

CSCI 1510

This Lecture:

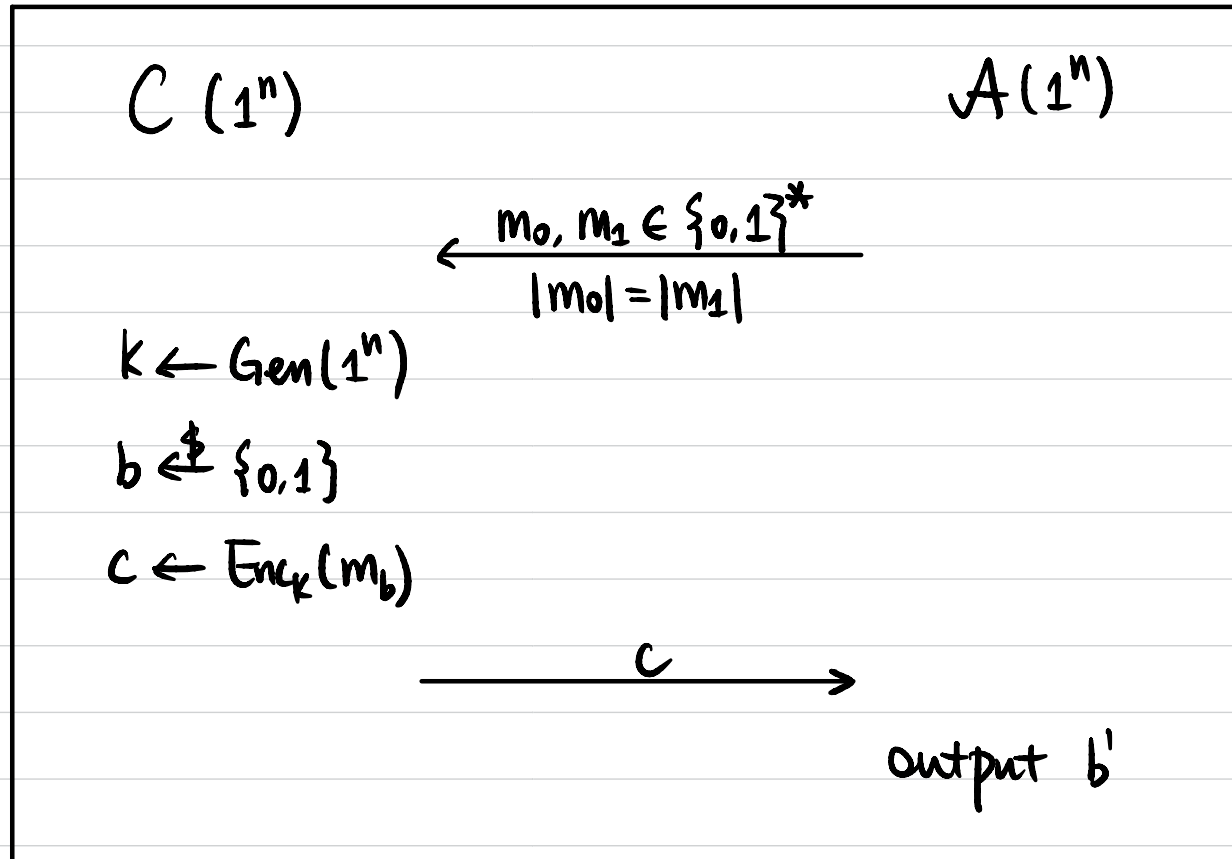
- Chosen Plaintext Attack (CPA) Security
- Pseudorandom Function (PRF)
- CPA-Secure Encryption from PRF
- Hybrid Argument

Computationally Secure Encryption

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

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

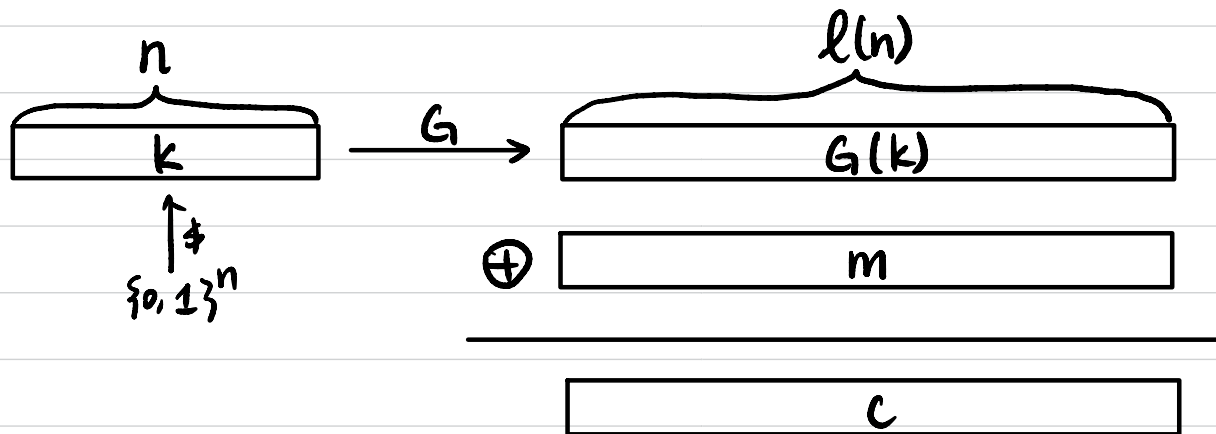
$$\Pr[b=b'] \leq \frac{1}{2} + \epsilon(n)$$



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



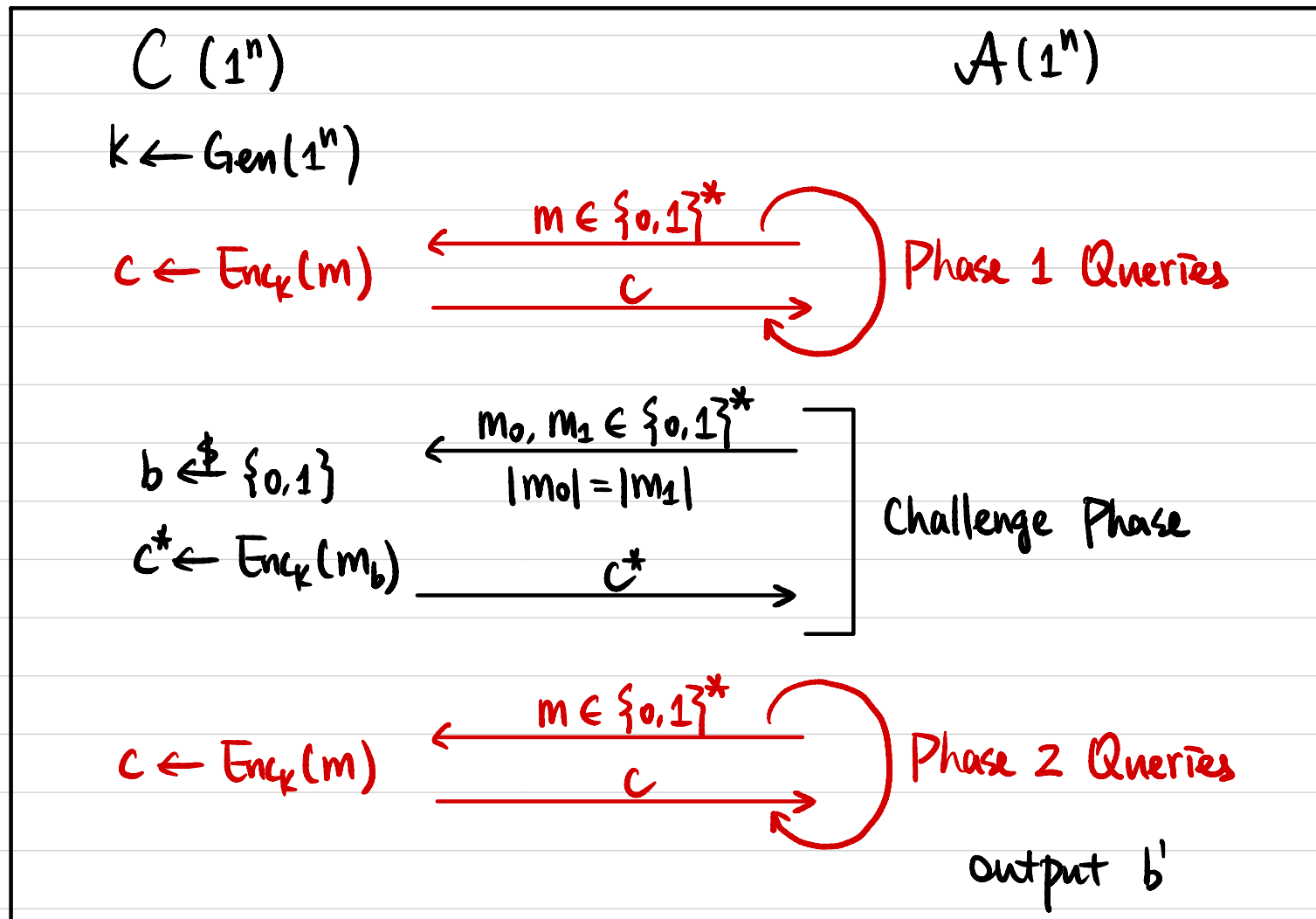
"pseudo OTP"

Does Pseudo OTP allow encryption of multiple messages?

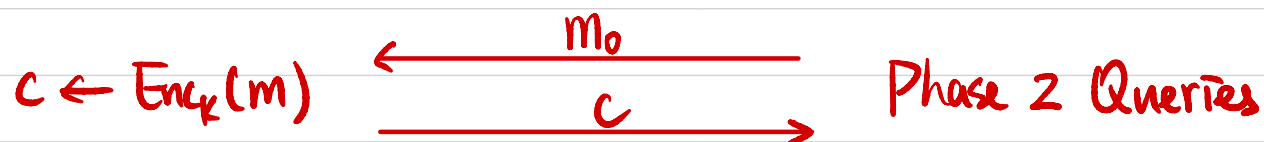
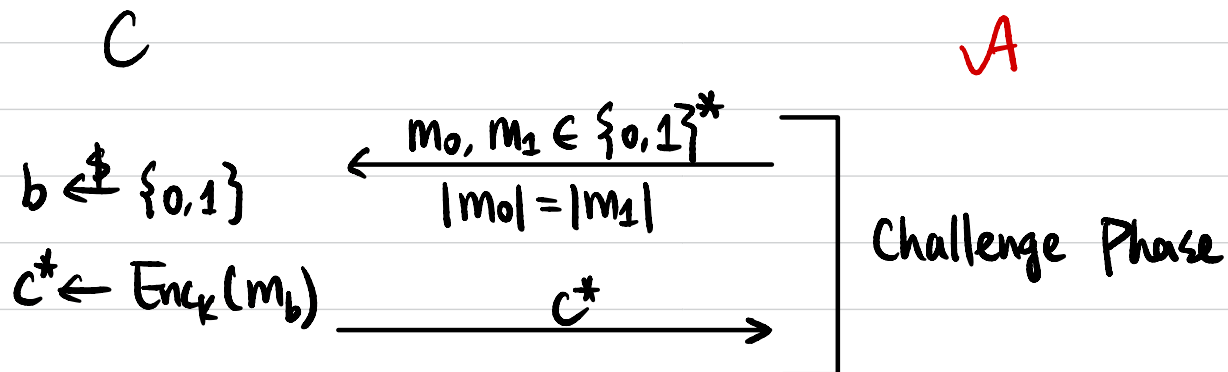
$$\begin{aligned} C_1 &= G(k) \oplus m_1 \\ C_2 &= G(k) \oplus m_2 \end{aligned} \quad \left. \begin{array}{l} \\ \end{array} \right\} \oplus \rightarrow m_1 \oplus m_2$$

Chosen Plaintext Attack (CPA) Security

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



Is Pseudo OTP CPA-secure? No!



If $c = c^*$, output 0
Otherwise output 1

Thm If the Enc algorithm is **deterministic** on the secret key k and message m , then the encryption scheme can't be CPA-Secure.

If a scheme is not CPA secure, is it necessarily deterministic?

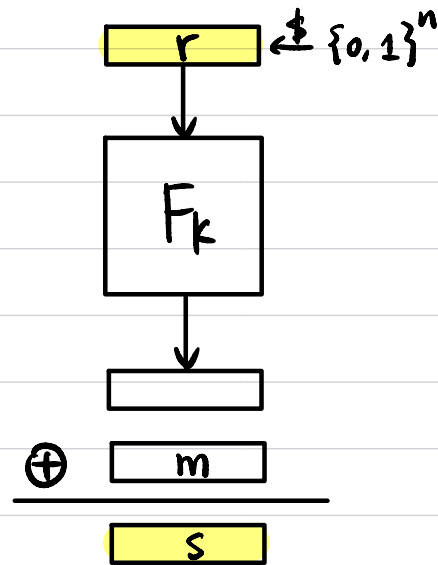
$\text{Enc}_k(m): r \leftarrow \{0,1\}, \text{ output } m \parallel r$

Constructing CPA-Secure Encryption

Pseudorandom Function (PRF)



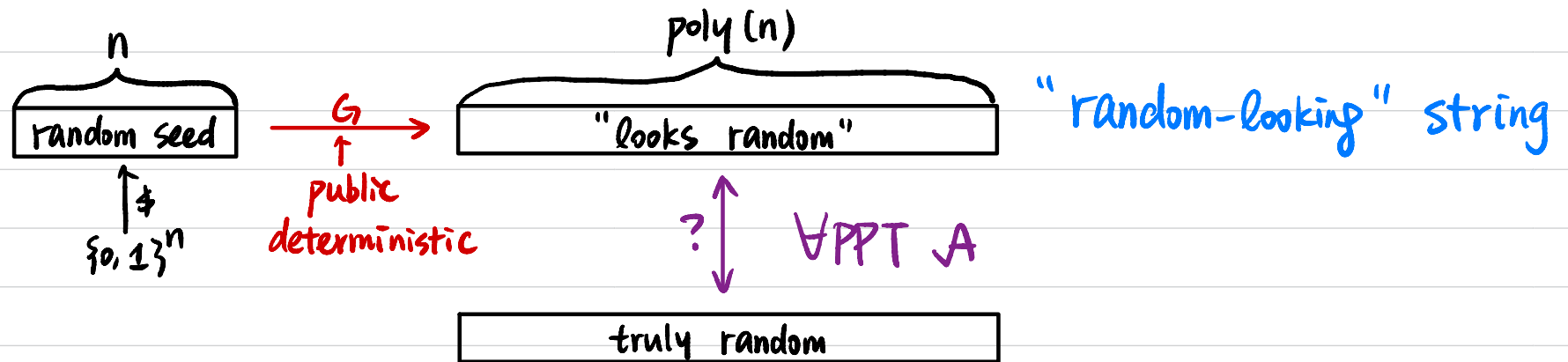
CPA-Secure Encryption



$c = \langle r, s \rangle$

Pseudorandom Function (PRF)

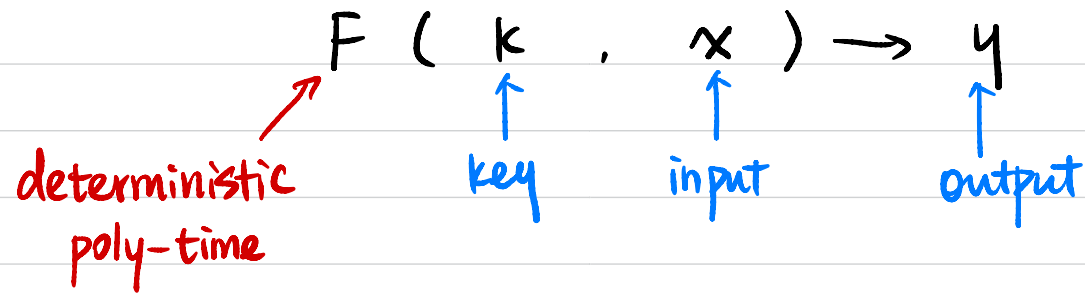
Pseudorandom Generator (PRG)



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

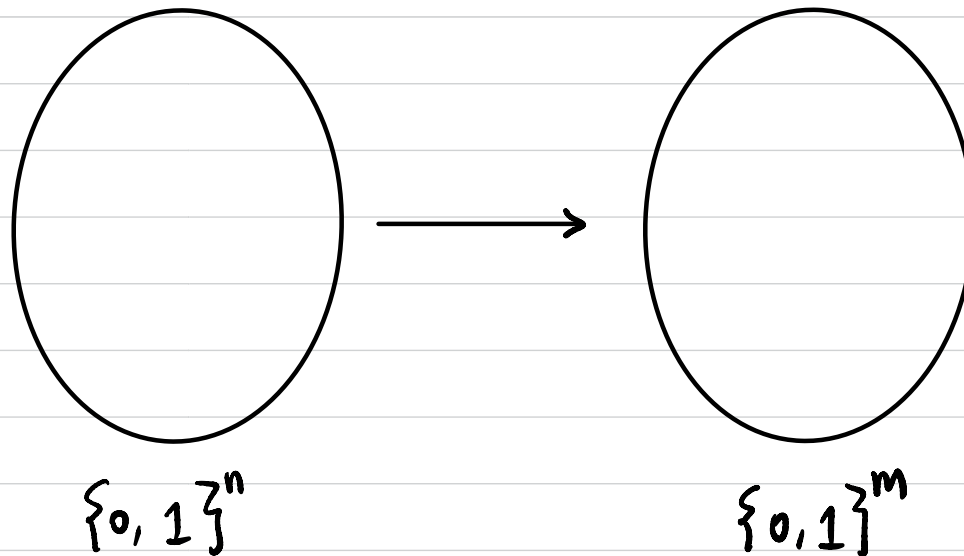
Pseudorandom Function (PRF)

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



$k \leftarrow \{0,1\}^k$

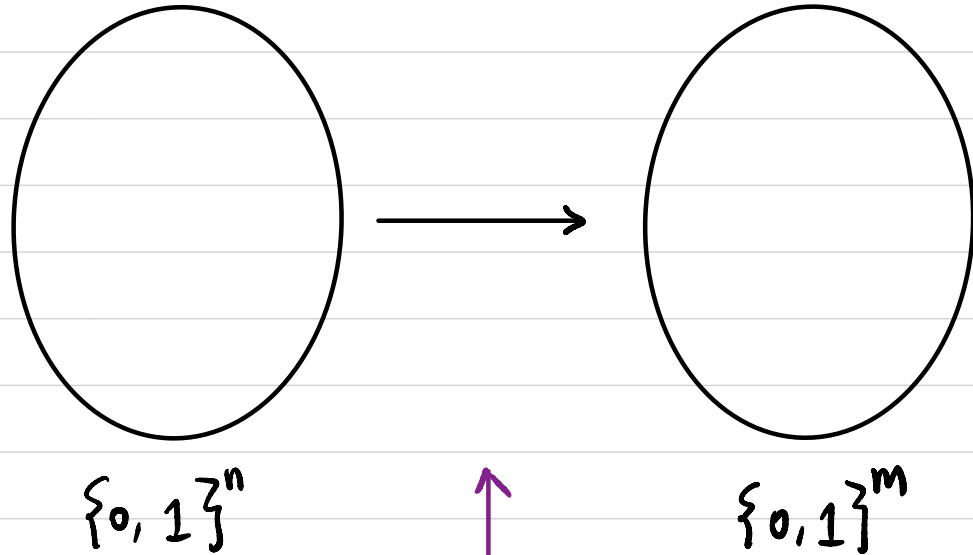
$F_k:$



"looks like a random function"

Pseudorandom Function (PRF)

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

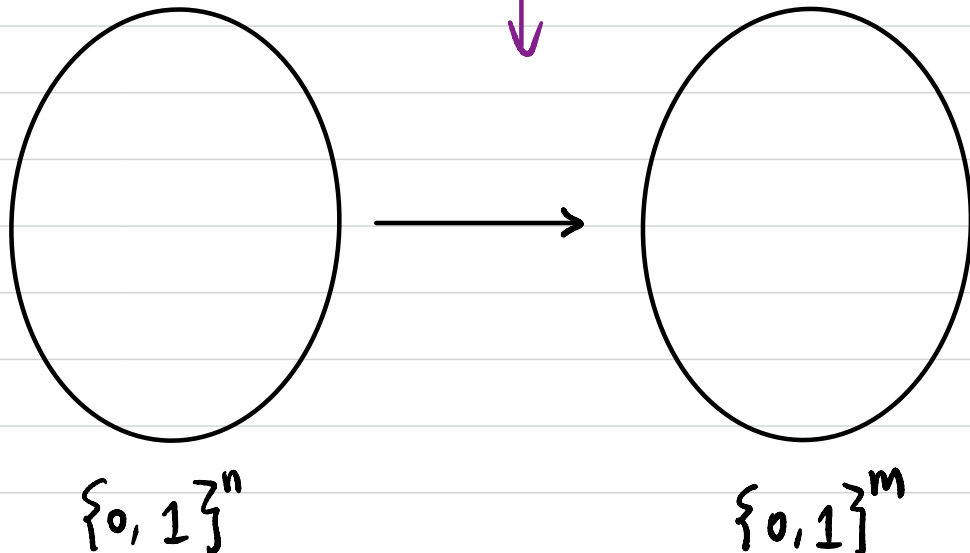


How many possible F_k 's?

2^λ

$$f \leftarrow \{F \mid F: \{0, 1\}^n \rightarrow \{0, 1\}^m\}$$

$f:$



How many possible f 's?

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

$\forall \text{PPT } A$
(not knowing k)

Pseudorandom Function (PRF)

Def 1 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 A , $\exists$ negligible function $\epsilon(\cdot)$ s.t. $\Pr[b=b'] \leq \frac{1}{2} + \epsilon(n)$

$C(1^n)$

$A(1^n)$

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

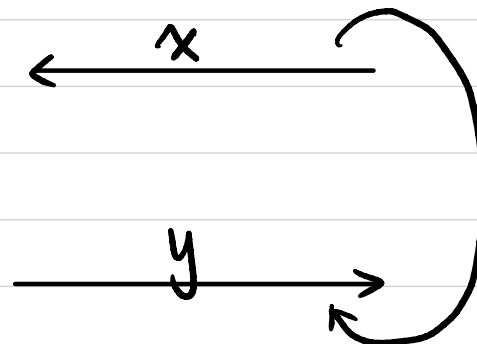
If $b=0$, then $k \xleftarrow{\$} \{0,1\}^n$

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

$\{ F \mid F: \{0,1\}^n \rightarrow \{0,1\}^n \}$

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

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



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 A ,
 $\exists$ negligible function $\epsilon(\cdot)$ s.t.

$$\left| \Pr_{k \leftarrow \mathcal{U}_n} [A^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \mathcal{F}_{\text{Func}_n}} [A^{f(\cdot)}(1^n) = 1] \right| \leq \epsilon(n)$$

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) $F'_k(x) = F_k(0 \| x) \| F_k(0 \| x)$

$F_k(0 \boxed{x}) \| F_k(0 \boxed{x})$

b) $F'_k(x) = F_k(0 \| x) \| F_k(1 \| x)$

$F_k(0 \boxed{x}) \| F_k(1 \boxed{x})$

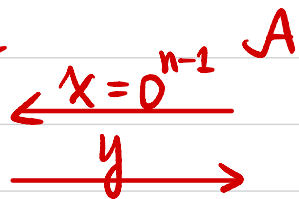
c) $F'_k(x) = F_k(0 \| x) \| F_k(x \| 0)$

$F_k(0 \boxed{x}) \| F_k(\boxed{x} 0)$

d) $F'_k(x) = F_k(0 \| x) \| F_k(x \| 1)$

$F_k(0 \boxed{x}) \| F_k(\boxed{x} 1)$

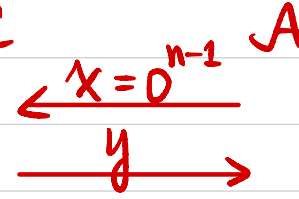
a) No! C



$y = y_0 \| y_1$

If $y_0 = y_1$, output 0
Otherwise output 1

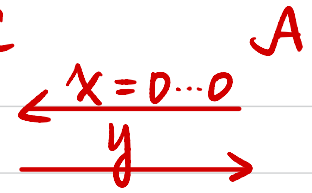
c) No! C



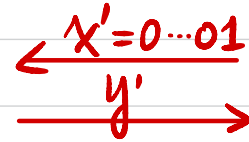
$y = y_0 \| y_1$

If $y_0 = y_1$, output 0
Otherwise output 1

d) No! C



$y = y_0 \| y_1$



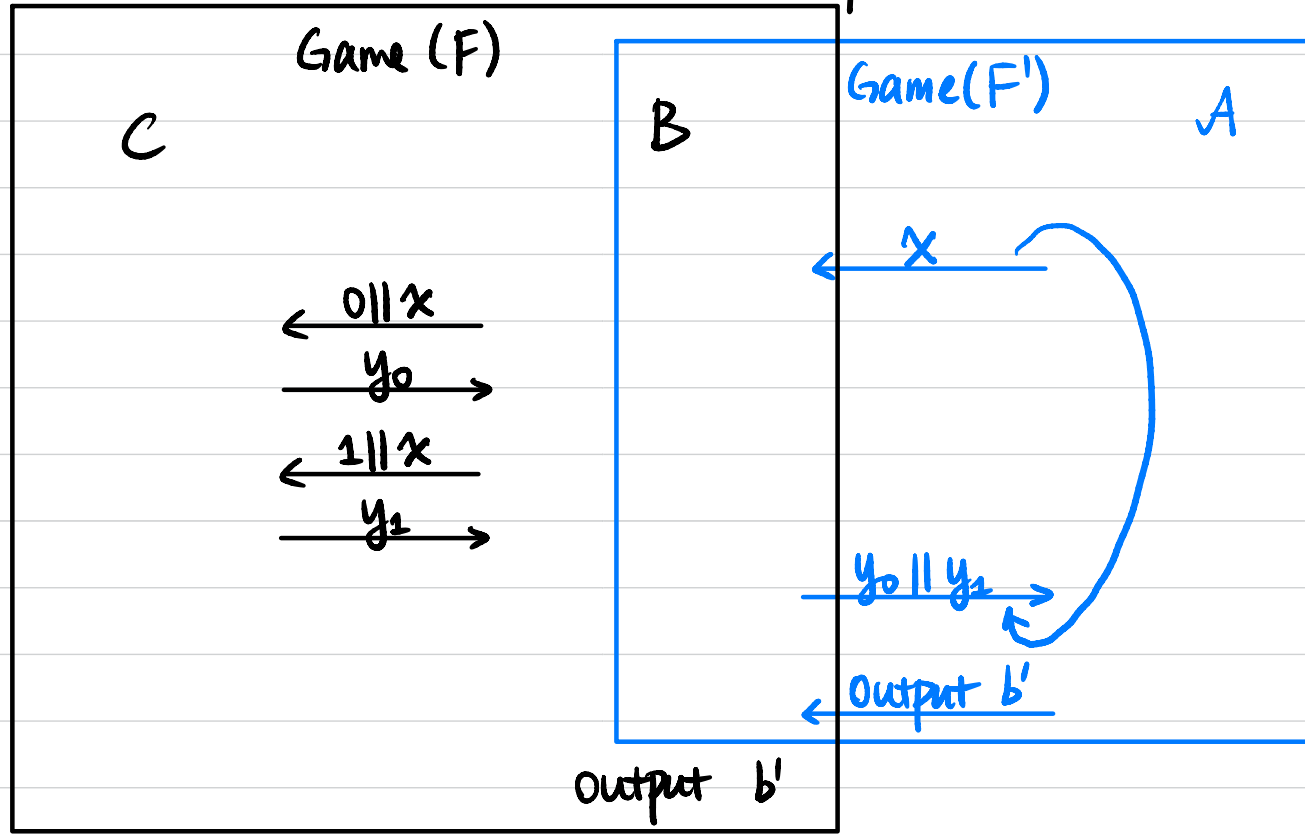
$y' = y'_0 \| y'_1$

If $y_1 = y'_0$, output 0
Otherwise output 1

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

Proof Assume not, then $\exists$ PPT A that breaks the pseudorandomness of F' .

We construct PPT B to break the pseudorandomness of F .



If $b=0$ (C uses F_k), then $y_0 || y_1 = F_k(0||x) || F_k(1||x) = F'_k(x)$, B is responding with $F'_k(\cdot)$.

If $b=1$ (C uses a random function), then $y_0 || y_1 = f(0||x) || f(1||x)$

For distinct x , $0||x$ & $1||x$ are all distinct,

y_0 & y_1 are independent random strings,

$\Rightarrow B$ is responding with $f(\cdot)$.

$$\Pr[b=b' \text{ in Game } F] = \Pr[b=b' \text{ in Game } F'] \geq \frac{1}{2} + \text{non-negl}(n).$$

PRF $\Leftrightarrow$ PRG

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

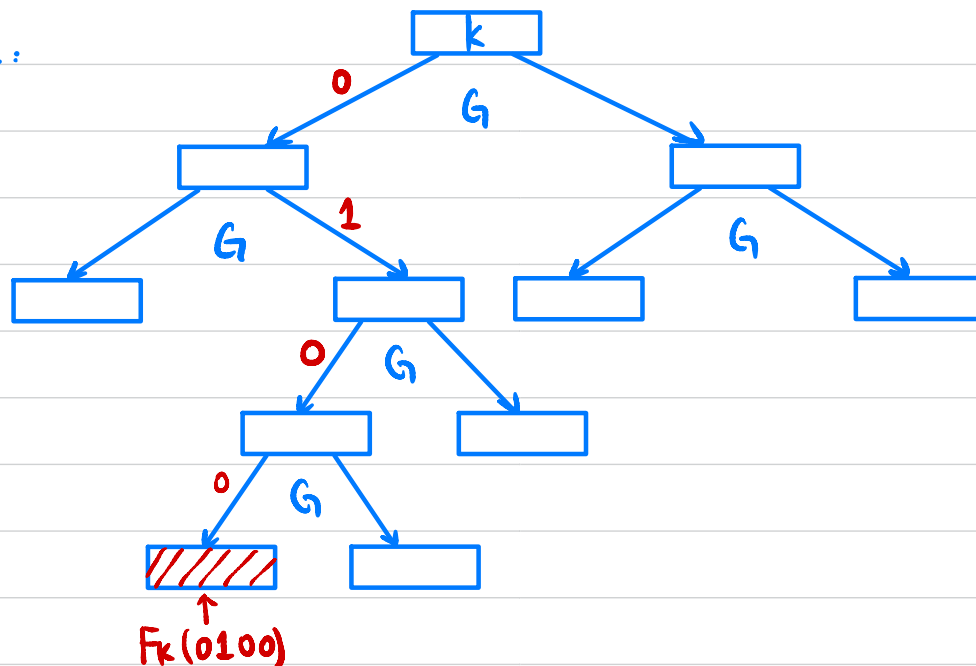
Construct $G: \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$

$$G(s) := F_s(0 \dots 0) \parallel F_s(0 \dots 01)$$

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

Construct $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$

GGM tree:



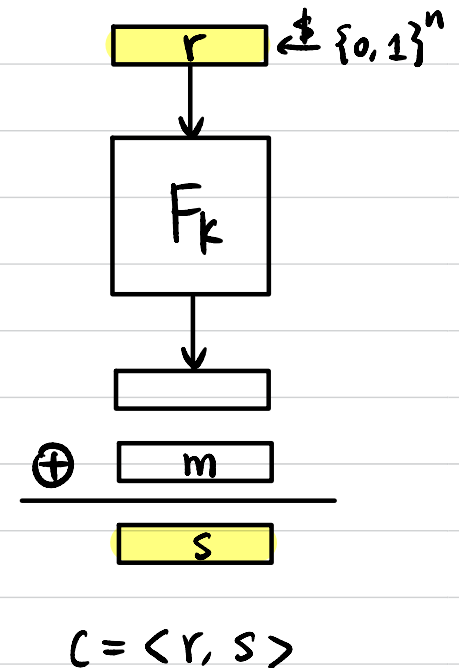
CPA-Secure Encryption Scheme

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

- $\text{Gen}(1^n)$: sample $k \leftarrow \{0,1\}^n$, output k .

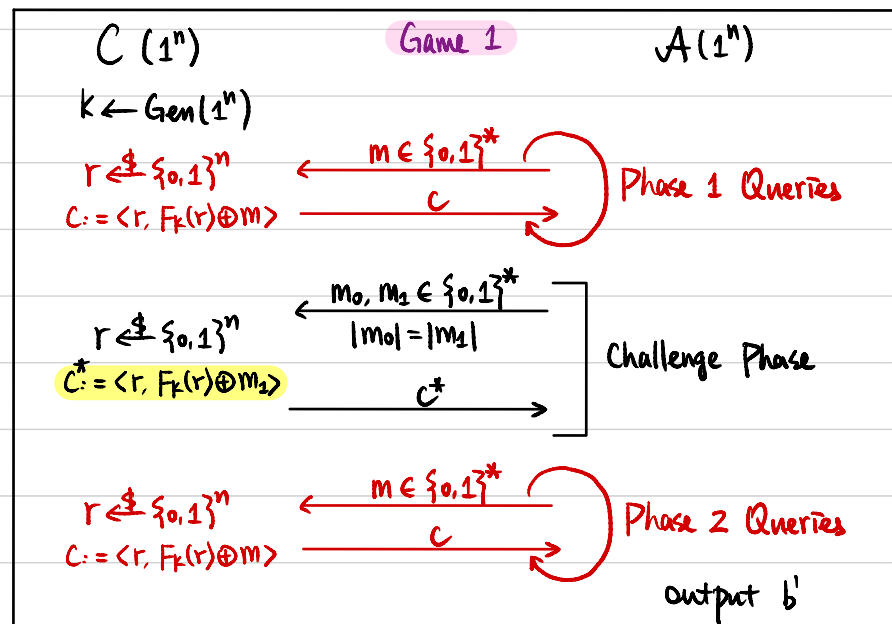
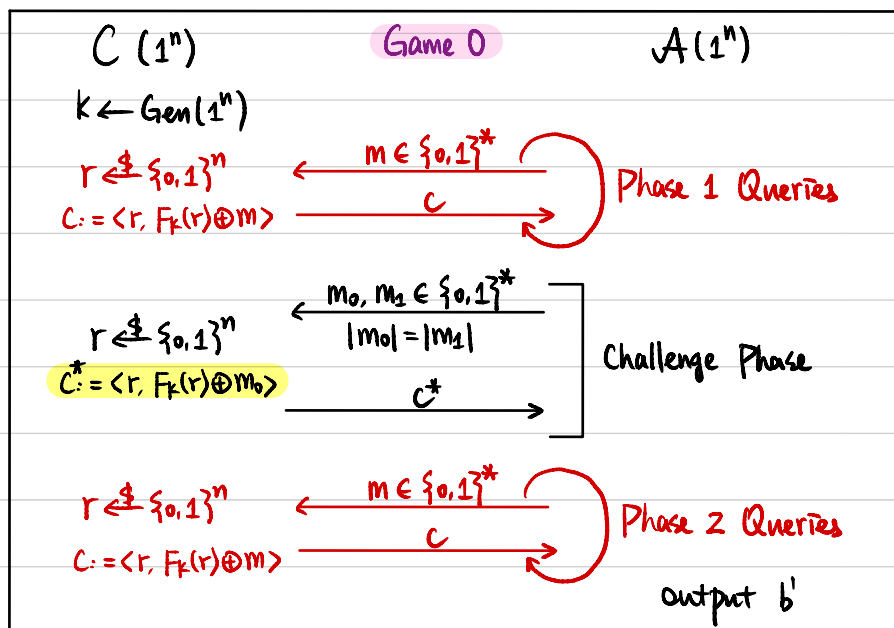
- $\text{Enc}_k(m)$: $m \in \{0,1\}^n$
 $r \leftarrow \{0,1\}^n$
output $c := \langle r, F_k(r) \oplus m \rangle$

- $\text{Dec}_k(c)$: $c = \langle r, s \rangle$
output $m := F_k(r) \oplus s$



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

Proof $\forall$ PPT A ,



$$|\Pr[A \text{ outputs } 1 \text{ in Game } 0] - \Pr[A \text{ outputs } 1 \text{ in Game } 1]| \leq \text{negl}(n) ?$$

