$F_k(\cdot)$ PRF

$G_k(x) = \text{rot}(F_k(x))$

$$\begin{tikzcd} 11000 \arrow[d] \\ 01100 \end{tikzcd}$$

If $F_K(\cdot)$ is a PRF, is $G_k(\cdot)$ a PRF?

-yes

Enc
MAC
Hash

$G_k(\cdot) \neq \text{PRF} \Rightarrow F_k(\cdot) \neq \text{PRF}$

$$|Pr(D^{G_k(\cdot)}(1^n)=1) - Pr(D^{f(\cdot)}(1^n)=1)| \neq \underset{\overset{\shortparallel}{\frac{1}{n^{100}}}}{negl(n)}$$

$$\begin{tikzcd} \text{Oracle } F_k(\cdot) \arrow[r, Rightarrow] \arrow[d] & \text{Oracle } G_k(\cdot) \\ \text{rot}(F_k(x)) & \end{tikzcd}$$

$$|Pr(\hat{D}^{F_k(\cdot)}(1^n)=1) - Pr(\hat{D}^{f(\cdot)}(1^n)=1| \neq negl(n)$$

$$\begin{tikzcd}[column sep=small]
 & m = m_1 \arrow[d] & \cdots & m_k \arrow[d] \\
\text{fresh} & \langle \textcircled{r}, t_1 & \cdots & t_k \rangle
\end{tikzcd}$$

$t_i = mac_k(r \| \cancel{\ell} \| \cancel{i} \| m_i)$

$\downarrow$

drop

-reordering -truncation -mix-and-match

$$\left[\begin{array}{l} m = m_1 \; m_2 \\ \langle r, t_1 \; t_2 \rangle \end{array}\right. \qquad \begin{array}{l} t_1 = mac_k(r \| \ell \| m_1) \\ t_2 = mac_k(r \| \ell \| m_2) \end{array}$$

$\downarrow$ A oracle $Mac_k(\cdot)$

$$\langle r, t_2, t_1 \rangle \xrightarrow{\text{tag for}} \begin{array}{l} m_2 m_1 \\ m_2 \neq m_1 \end{array}$$

$m = m_1 \; m_2$

$\langle r, t_1, t_2 \rangle$

$$\langle r, t_1 \rangle \xrightarrow{\text{tag for}} m_1$$

~~MA~~

$F_k(\cdot)$ is PRF $\Longrightarrow$ MAC_k is secure

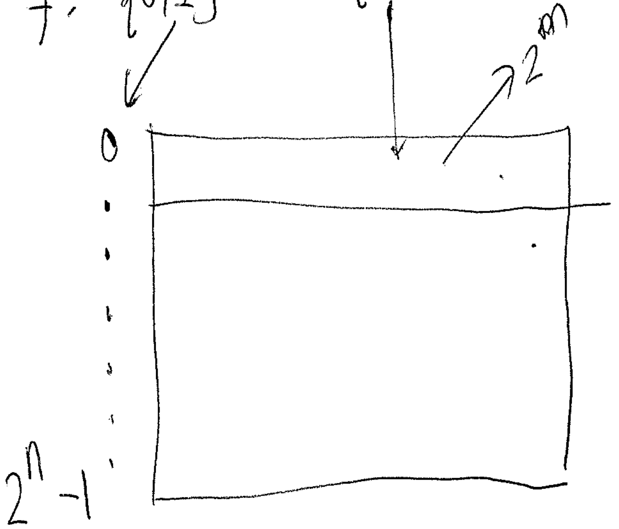
$t = F_k(m)$

$Mac_k(\cdot) \neq$ secure $\Longrightarrow$ $F_k(\cdot) \neq PRF$

$\mathcal{A} \longrightarrow \mathcal{D}$

Mac-forge

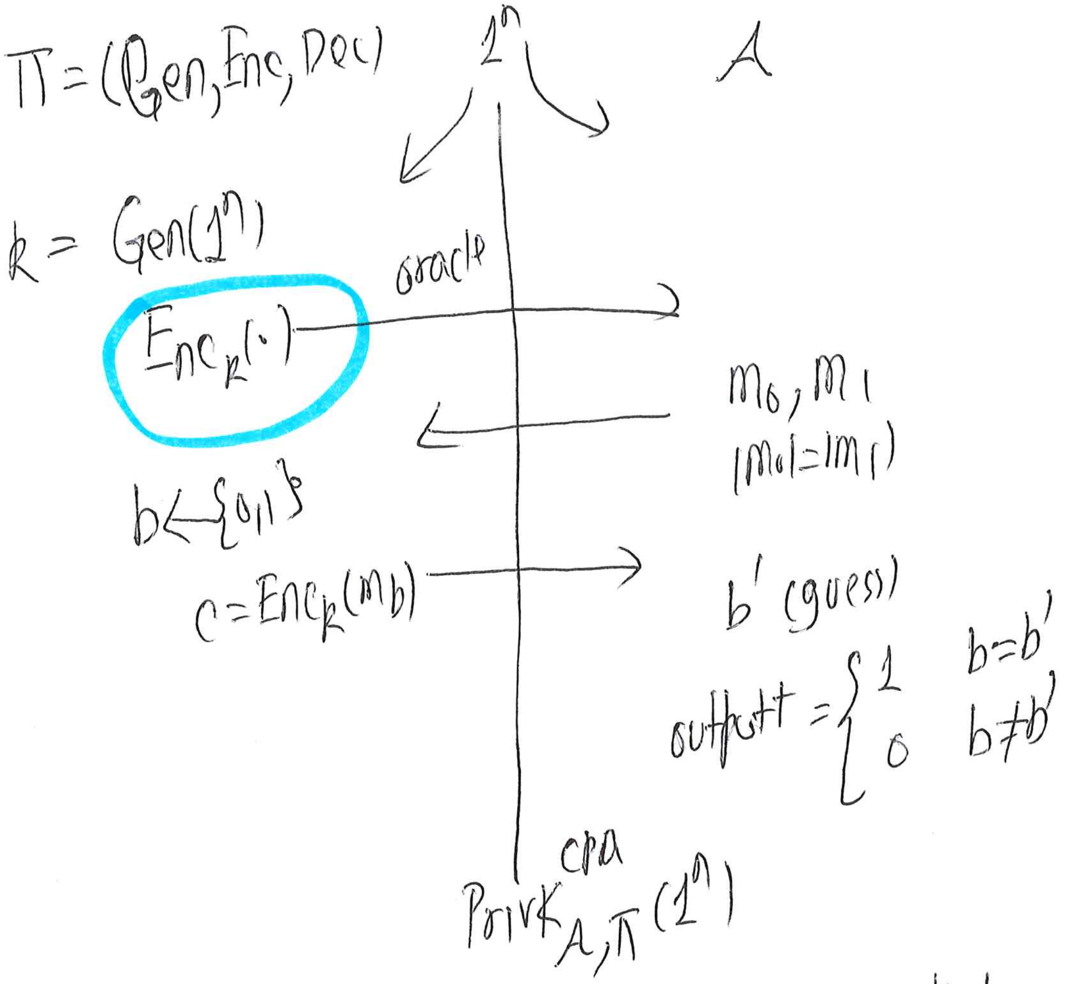
$f: \{0,1\}^n \longrightarrow \{0,1\}^m$



$$\underbrace{2^m \cdot 2^m \cdot \ldots 2^m}_{2^n \text{ times}}$$

$$\shortparallel$$

$$2^m \cdot 2^n$$



$\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$

1^n

$\mathcal{A}$

$k = \text{Gen}(1^n)$

oracle

$\text{Enc}_k(\cdot)$

m_0, m_1

$|m_0| = |m_1|$

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

$c = \text{Enc}_k(m_b)$

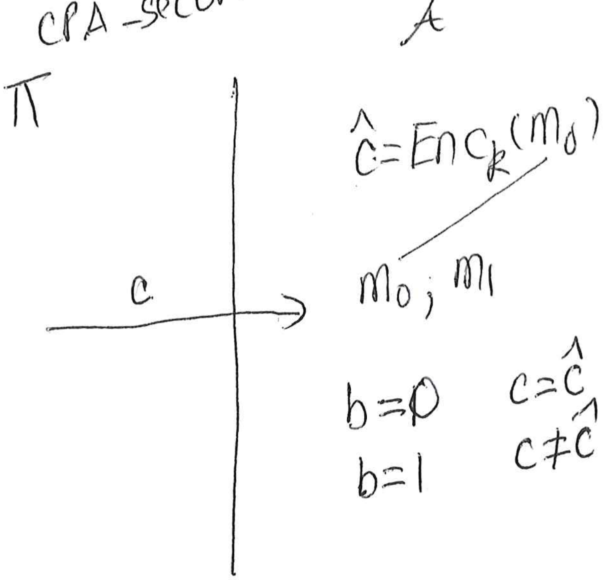
b' (guess)

$$\text{output} = \begin{cases} 1 & b = b' \\ 0 & b \neq b' \end{cases}$$

$\text{PrivK}^{cpa}_{\mathcal{A},\Pi}(1^n)$

For all PPT $\mathcal{A}$ $|\Pr(\text{PrivK}^{cpa}_{\mathcal{A},\Pi}(1^n) = 1| \leq \frac{1}{2} + \text{negl}(n)$

-no deterministic scheme is CPA-secure.



$\mathcal{A}$

Π

$\hat{c} = \text{Enc}_k(m_0)$

$m_0; m_1$

c

$b = 0$ $c = \hat{c}$

$b = 1$ $c \neq \hat{c}$

$H(\cdot\ )$

2nd-preimage

$\mathcal{A}$: given $x, H^s(\cdot)$

out x'

$H^s(x)=H^s(x')$

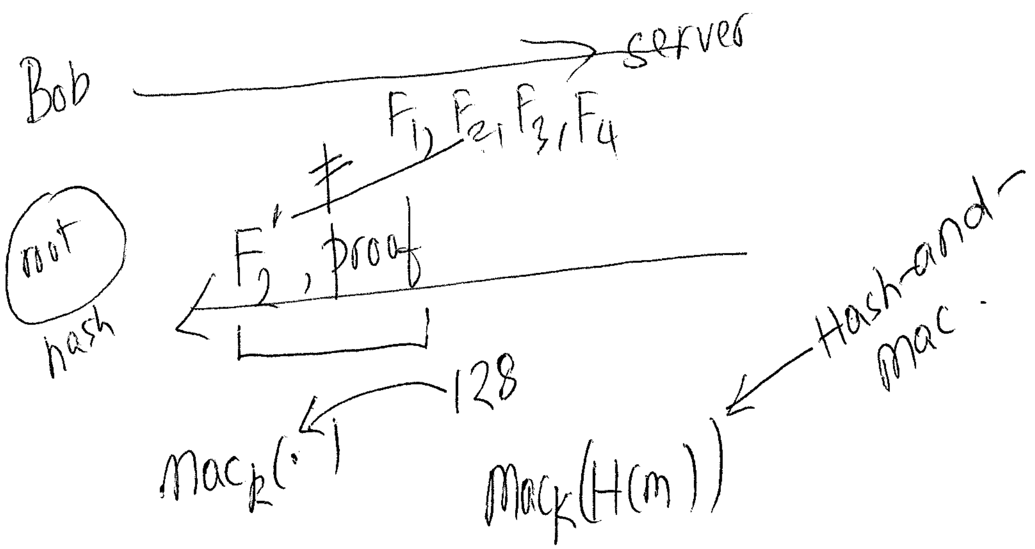
preimage.

$\mathcal{A}$: 128

given $H^s(\cdot), y$

out x

$H^s(x)=y$


Bob
server
F1, F2, F3, F4
≠
F2', proof
root hash
128
mac_k(·)
Mac_k(H(m))
Hash-and-mac.