IND-CPA Notion

Recap

Ch | A

$k \leftarrow Kg(1^n)$

$b \xleftarrow{\$} \{0,1\}$ ← m_0, m_1

$c := Enc(k, m_b)$

$c \rightarrow$

$\leftarrow \hat{b}$

$Pr[PrivK^{eav}_{\mathcal{A},\pi}(n) = 1]$

$= Pr[\hat{b} = b]$

$\pi \rightarrow$ IND-Eav if

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

for all PPT $\mathcal{A}$.

Attacker Power

(IND-EAV)

- Ciphertext only
- Only works for Single-pair of Message

$c = G(k) \oplus m$

↓

IND-EAV secure if G is a PRG

IND-EAV notion for multiple Messages

Ch | A

$\mathcal{A} \rightarrow (M_0, M_1)$

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

$M_0 = (m_0^1, m_0^2, .., m_0^t)$

$M_1 = (m_1^1, m_1^2, .., m_1^t)$

$\forall i = 1(1)t$

$c_i = Enc(k, m_b^i)$

$|m_0^i| = |m_1^i|, \forall i$

$C = (c_1, ..., c_t) \rightarrow$

$\leftarrow \hat{b}$

Th^m: There doesn't exist any deterministic (stateless) Enc algo that is IND-EAV Secure for multiple encryption

Ch | A

$\leftarrow (M_0, M_1)$

$M_0 = (m_0, m_0)$

$M_1 = (m_1, m_1)$

$C = (c_0, c_1) \rightarrow$

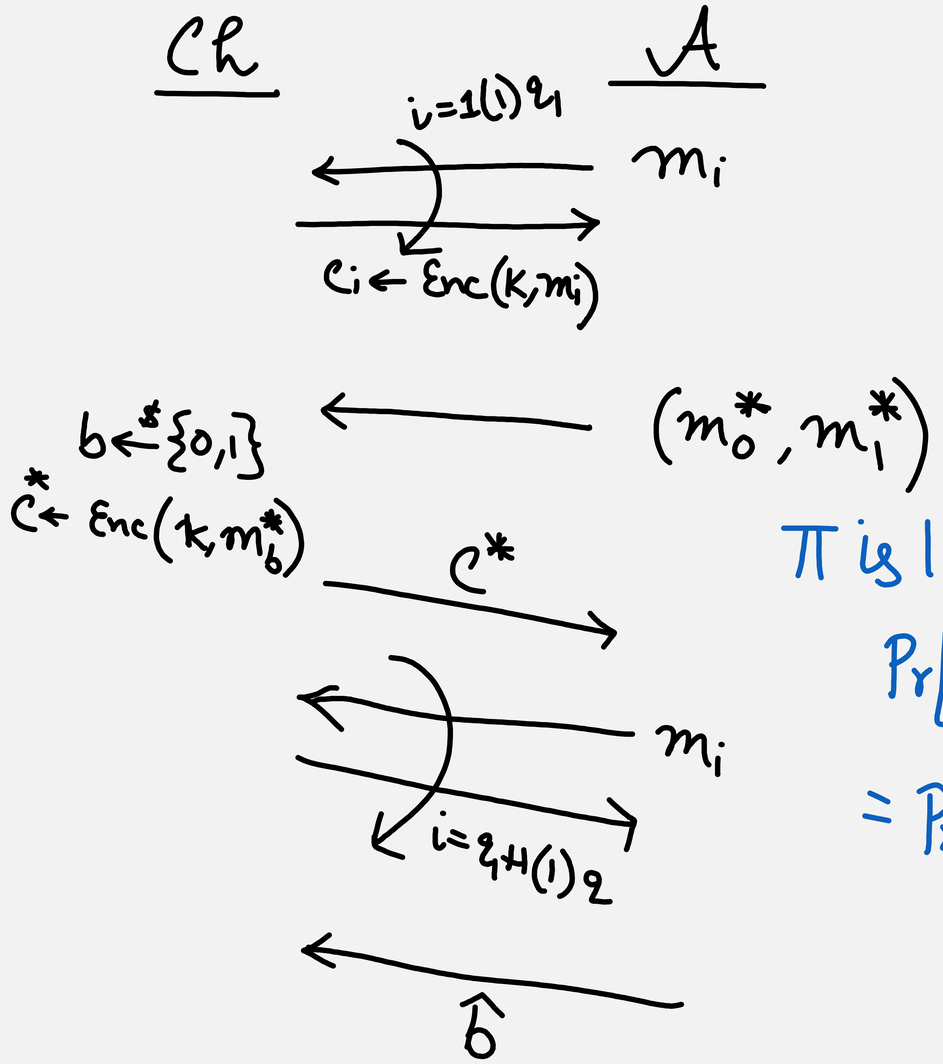
$\leftarrow \hat{b}$

if $c_0 = c_1$ then $\hat{b} \leftarrow 0$ else $\hat{b} \leftarrow 1$

if $b = 0 \Rightarrow$ $c_0 = G(k) \oplus m_0$, $c_1 = G(k) \oplus m_0$

if $b = 1 \Rightarrow$ $c_0 = G(k) \oplus m_0$, $c_1 = G(k) \oplus m_1$

IND-CPA (Indistinguishability under Chosen Plaintext Attack)

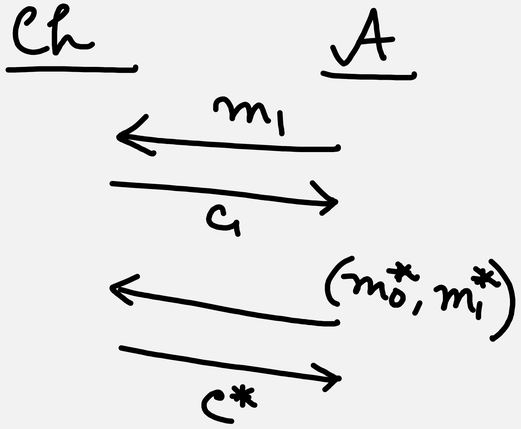


π is IND-CPA if $\forall$ PPT $\mathcal{A}$,

$$Pr[PrivK^{CPA}_{\mathcal{A},\pi}(n)=1]$$
$$= Pr[\hat{b}=b] \leq \frac{1}{2} + negl(n)$$

Does COTP achieve IND-CPA?

NO



$G(k) \oplus m_1 = c_1$

$\Rightarrow G(k) = m_1 \oplus c_1$

$c^* = G(k) \oplus m_0^*$ or $G(k) \oplus m_1^*$

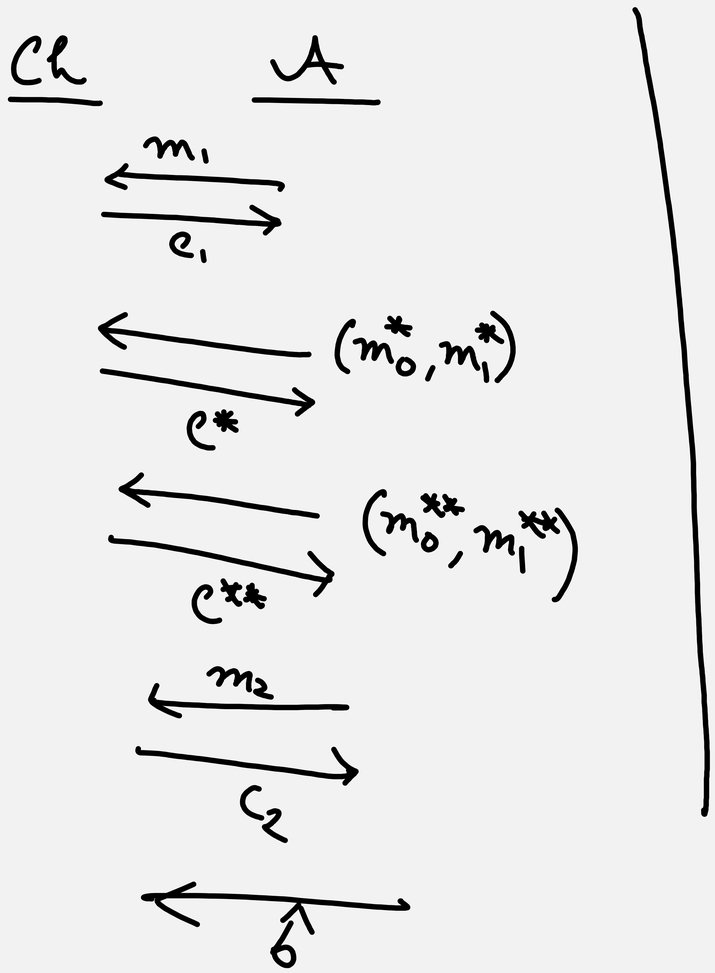
If $c^* = m_0^* \oplus m_1 \oplus c_1$

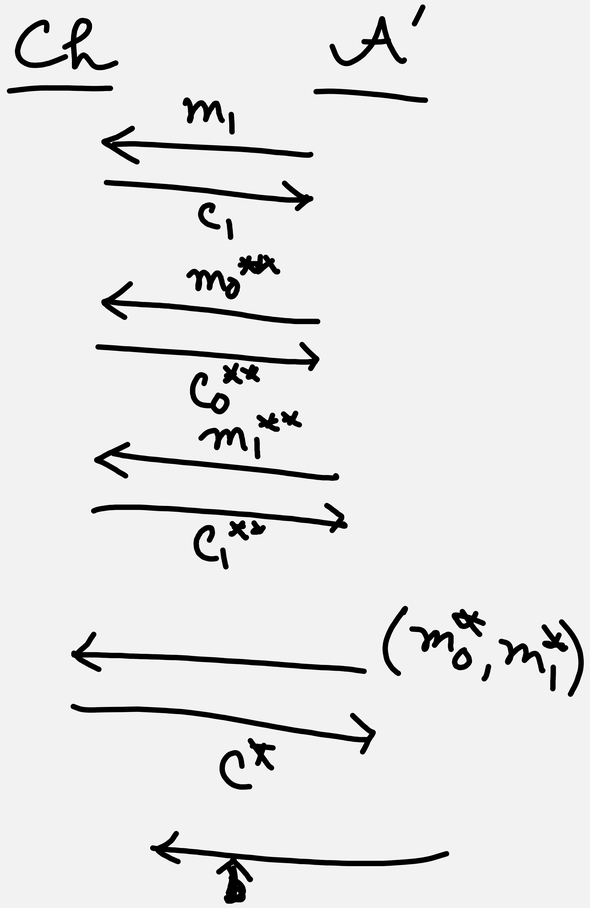
else $\hat{b}=0$

$\hat{b}=1$

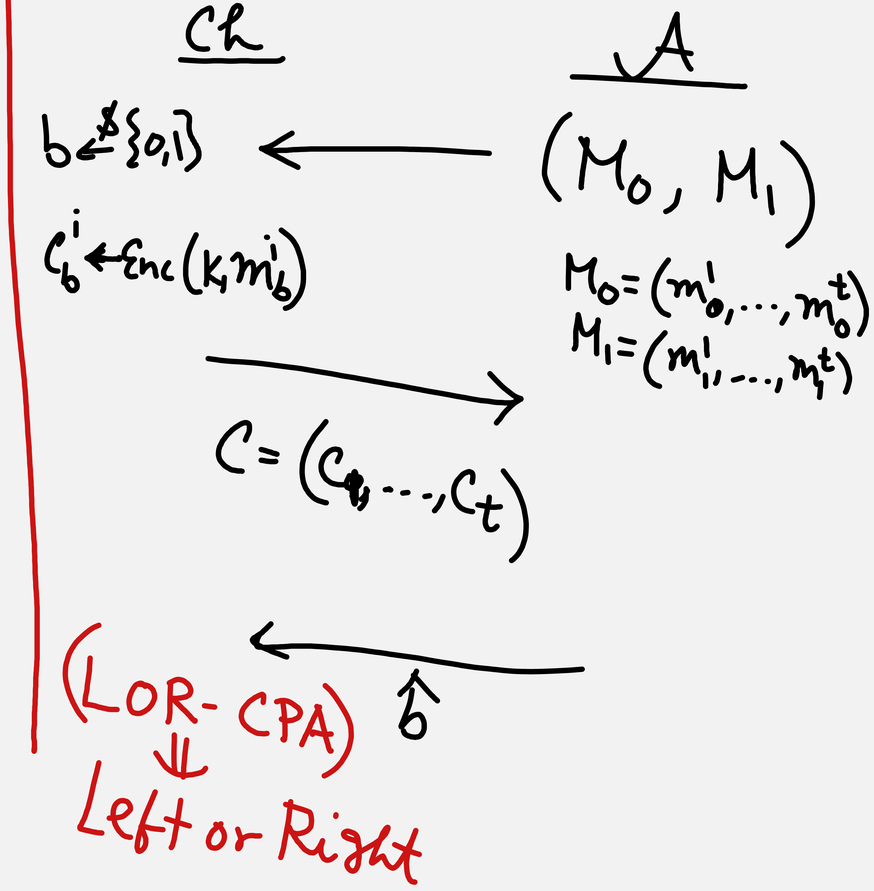
$\hat{b}$

Th^m: Π is IND-CPA secure against single-message adversary **if and only if** Π is IND-CPA for multiple messages.





Simple Variant of multiple messages



Pseudo-Random Function (PRF)

$F: \mathcal{K} \times \mathcal{M} \to \mathcal{R}$ is called PRF if

$\forall$ PPT adversary (called "Distinguisher") $\mathcal{D}$, the following holds:

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

- $\mathcal{K} = \mathcal{M} = \mathcal{R} = \{0,1\}^n$

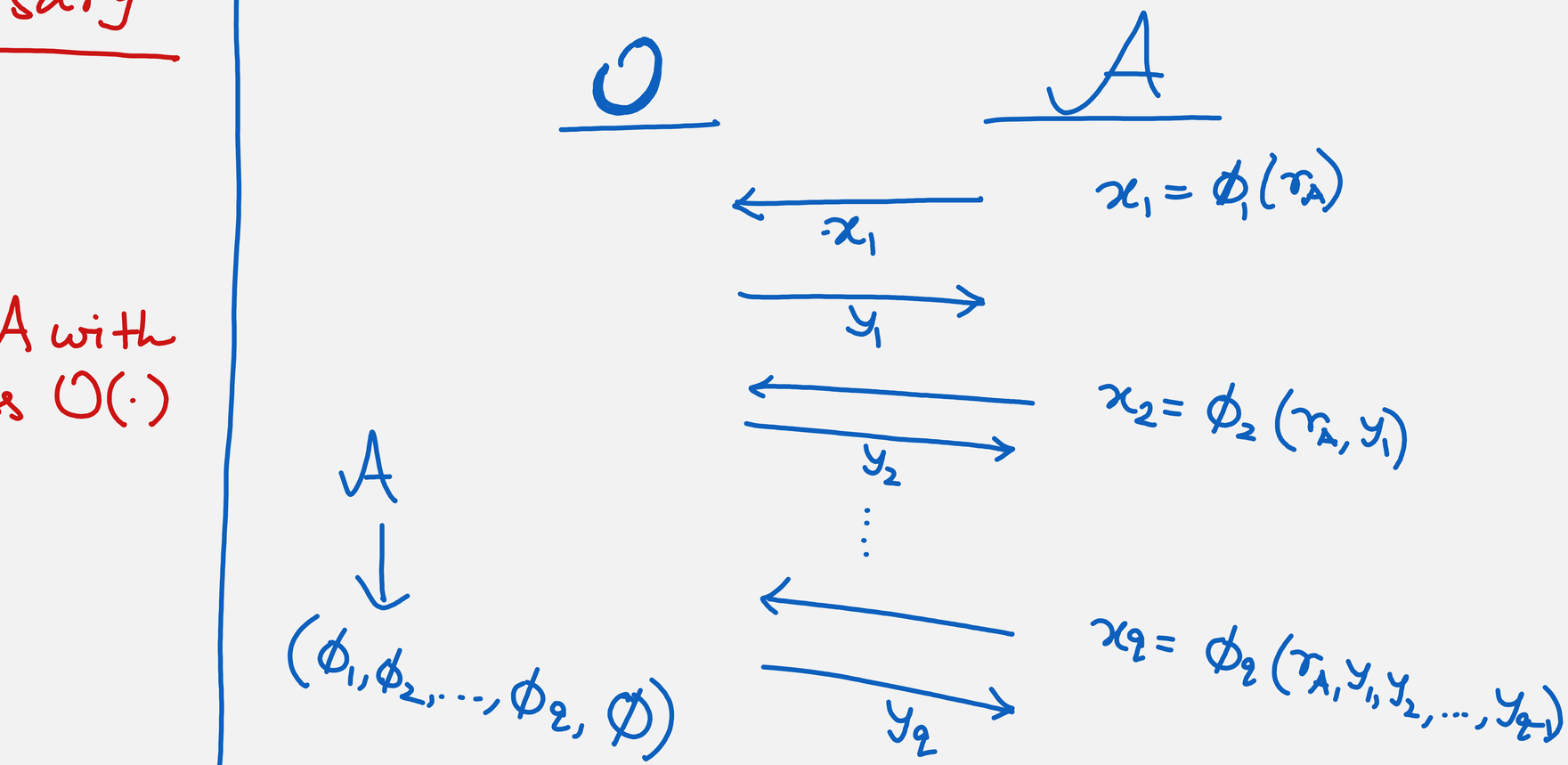
$$|Func(\{0,1\}^n, \{0,1\}^n)|$$

$$= (2^n)^{2^n} = 2^{n \cdot 2^n}$$

Oracle Adversary

$A^{O}(\cdot)$

↳ Adversary A with oracle access $O(\cdot)$



adaptive adversary

↳ i^{th} query depends on previous $(i-1)$ many responses

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

$F_k(m) = k \oplus m$

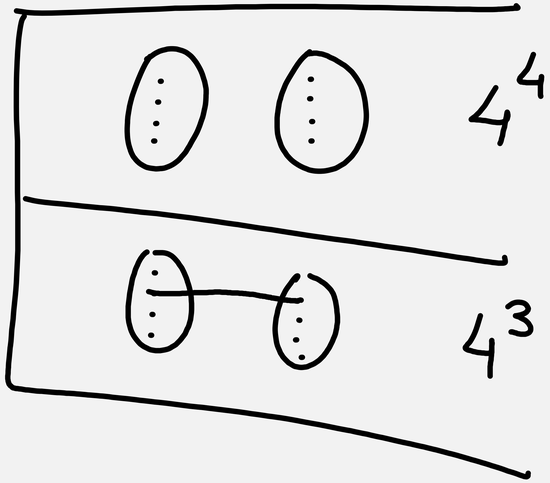
Is F a PRF?

NO

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

$\Pr[\mathcal{D}^{f(\cdot)} = 1] = \Pr[f(m_1) \oplus f(m_2) = m_1 \oplus m_2] = \frac{1}{2^n}$

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



$\mathcal{O}$	$\mathcal{D}$
F_k / f	
$b=1$ $b=0$	
$b \xleftarrow{\$} \{0,1\}$	m_1
if $b=1$	$\leftarrow$ c_1
Use F_k as $\mathcal{O}$	m_2
else	$\leftarrow$ c_2
Use f as $\mathcal{O}$	

If $\mathcal{O} = F_k$:

$c_1 = k \oplus m_1$

$c_2 = k \oplus m_2$

$\Rightarrow m_1 \oplus m_2 = c_1 \oplus c_2$

If $\mathcal{O} = f$:

$c_1 = f(m_1)$

$c_2 = f(m_2)$

$f(m_1) \oplus f(m_2) = m_1 \oplus m_2$

$m_1 \oplus m_2 = c_1 \oplus c_2$

ret 1

else

ret 0

$\Pr[f(m_1) = c_1] = \frac{\#f : f(m_1) = c_1}{\#f} = \frac{(2^n)^{2^n - 1}}{(2^n)^{2^n}} = \frac{1}{2^n}$

$\Pr[f(m_1) \oplus f(m_2) = c] = \sum_{c_1 \in \{0,1\}^n} \Pr[f(m_2) = c \oplus c_1 \mid f(m_1) = c_1] \cdot \Pr[f(m_1) = c_1] = \frac{1}{2^n}$

Encryption Scheme with IND-CPA Security

$\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^n$

$F: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$

Thm: If F is a PRF then Π achieves IND-CPA Security

Enc(k, m)

- Choose $r \xleftarrow{\$} \{0,1\}^n$
- define $c \leftarrow \left(r, F_k(r) \oplus m\right)$

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

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

- length-expanding
- randomized