Some Interesting Problems

① Let F be PRF,

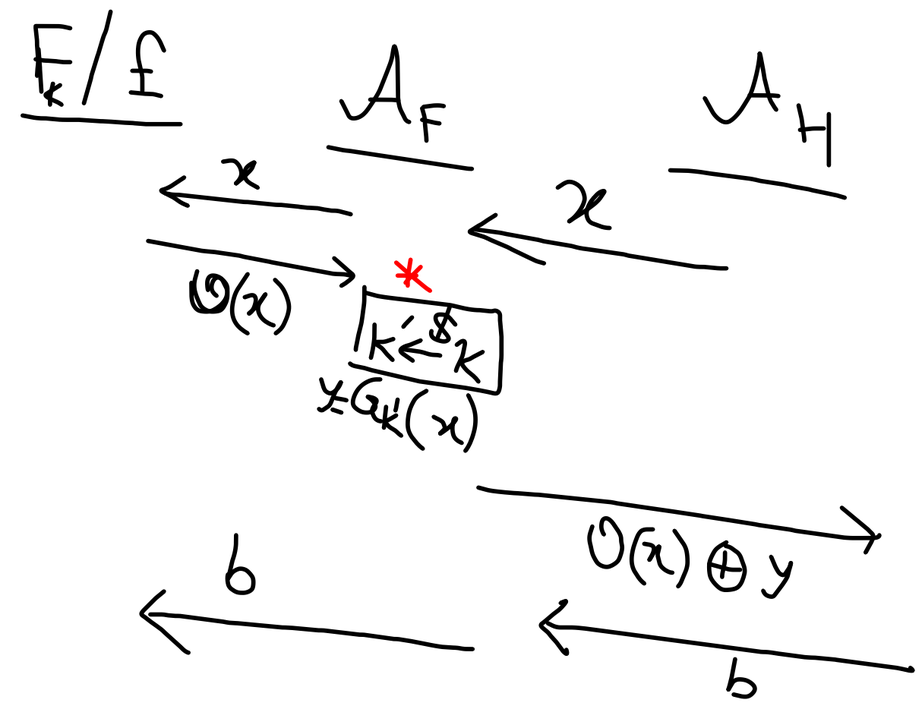
② $H^{(x)}_{K,K'} := F_K(x) \oplus G_{K'}(x)$

ⓑ $H^{(x)}_{K,K'} = F_K(x) \| G_{K'}(x)$

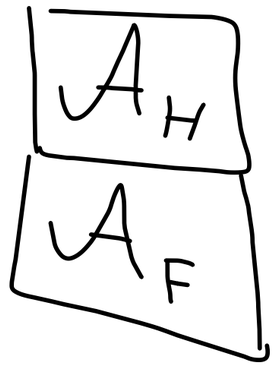
x x

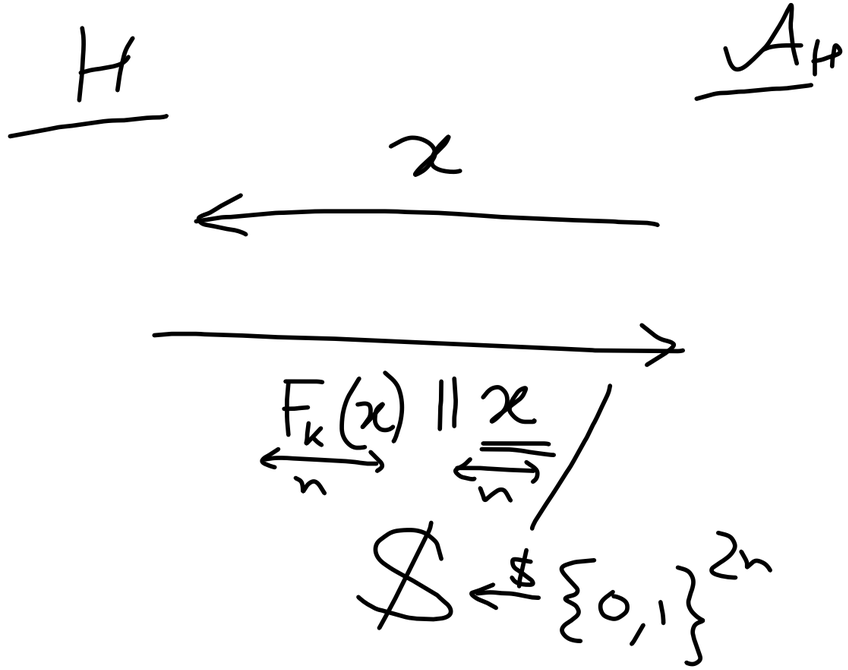
(*) → 1 time

F_K / f



Is H PRF?



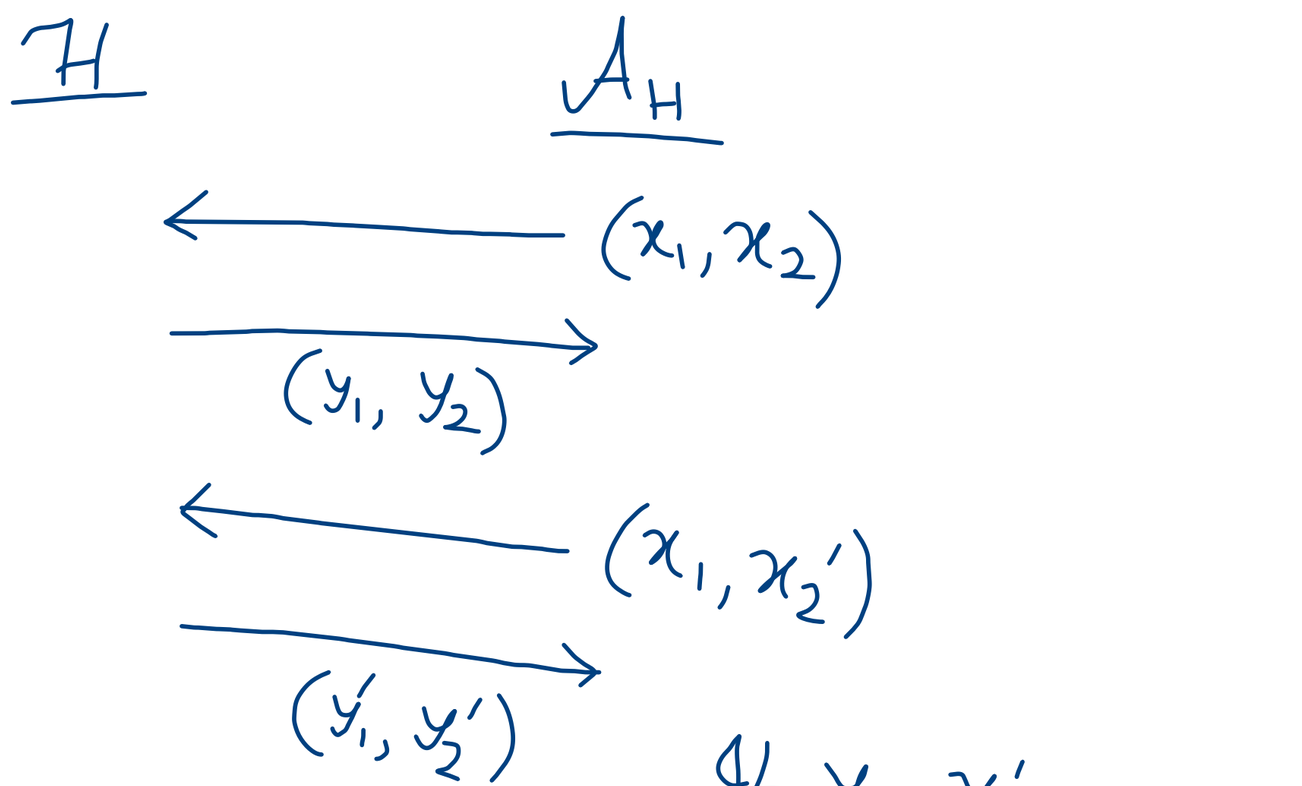


$H_{k_1 k_2}(x) = F_{k_1}(x) \,||\, G_{k_2}(x)$

↳ We need both F & G to be PRF

$$H_{K_1,K_2}(x_1, x_2) = F_{K_1}(x_1) \,||\, G_{K_2}(x_2)$$

(F, G Both PRF)



- PRF
- MAC

$H_{k_1,k_2}(x_1,x_2) = F_{k_1}(x_1) \oplus G_{k_2}(x_2)$

$\{ K_1, K_2 \leftarrow$ indep unif
$F, G \rightarrow$ PRF

(m_1, m_2)

$T = ?$

$\leftarrow (m_1, *)$
$\rightarrow y_1$
$\leftarrow (0, m_2)$
$\rightarrow y_2$
$\leftarrow (0, *)$
$\rightarrow y_3$

$y_1 \oplus y_2 \oplus y_3$

H	A_H
	$\leftarrow m_1', m_2'$
	(x_1, x_2)
y_1	$\rightarrow$
	m_1' (m_2)
	$\leftarrow (x_1, x_2')$
y_2	$\rightarrow$
	(m_1) m_2'
	$\leftarrow (x_1', x_2)$
y_3	$\rightarrow$
	$\leftarrow (x_1', x_2')$
	m_1 m_2
y_4	$\rightarrow$

$y_1 = F_{k_1}(x_1) \oplus G_{k_2}(x_2)$

$y_2 = F_{k_1}(x_1) \oplus G_{k_2}(x_2')$

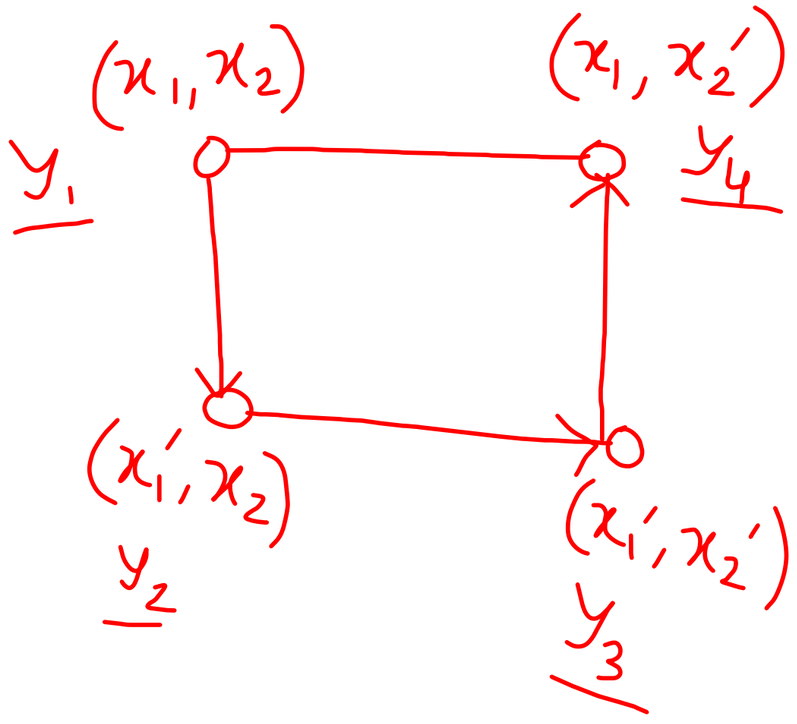
$y_3 = F_{k_1}(x_1') \oplus G_{k_2}(x_2)$

$y_1 \oplus y_2 \oplus y_3 = F_{k_1}(x_1') \oplus G_{k_2}(x_2')$

$y_1 \oplus y_2 = G_{k_2}(x_2) \oplus G_{k_2}(x_2')$

If $y_1 \oplus y_2 \oplus y_3 \stackrel{?}{=} y_4$ }

Alternating Cycle



Is H is Secure?

② $H_K(x) = F_K(x) \oplus G_K(x)$

(Both F & G are PRF)

(Dependent key)

If $F \equiv G$

→ Not Secure

$G_K(x) = 2 \cdot F_K(x)$

→ Secure

/ $G(x) = 0$ (G not PRF)

↓

Secure

② Is H is Secure?

$$H_K(x) = F_K(x) \oplus G_K(x)$$

(Both F & G are PRF)

(Dependent key)

If $F \equiv G$
→ Not Secure

$G_K(x) = 2 \cdot F_K(x)$
→ Secure

/ $G(x) = 0$ (G not PRF)
↓
Secure

$$H_{k_1,\ldots,k_n}(x_1, x_2, \ldots, x_n) := F_{k_1}(x_1) \oplus F_{k_2}(x_2) \oplus \cdots \oplus F_{k_n}(x_n)$$

Mount an universal forgery

$(m_1, \ldots m_n, C_1 \oplus C_2 \oplus C_3)$

$\Downarrow$

Forgery

$\longleftarrow$ $(m_1' m_2 \cdots m_n)$

C_1

$\longleftarrow$ $(m_1\ m_2'\ m_3 \cdots m_n)$

C_2

$\longleftarrow$ $(m_1'\ m_2'\ m_3 \cdots m_n)$

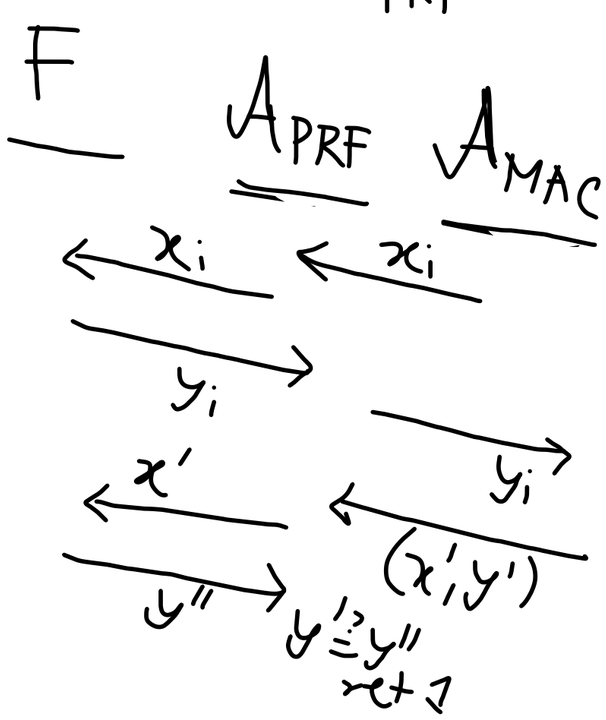
C_3

PRF & MAC

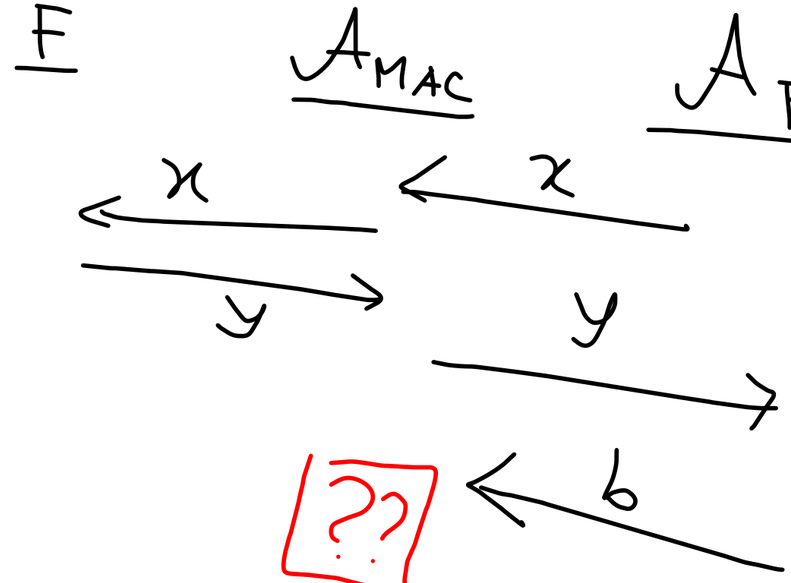
PRF ⇒ MAC

If F is a PRF, F is MAC

$\mathcal{A}_{MAC} \rightarrow \mathcal{A}_{PRF}$



MAC ⇒ PRF



MAC $\not\Rightarrow$ PRF

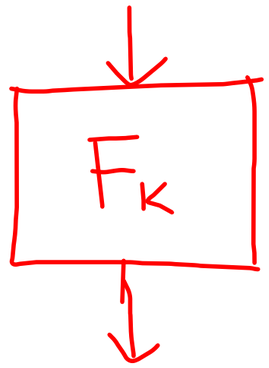
Let F be PRF. F is a MAC. How about $F'_k(m) = F_k(m) \| \underline{0}$?

(m ↑)

Is F' a MAC?

$\Downarrow$

$F' \Rightarrow$ not a PRF



F: PRF

E: PRP

$\Rightarrow$ Block-Cipher

$k \geq n$

$n = 128, 256, 64$

- # permutations of n-bit: $2^n!$
- # distinct perm. $= 2^k$
  - Design
  - AES, Present
  - Cryptanalysis

$E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$

$\forall k \in K, \; E_k: \{0,1\}^n \rightarrow \{0,1\}^n$

Security: (PRP) $\hookrightarrow$ permutation