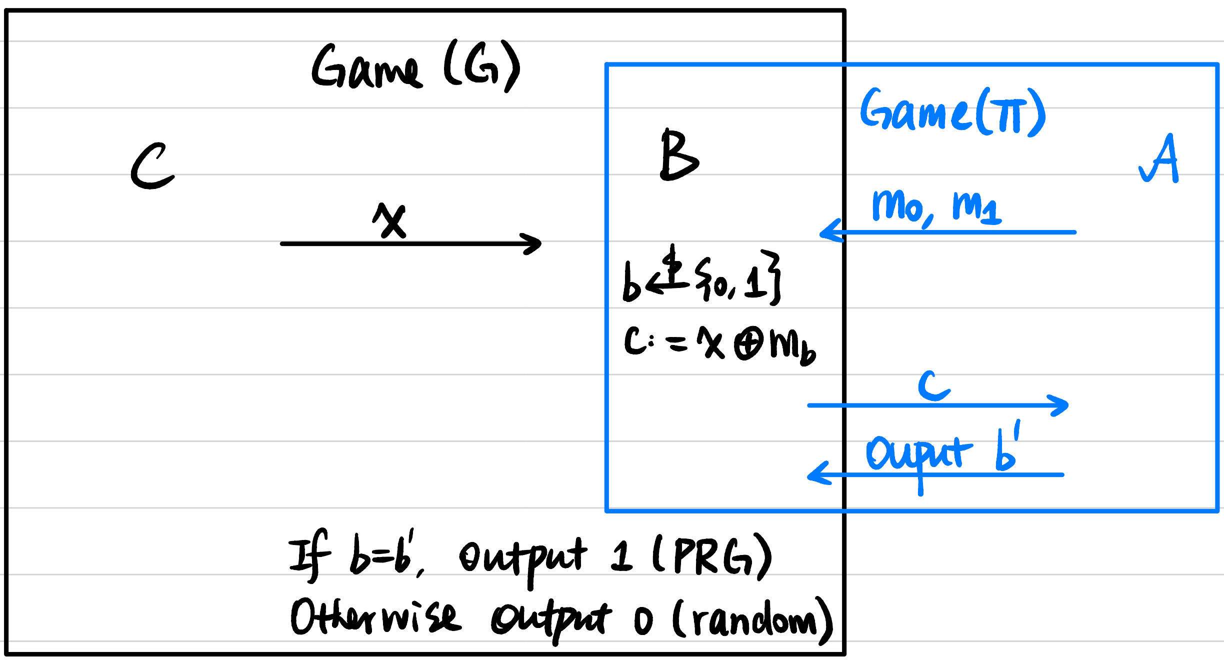


"pseudo OTP"

Proof of Security

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

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.



$$\Pr[B \text{ guesses correctly}] = \Pr[x \leftarrow G(U_n)] \cdot \Pr[b=b' \mid x \leftarrow G(U_n)] + \Pr[x \leftarrow U_{2n}] \cdot \Pr[b=b' \mid x \leftarrow U_{2n}]$$

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

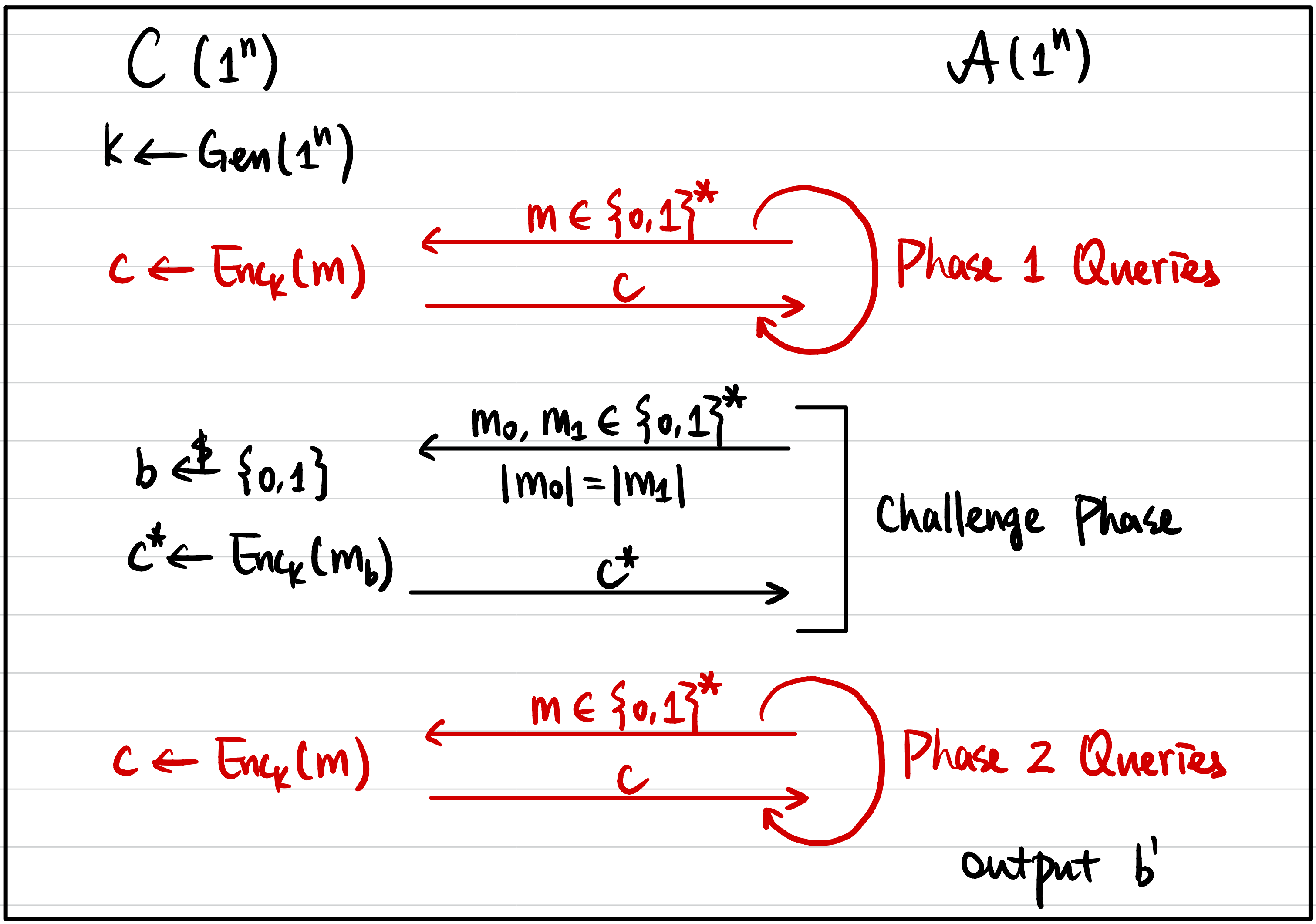
$$\geq \frac{1}{2} \cdot \left(\frac{1}{2} + \text{non-negl}(n)\right) + \frac{1}{4} = \frac{1}{2} + \frac{1}{2} \cdot \text{non-negl}(n).$$

Does Pseudo OTP allow encryption of multiple messages?

$$\mathrm{Enc}_k(m_1) \to G(k) \oplus m_1$$
$$\mathrm{Enc}_k(m_2) \to G(k) \oplus m_2$$
$$\to m_1 \oplus m_2$$

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? No!

$$\begin{array}{ccc}
C & & \mathcal{A} \\
 & \xleftarrow{\quad m_0 \quad} & \\
 & \xrightarrow{\quad c_0 = G(k) \oplus m_0 \quad} & \\
 & \xleftarrow{\quad m_1 \quad} & \\
 & \xrightarrow{\quad c_1 = G(k) \oplus m_1 \quad} & \\
 & \xleftarrow{\quad m_0, m_1 \quad} & \\
 & \xrightarrow{\quad c^* \quad} & \\
 & & \text{output } b \text{ if } c^* = c_b
\end{array}$$

<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

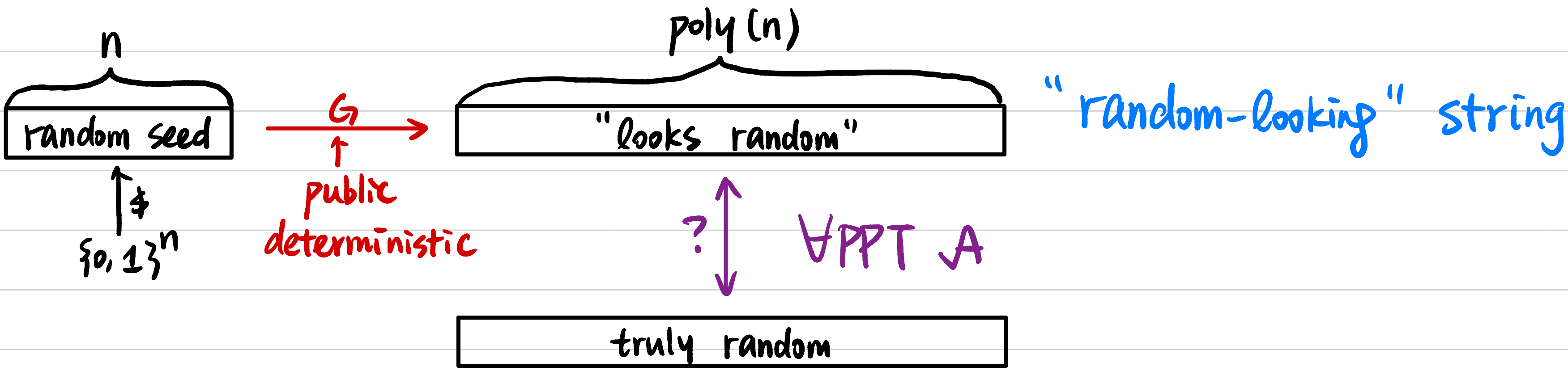
Pseudorandom Function (PRF)

$$\Downarrow$$

CPA-Secure Encryption

Pseudorandom Function (PRF)

Pseudorandom Generator (PRG)



Pseudorandom Function (PRF): "random-looking" function

Pseudorandom Function (PRF)

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

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

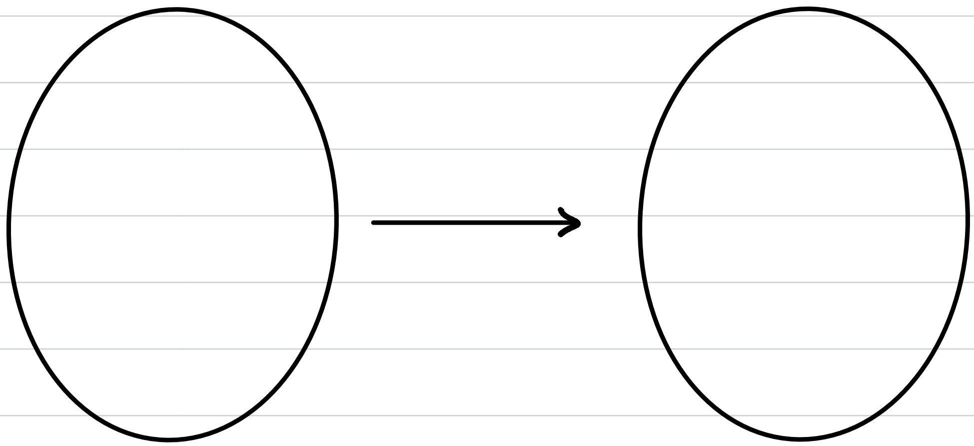
deterministic poly-time

key

input

output

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



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

"looks like a random function"

Pseudorandom Function (PRF)

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

How many possible F_k's ?

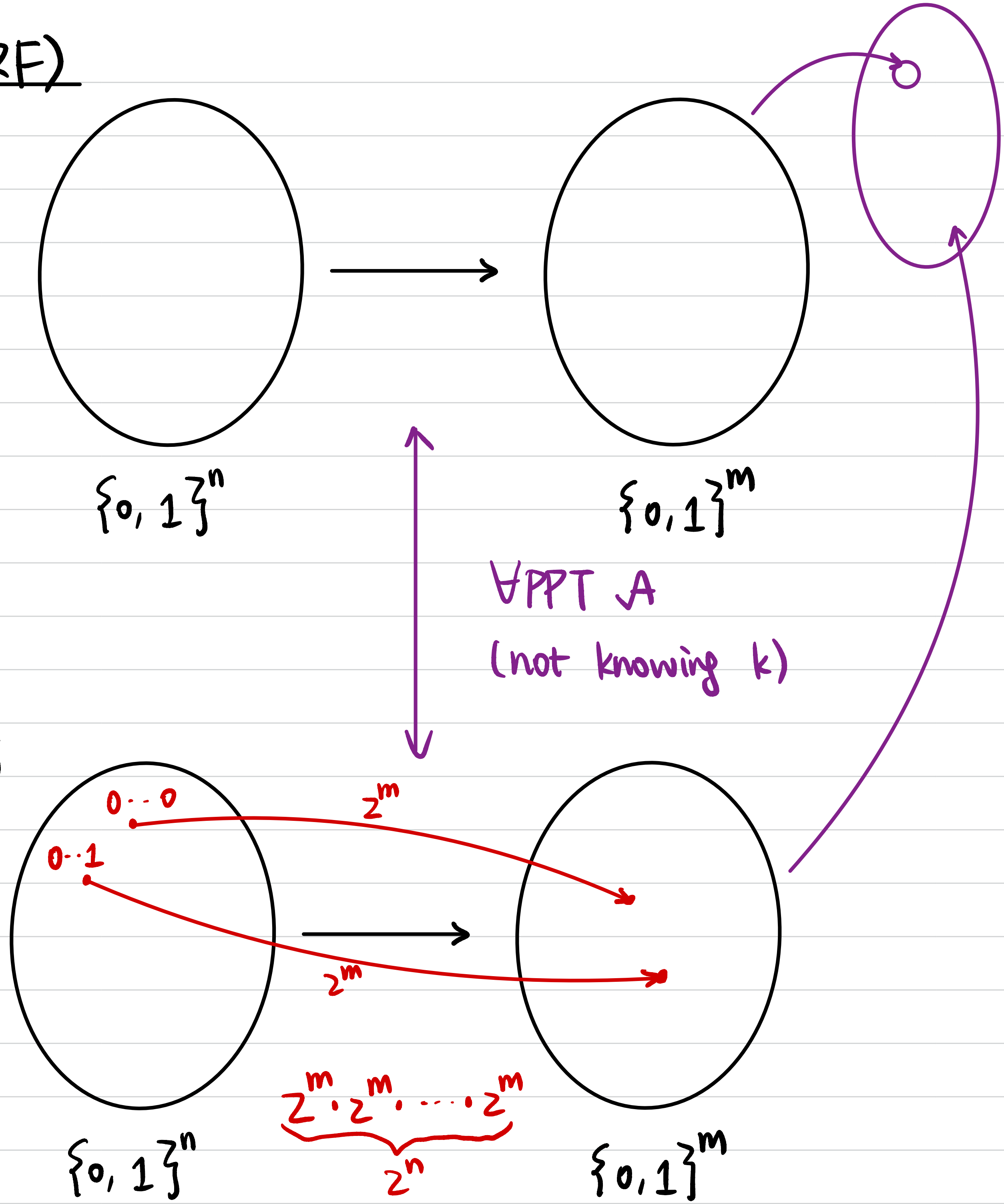
2^λ

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

$f :$

How many possible f's ?

$(2^m)^{2^n}$



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

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

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

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

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 $y := f(x)$ $\qquad$ $\xrightarrow{\quad y \quad}$

output b'

Pseudorandom Function (PRF)

Def 2 Let $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ 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? No!

$$C \xleftarrow{\quad x_1 \quad} \mathcal{A}$$
$$C \xrightarrow{\quad y_1 \quad} \mathcal{A}$$
$$C \xleftarrow{\quad x_2 \quad} \mathcal{A}$$
$$C \xrightarrow{\quad y_2 \quad} \mathcal{A}$$

If $x_1 \oplus x_2 = y_1 \oplus y_2$, output 0 (PRF)

Otherwise, output 1 (random)

Exercises

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

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

Is F' necessarily a PRF?

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

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

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

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

a) C $\qquad$ A

$C \xleftarrow{\;x\;} A$

$C \xrightarrow{\;y_1 \| y_2\;} A$

$y_1 \stackrel{?}{=} y_2$

c) C $\qquad$ A

$C \xleftarrow{\;x = 0\cdots0\;} A$

$C \xrightarrow{\;y_1 \| y_2\;} A$

$y_1 \stackrel{?}{=} y_2$

d) C $\qquad$ A

$C \xleftarrow{\;x_1 = 0\cdots0\;} A$

$C \xrightarrow{\;y_1 \| y_2\;} A$

$C \xleftarrow{\;x_2 = 0\cdots1\;} A$

$C \xrightarrow{\;y_3 \| y_4\;} A$

$y_2 \stackrel{?}{=} y_3$

b) $F'_k(x) = F_k(0\|x) \,\|\, F_k(1\|x)$ is a PRF

<u>Proof</u> Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the pseudorandomness of F'.

We construct PPT B to break the pseudorandomness of F.