CPA-Secure Encryption

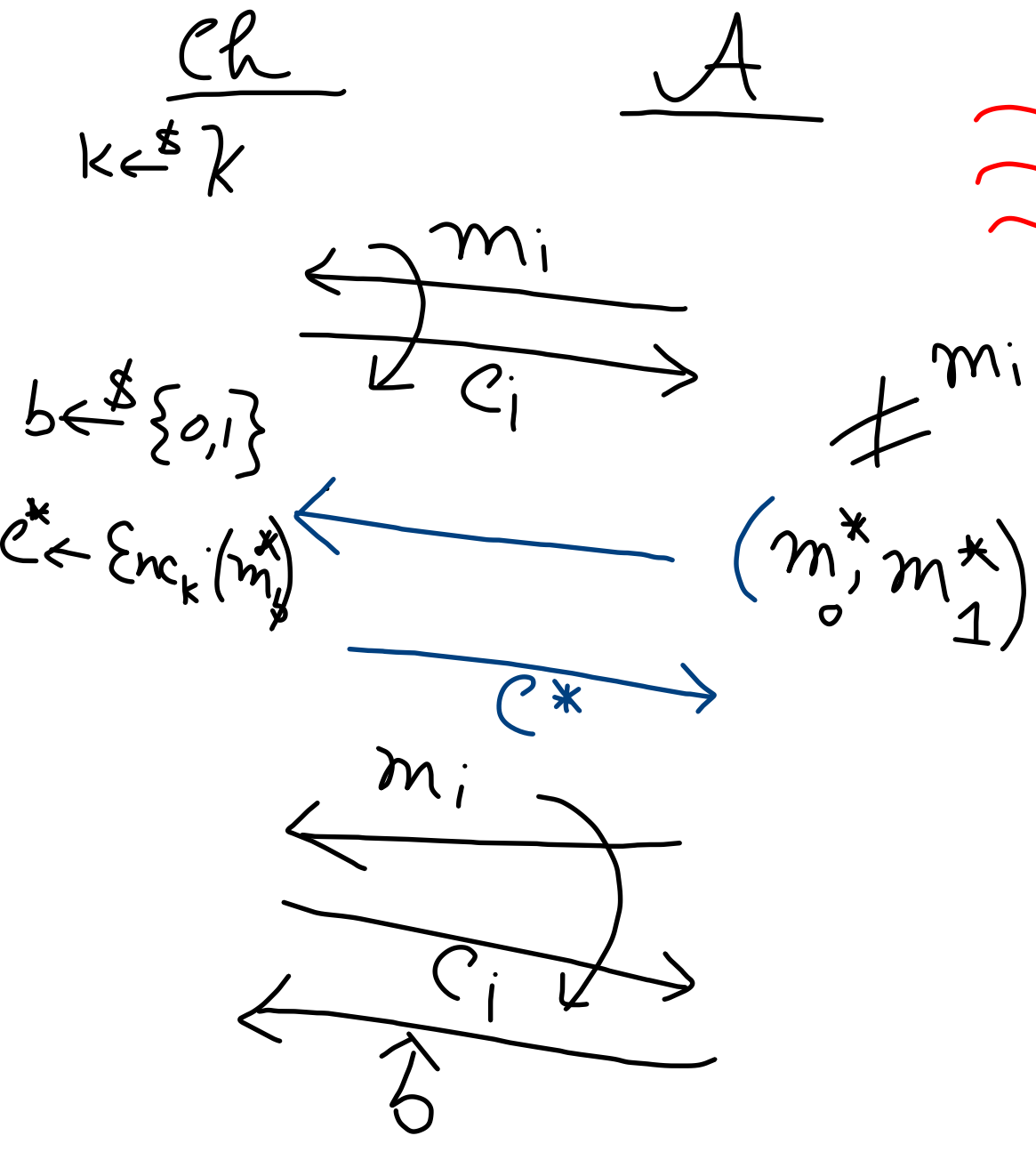
Recap

- Indistinguishability under Eavesdropping (S1)
- $G \rightarrow$ PRG, then Π that achieves S1.
- S1 $\rightarrow$ defined for single C/Ts
- S1' $\rightarrow$ Ind under eavesdropping (multiple encryption)
- Π doesn't achieve S1' (Infact no deterministic Π can achieve S1')
- S2 $\rightarrow$ S1 + CPA
- S2' $\rightarrow$ S2 + Multencryption (LOR)
- S2 $\equiv$ S2'

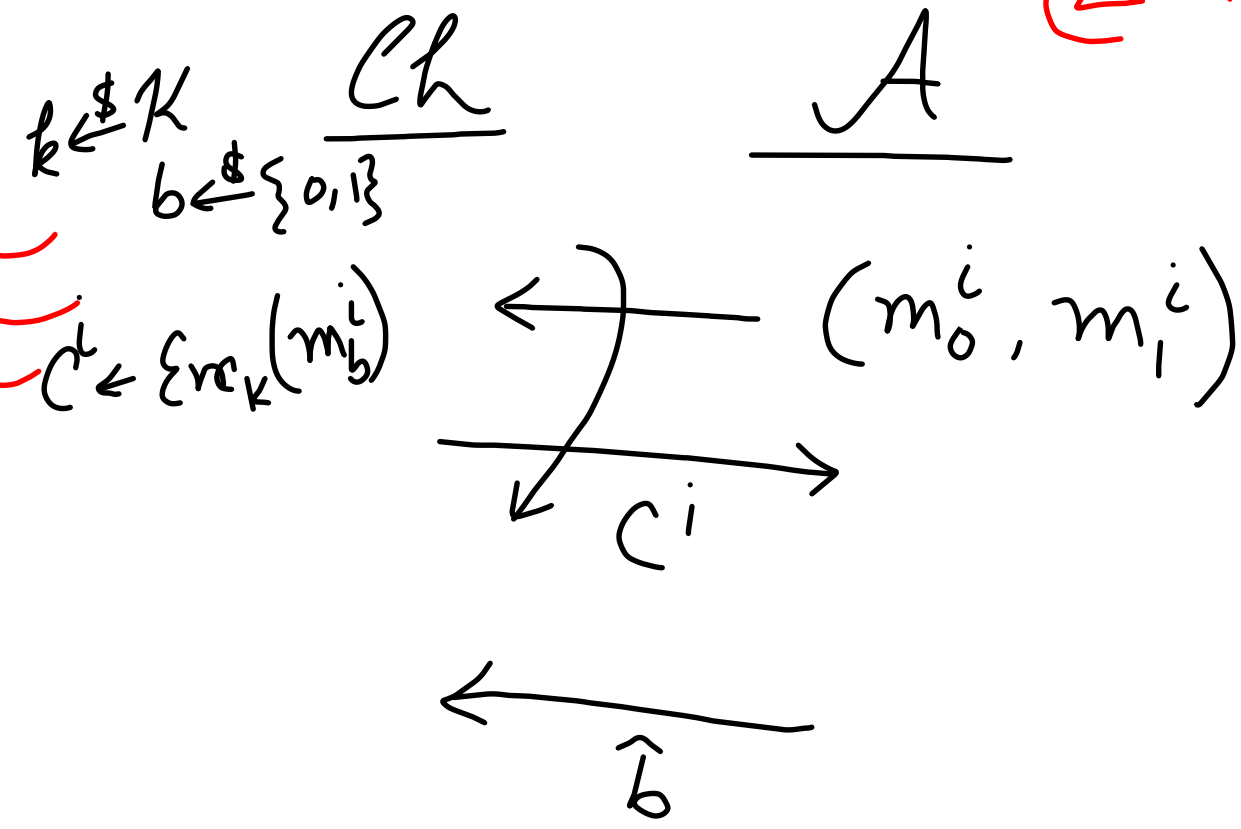
Content

- PRF (PRP, SPRP)
- $\Pi \rightarrow$ Assuming PRF exists, achieves S_2
- Modes of operation using PRF/PRP

Indistinguishability under CPA

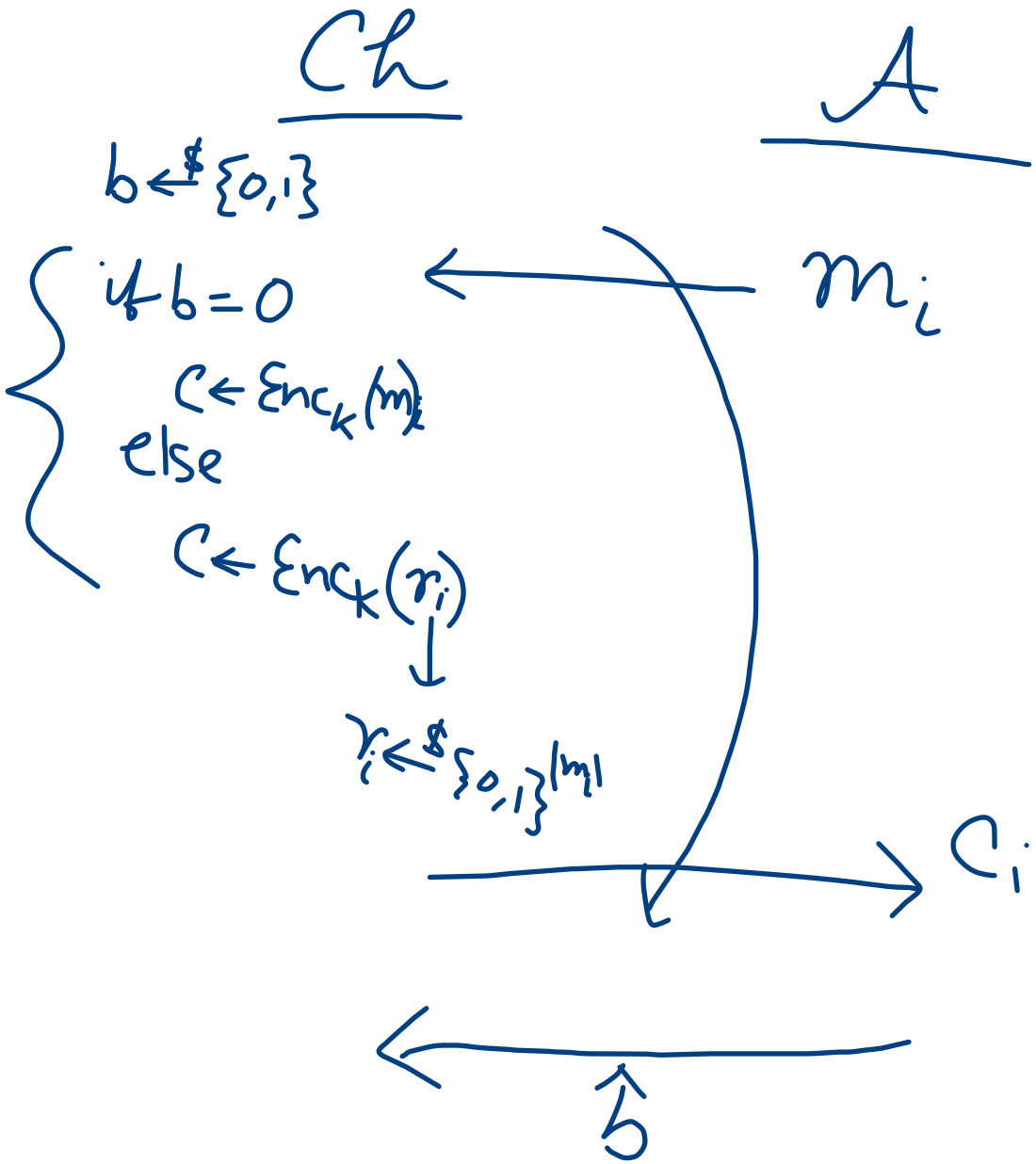


Ind under CPA (Multiple Enc) (LOR)



Ind under CPA (ROR)

↳ (Real or Random)



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

↳ π Secure

Result

LOR ≡ ROR (Home Work)

PRF (Pseudo Random Function)

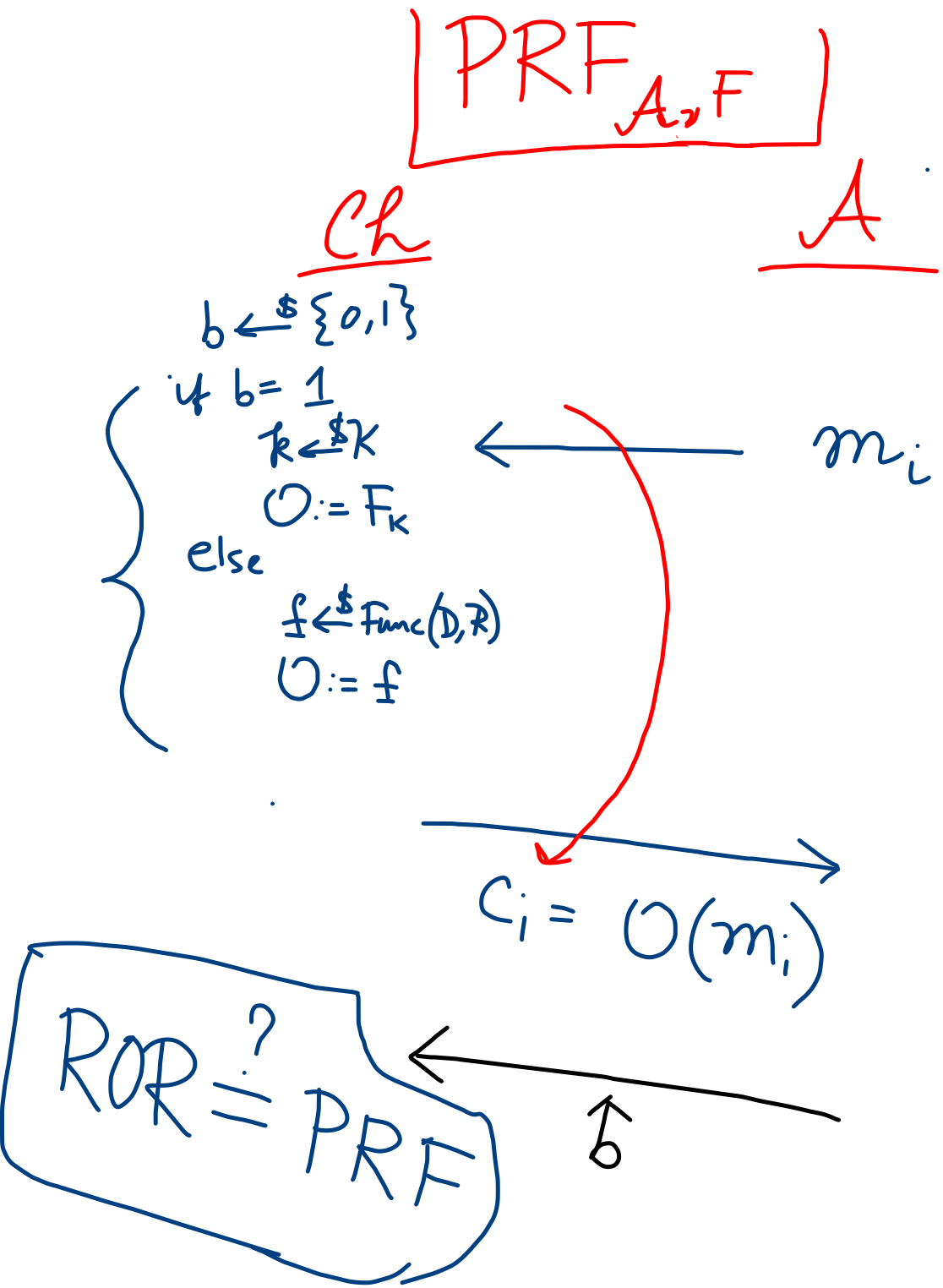
$F: \{0,1\}^{*}_{(key)} \times \{0,1\}^{*}_{(i/p)} \to \{0,1\}^{*}_{(o/p)}$ is called a PRF

if $\forall$ PPT adv $\mathcal{D}$, $\exists$ negl, (Security parameter $\to n$)

$$\forall K \in \mathcal{K}, \left| \Pr\left[\mathcal{D}^{F_K(\cdot)} = 1\right]_{K \xleftarrow{\$} \mathcal{K}} - \Pr\left[\mathcal{D}^{f(\cdot)} = 1\right]_{f \xleftarrow{\$} Func} \right| \leq negl(n)$$

(Indistinguish F_K from a random function.)

Permutation
↳ PRP



$$\begin{cases} PRF_{A,F} = 1 \text{ if } b = \hat{b} \end{cases}$$

$$\boxed{Pr\left[PRF_{A,F} = 1\right] \leq \frac{1}{2} + negl}$$

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

$$= \frac{1}{2}\left[\hat{b} = 1 \mid b = 1\right] + \frac{1}{2}\left[\hat{b} = 0 \mid b = 0\right]$$

$$= \frac{1}{2} Pr\left[A^{F_k} = 1\right] + \frac{1}{2} \cdot Pr\left[A^{f} = 0\right]$$

$$= \frac{1}{2} + \frac{1}{2}\left(Pr\left[A^{F_k} = 1\right] - Pr\left[A^{f} = 1\right]\right) \quad \left(1 - Pr\left[A^{f} = 1\right]\right)$$

Examples

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

$F_k(x) = k \oplus x$

Is F a PRF?

F_k / f — A

$A \to F_k/f$: x_1

$F_k/f \to A$: y_1

$A \to F_k/f$: x_2

$F_k/f \to A$: y_2

$A \to F_k/f$: $\hat{b}$

If $(x_1 \oplus x_2 = y_1 \oplus y_2)$ then $\hat{b} \leftarrow 1$

else $\hat{b} \leftarrow 0$

If $b=1$ i.e. F_k

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

$y_1 = f(x_1)$

$y_2 = f(x_2)$

$f(x_1) \oplus f(x_2) \oplus x_1 \oplus x_2 = 0$

$$Adv^{PRF}_{A,\pi} = \left| 1 - \frac{1}{2^n} \right|$$

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

π

$\underline{Enc_K(M)}$

- $r \xleftarrow{\$} \{0,1\}^n$
- return $(r, F_K(r) \oplus m)$

$\underline{Dec_K(C)}$

- $(C_1, C_2) \leftarrow C$
- $m \leftarrow F_K(C_1) \oplus C_2$

If F is PRF secure then π is IND-CPA

$F_K / \mathfrak{f}$

$\mathcal{D}$

$\mathcal{A}$

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

m_i

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

r_i

$y_i = \mathcal{O}(r_i)$

$c_i = (r_i, y_i \oplus m_i)$

c_i

Π

Case F_K

m_i

r_i

$F_K(r_i) \oplus m_i$

(m_0^*, m_1^*)

$c_i^* = F_K(r^*) \oplus m_i^*$

b

r^*

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

y^*

$c^* = (r^*, m_b^* \oplus y^*)$

$\hat{b}$

1, if $\hat{b} = b$

This is the O/p (not bit guessing)

(m_0^*, m_1^*)

Π

Case $\mathfrak{f}$

m_i

$(r_i, m_i \oplus y_i)$

(m^*, y^*)

b

Ex

F : PRF

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

$F': \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^{2n+2}$

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

is not PRF.

$F_k(0\|x)$ → $0\_\_\_$; $F_k(x\|1)$ → $\_\_\_1$

F′ — A

$M_1 = 001$

$c_1 = F_k(0001) \| F_k(0011)$ (c_1^2)

$M_2 = 011$

$c_2 = F_k(0011) \| F_k(0111)$ (c_2^1)

PRF Adv

$$\left| 1 - \frac{1}{2^{n+1}} \right|$$

$F \to PRF$

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

$$\left| Pr[PrivK^{CPA}_{\pi, A} = 1] - Pr[PrivK^{CPA}_{\tilde{\pi}, A} = 1] \right| \leq negl(n)$$

BAD occurs if $r^* \in \{r_1, \ldots, r_q\}$ $\Rightarrow$ if BAD occurs then A can trivially distinguish

$$Pr[PrivK^{CPA}_{\tilde{\pi}, A} = 1]$$

$$\leq Pr[BAD] + Pr[PrivK^{CPA}_{\tilde{\pi}, A} = 1 \wedge \overline{BAD}]$$

$$\leq \left(\frac{q}{2^n} + \frac{1}{2}\right)$$

$$\Pr\left[\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},\Pi} = 1\right] \leq \frac{1}{2} + \frac{q}{2^n} + \mathrm{negl}(n)$$