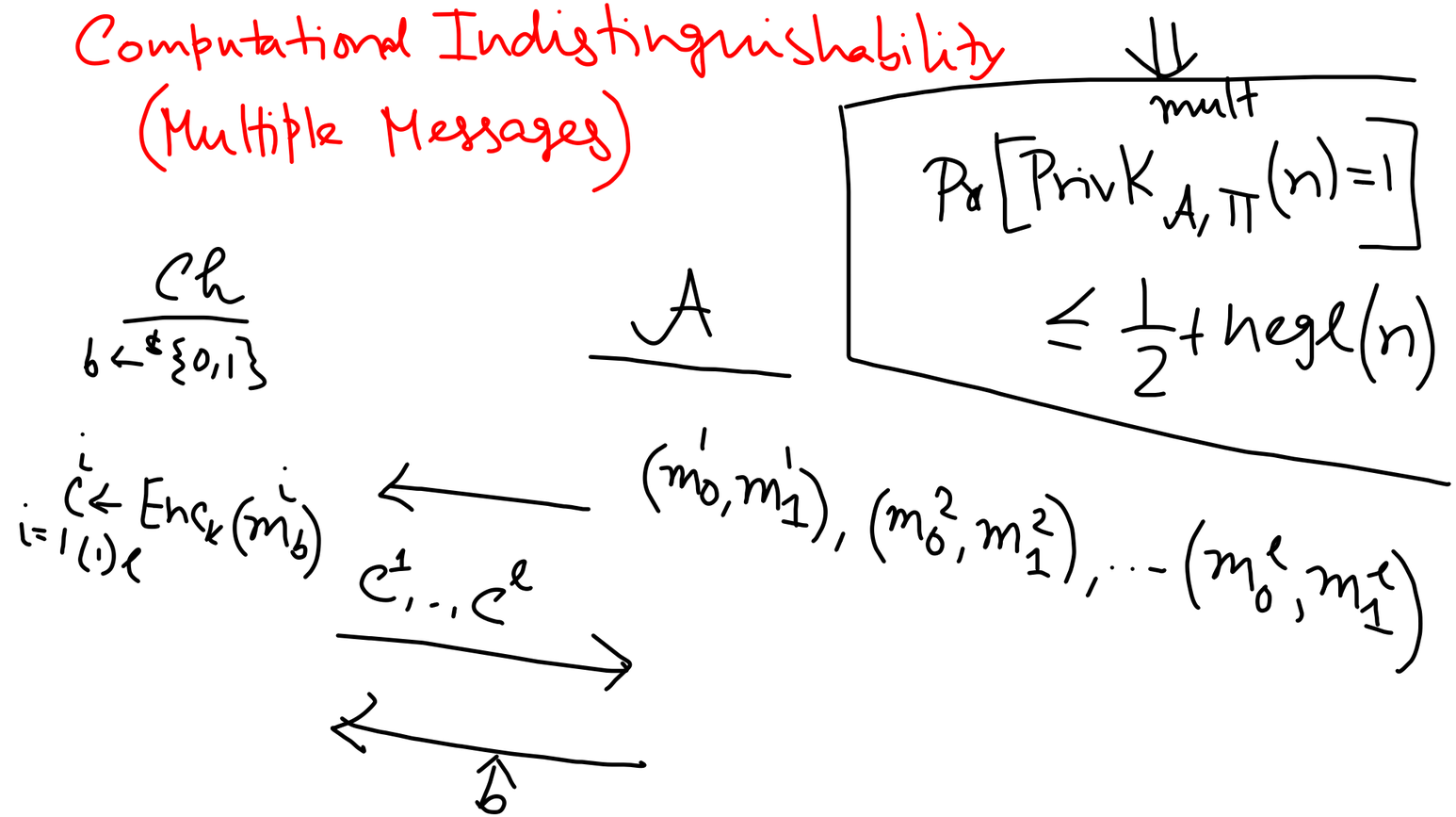
Stronger Security Notions

– Multiple Messages.

Recap

1. Perfect Secrecy
   - Limitation
2. Computational (CI) Indistinguishability
   - ≡ Semantic Security
3. If $G \to$ PRG exists, then $\exists\ \Pi \to$ CI
4. Limitated to single message encryption
5. Ciphertext only attack model.

Computational Indistinguishability (Multiple Messages)



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

Ch | **A**

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

$((m_0, m_0), (m_0, m_1))$ ←

$c^1 = Enc_k(m_0)$

$c^2 = Enc_k(m_b)$

→ (c^1, c^2)

If $c^1 = c^2$ then $\hat{b} = 0$

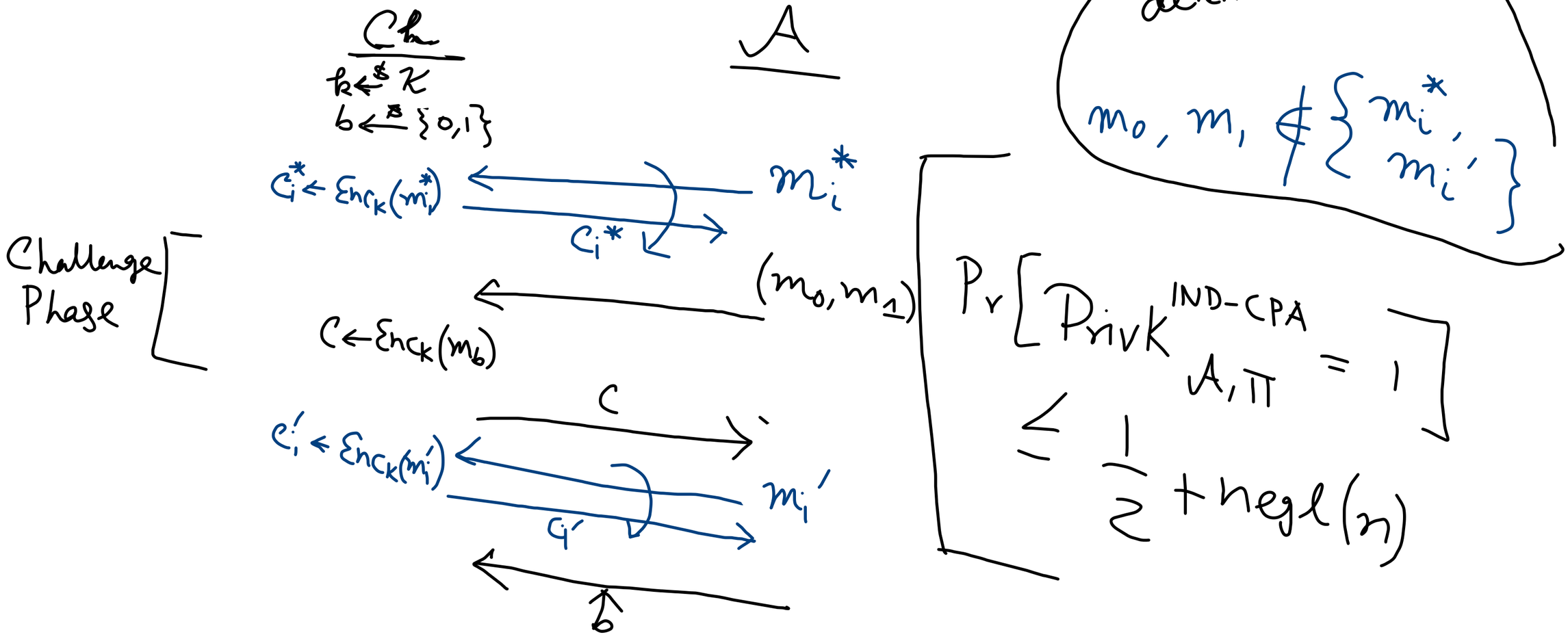
else $\hat{b} = 1$

← $\hat{b}$

(*) Encryption scheme is deterministic

Indistinguishability under Chosen Plaintext Attack

(IND-CPA)



Indistinguishability under Chosen Plaintext Attack

Left or Right (LOR) setting

(IND-CPA)

Ch

$k \xleftarrow{\$} \mathcal{K}$

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

A

deterministic

$m_0, m_1 \notin \{m_i^*, m_i'\}$

Challenge Phase

$c^i \leftarrow Enc_k(m_b^i)$

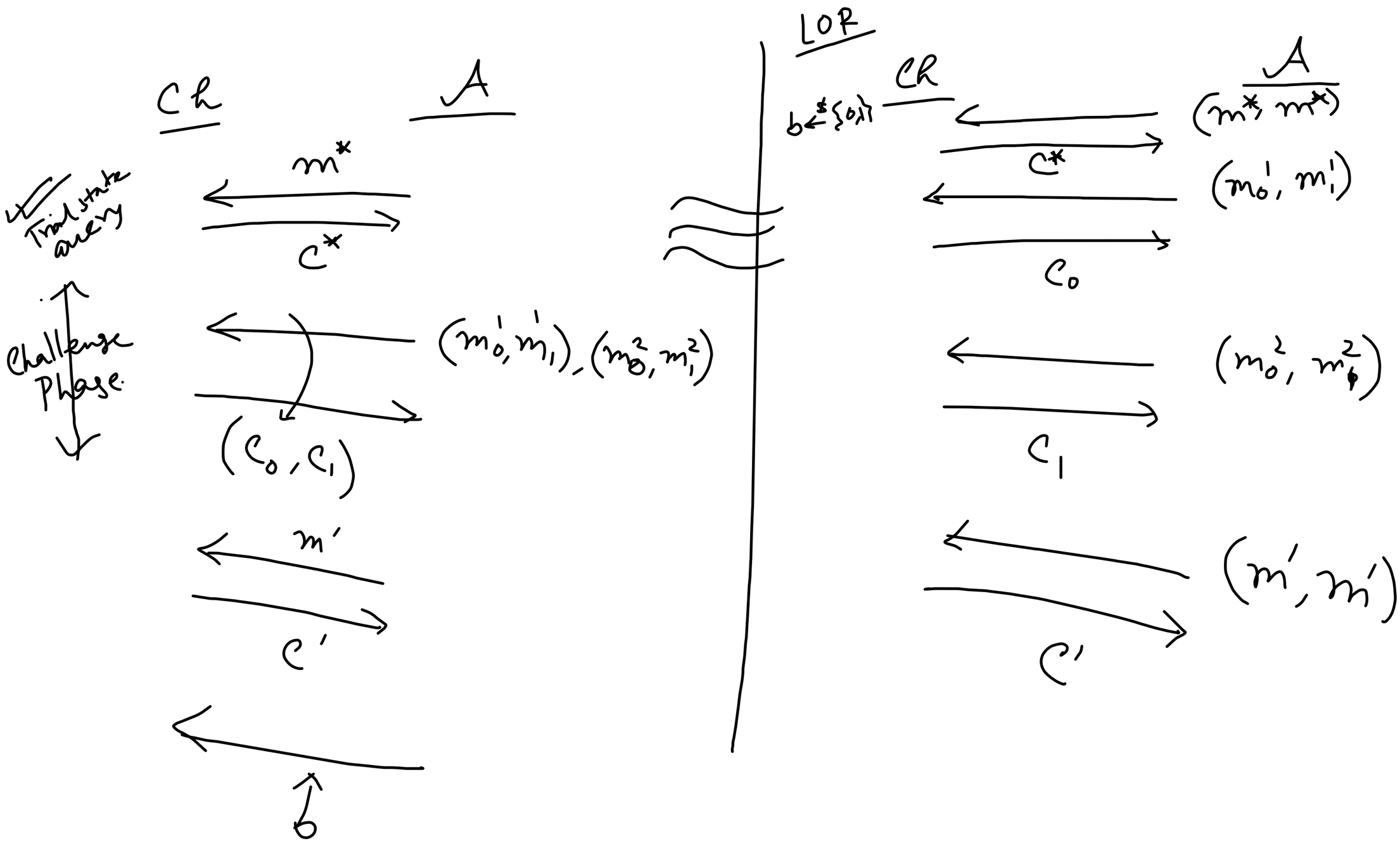
(m_0^i, m_1^i)

c^i

b

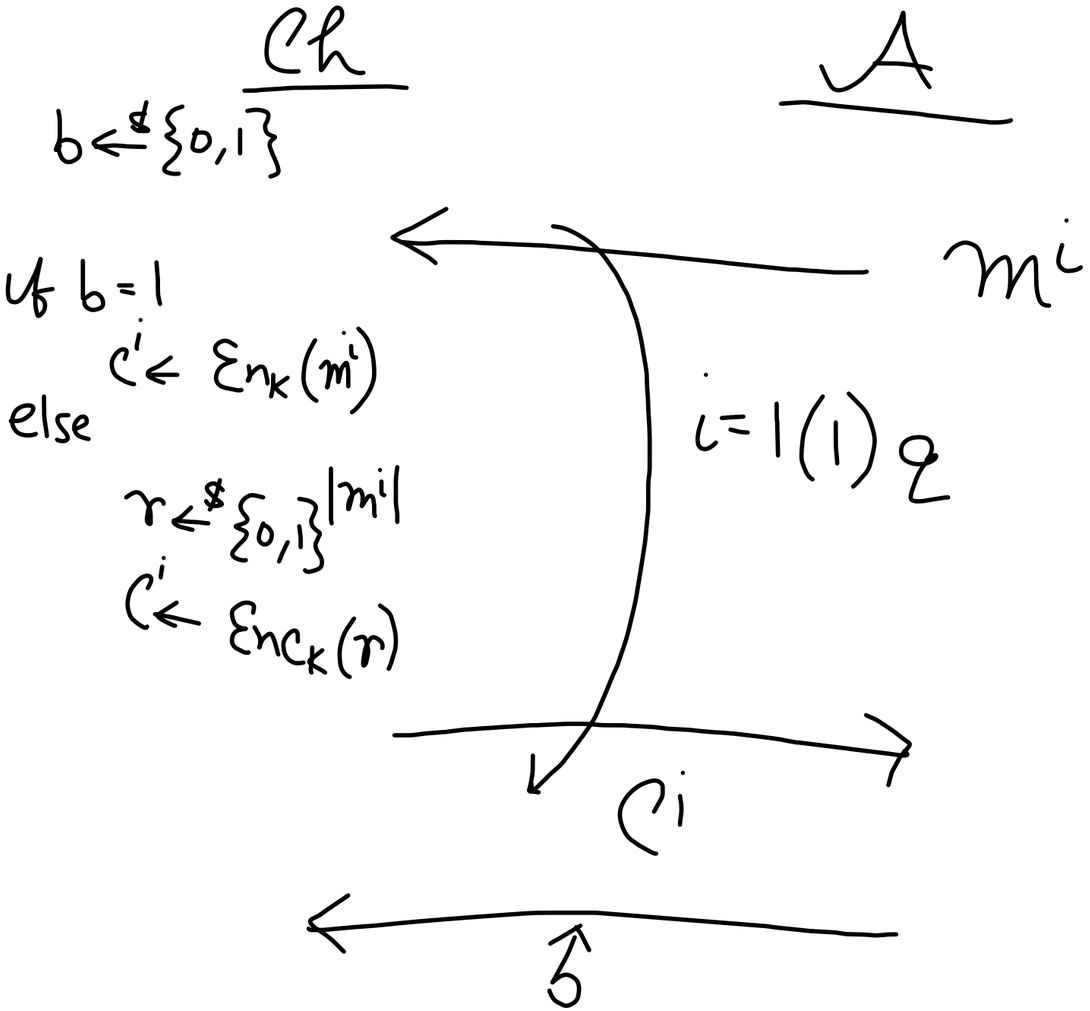
$Pr[PrivK^{IND-CPA}_{A,\Pi} = 1] \leq \frac{1}{2} + negl(n)$

* Multiple Enc
* CPA adversary Model.


LOR
Ch
A
CR
A
$b \xleftarrow{\$} \{0,1\}$
(m^*, m^*)
m^*
c^*
c^*
(m_0', m_1')
c_0
Trivial state query
Challenge Phase
(m_0', m_1') (m_0^2, m_1^2)
(c_0, c_1)
(m_0^2, m_1^2)
c_1
m'
c'
(m', m')
c'
b

If Π is IND-CPA secure under Single messages
then Π is IND-CPA secure under multiple messages
or IND-CPA secure in LOR setting.

IND-CPA in ROR (Real or Random)



Th^m:

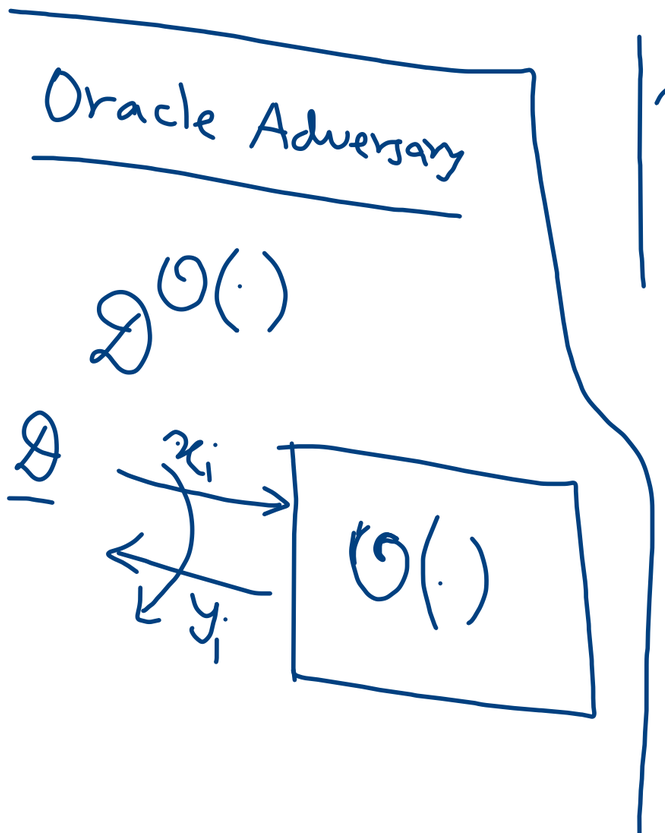
Π is LOR secure **iff**

Π is ROR secure

Ideal Object → Pseudorandom Function (PRF)

$F: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ is a fixed length PRF

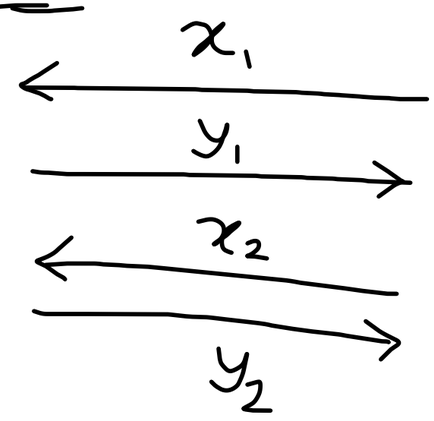
if for all PPT distinguisher $\mathcal{D}$



$$\left| \Pr_{k \xleftarrow{\$} \mathcal{K}}\left[\mathcal{D}^{F_k(\cdot)}(1^n) = 1\right] - \Pr_{f \xleftarrow{\$} Func(\{0,1\}^n, \{0,1\}^n)}\left[\mathcal{D}^{f(\cdot)}(1^n) = 1\right] \right| \leq negl(n)$$

① $F_k(x) = k \oplus x$. Is F a PRF?

F_k / f — $\mathcal{D}$



$\mathcal{D}$ returns 1 if $x_1 \oplus x_2 = y_1 \oplus y_2$

$y_1 = k \oplus x_1$
$y_2 = k \oplus x_2$
$y_1 \oplus y_2 = x_1 \oplus x_2$

$f \leftarrow Func(\{0,1\}^n, \{0,1\}^n)$

$\Pr[f(x) = c] = ?$

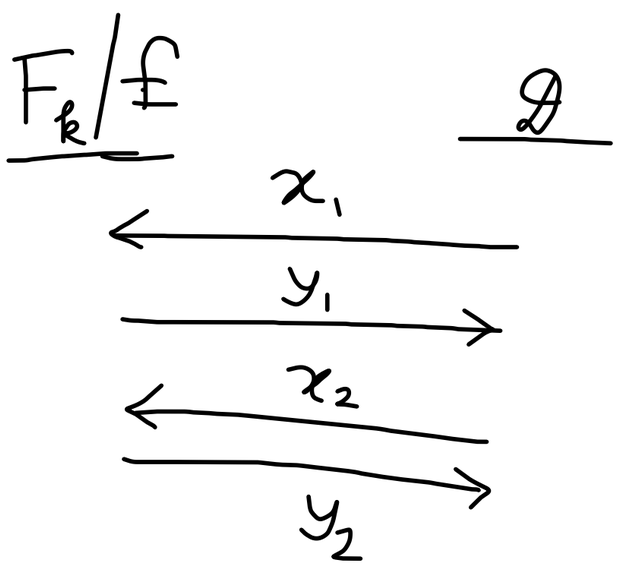
$\Pr[f(x_1) \oplus f(x_2) = c] = ?$

$$\Pr\left[\mathcal{D}^{F_k(\cdot)}(1^n) = 1\right] = 1$$

$$\Pr\left[\mathcal{D}^{f(\cdot)}(1^n) = 1\right] = \Pr\left[f(x_1) \oplus f(x_2) = x_1 \oplus x_2\right] \approx \frac{1}{2^n}$$

$$\left|\Pr\left[\mathcal{D}^{F_k(\cdot)}(1^n) = 1\right] - \Pr\left[\mathcal{D}^{f(\cdot)}(1^n) = 1\right]\right| = \left(1 - \frac{1}{2^n}\right)$$

① $F_k(x) = k \oplus x$. Is F a PRF?



$\mathcal{D}$ returns 1 if $x_1 \oplus x_2 = y_1 \oplus y_2$

$y_1 = k \oplus x_1$
$y_2 = k \oplus x_2$
$y_1 \oplus y_2 = x_1 \oplus x_2$

$f \leftarrow Func(\{0,1\}^n, \{0,1\}^n)$

$\Pr[f(x) = c] = ?$

$\Pr[f(x_1) \oplus f(x_2) = c] = ?$

$$\Pr\left[\mathcal{D}^{F_k(\cdot)}(1^n) = 1\right] = 1$$

$$\Pr\left[\mathcal{D}^{f(\cdot)}(1^n) = 1\right] = \Pr\left[f(x_1) \oplus f(x_2) = x_1 \oplus x_2\right] \approx \frac{1}{2^n}$$

$$\left|\Pr\left[\mathcal{D}^{F_k(\cdot)}(1^n) = 1\right] - \Pr\left[\mathcal{D}^{f(\cdot)}(1^n) = 1\right]\right| = \left(1 - \frac{1}{2^n}\right)$$

② $\Pi = (KG, Enc, Dec)$

$F: K \times \{0,1\}^n \to \{0,1\}^n$

$F \to PRF$

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

KG:
- $k \xleftarrow{\$} K$

Enc (m, k)

$r \xleftarrow{\$} \{0,1\}^n$

$c = (r, F_k(r) \oplus m)$

Dec $(c = (c_1, c_2), k)$

- $m = c_2 \oplus F_k(c_1)$

Π is IND-CPA secure (LOR) assuming F is a PRF

$$= \begin{pmatrix} r, & F_k(r) \oplus m \end{pmatrix}$$
$$\begin{pmatrix} c_1, & c_2 \end{pmatrix}$$

$r = c_1$

$$\begin{cases} F_k(r) \oplus m = c_2 \\ F_k(c_1) \oplus m = c_2 \\ m = F_k(c_1) \oplus c_2 \end{cases}$$