PSEUDO-RANDOM PERMUTATION (PRP)

Verificador. Adversario

① Ver elige $b \in \{0,1\}$

- si $b=0$, elige clave $k \in K$, define $\boxed{f(x) = Enc(k,x)}$
- si $b=1$, elige una permutación al azar $\boxed{f(x) = \pi(x)}$

② El adversario elige un mensaje m, y el verificador le entrega $f(m)$.

③ el paso 2 se repite
q veces

④ adversario tiene que
decidir si $b=0$ o $b=1$

Enc es un pseudo-random
permutation (PRP)

Ejemplo: OTP no es
un PRP con $q=2$

Verificador elige $b \in \{0,1\}$

$b=0$, elige k $\quad f(x) = Enc(k,x)$

$b=1$, elige Π $\quad f(x) = \Pi(x)$

(2) $\quad m_1 \to f(m_1)$

$\quad \overline{m_1} \to f(\overline{m_1})$

(4) $\quad f(m_1)$ XOR $f(\overline{m_1})$

$b=0$

$(m_1 \text{ XOR } K) \text{ XOR } (\overline{m_1} \text{ XOR } K)$

$= \underline{(m_1 \text{ XOR } \overline{m_1})} \text{ XOR } (\cancel{K \text{ XOR } K}) \; 0$

$= \underline{1 \dots 1}$

$b = 1$ $\qquad m_1 \to \overline{\Pi}(m_1)$

$\qquad\qquad \overline{m_1} \to \overline{\Pi}(\overline{m_1})$

¿Qué tendría que pasar para que $\overline{\Pi}(m_1)$ XOR $\overline{\Pi}(\overline{m_1}) = 1 \ldots 1$?

$$Pr\left(\overline{\Pi}(m_1) \text{ XOR } \overline{\Pi}(\overline{m_1}) = 1 \ldots 1\right)$$

$$= \boxed{\overline{\Pi}(\overline{m_1})} = \boxed{\overline{\overline{\Pi}(m_1)}}$$

$$\overline{\Pi}(m_1) = m$$

$$Pr\left(\overline{\Pi}(\overline{m_1}) = \overline{m}\right) = \frac{1}{2^n}$$

supongamos que los mensajes tienen largo n

$$m_1 \longrightarrow f(m_1) = \Pi(m_1)$$

$$\overline{m_1} \longrightarrow f(\overline{m_1}) = \Pi(\overline{m_1})$$

$$Pr\big(f(m_1) \text{ XOR } f(\overline{m_1}) = 1\ldots1\big)$$

$$Pr\big(\Pi(m_1) \text{ XOR } \Pi(\overline{m_1}) = 1\ldots1\big)$$

$$\Pi(\overline{m_1}) = \overline{\Pi(m_1)}$$

$$m = \Pi(m_1)$$

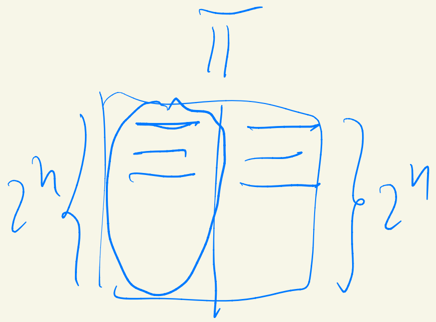
$$Pr\big(\Pi(\overline{m_1}) = \overline{m}\big) = \frac{1}{2^n}$$

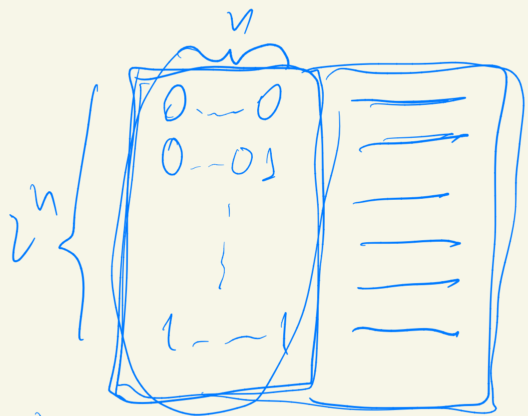
$$Pr\big(\Pi(x) = y\big) = \frac{1}{2^n}$$

$$Pr\big(\Pi(0\ldots0) = 1\ldots1\big) = \frac{1}{2^n}$$

$$\Pi \quad \overset{n}{\boxed{2^n}}\,\overset{n}{\boxed{2^n}}$$

$\Pi(0 \dots 0) = 1 \dots 1$





$f: \{0,1\}^n \to \{0,1\}^n$

$\cancel{2^{2^n}}$

$\boxed{(2^n)!}$

00	10
01	00
10	11
11	01

$n = 2$

$(2^n)!$

$1 \to 3$
$2 \to 2$
$3 \to 1$
$4 \to 4$

$2^2 = 4$

$4! = 24$

$1, 2, 3 \to 6$

$1, 2, 3, 4$

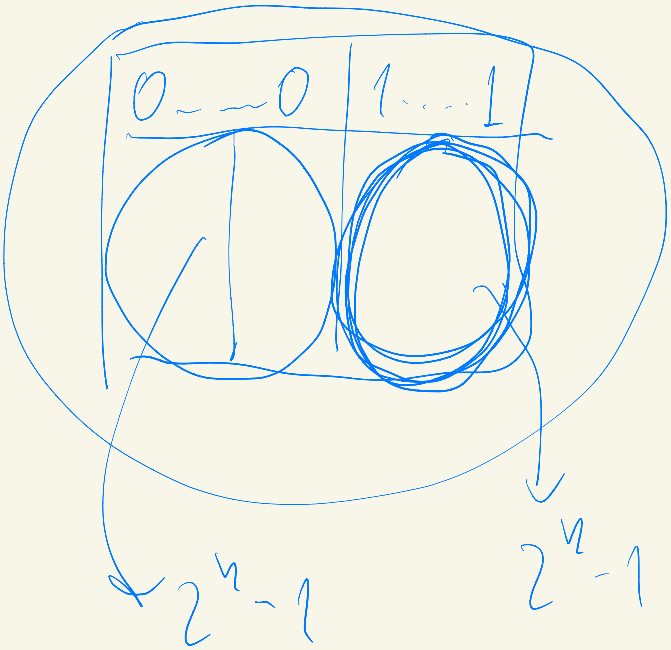
1 $\quad$ 6 +

2 $\quad$ 6 +

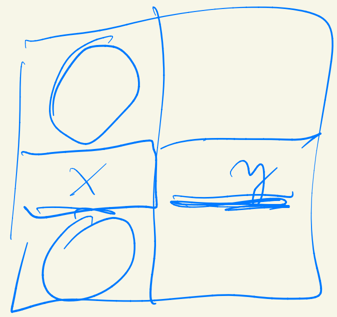
3 $\quad$ 6 +

4 $\quad$ 6 +

24



$(2^n - 1)!$



$$Pr\left(\pi(0\ldots0) = 1\ldots1\right) = \frac{(2^n-1)!}{(2^n)!} = \frac{1}{2^n}$$

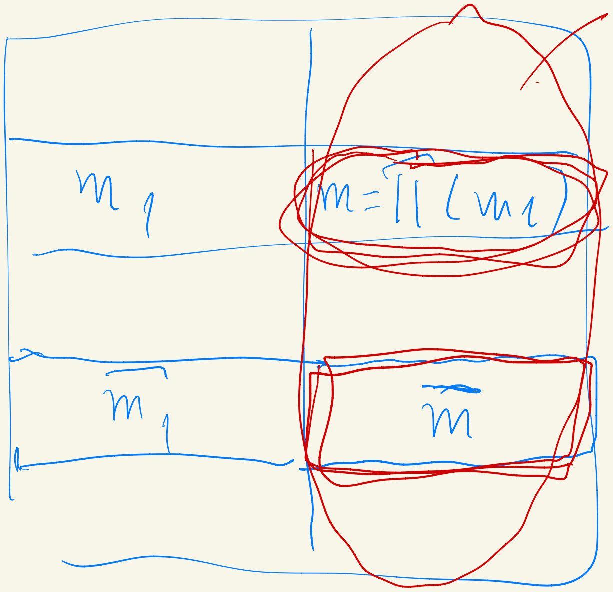
$$m_1 \to \overline{\Pi(m_1)}$$

$$\overline{m}_1 \to \overline{\Pi(\overline{m}_1)}$$

$$\Pr\left(\overline{\Pi(m_1)} \text{ XOR } \overline{\Pi(\overline{m}_1)} = 1 \ldots 1\right)$$

$$m = \overline{\Pi(m_1)}$$

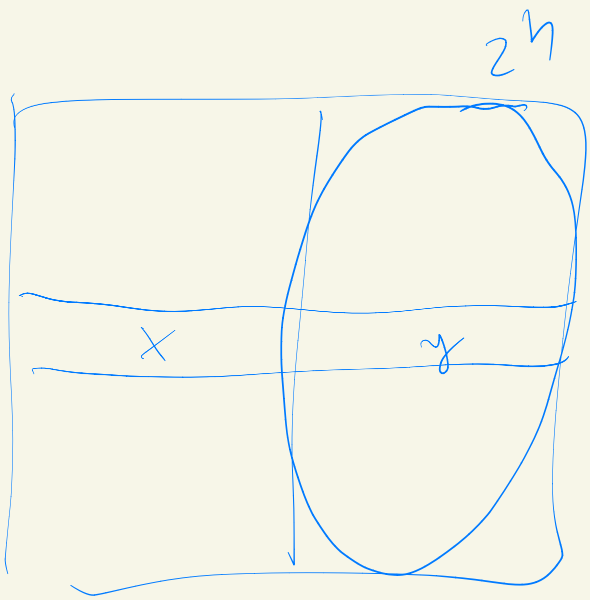
$$\Pr\left(\overline{\Pi(\overline{m}_1)} = \overline{m}\right) = \frac{1}{2^n - 1}$$



$\boxed{2^n - 1}$

$$\frac{(2^n-2)!}{(2^n-1)!}$$

$$\frac{1}{2^n-1}$$



m_1	$m = \Pi(m_1)$
$\bar{m}_1$	$\bar{m}$

$2^n - 1$

$$\frac{1}{2^n - 1}$$

OTP

V:

$b=0 \rightarrow k \in K \qquad f(x) = Enc(k, x)$

$b=1 \rightarrow \Pi \qquad f(x) = \Pi(x)$

A:

$m_1 \rightarrow f(m_1)$

$\overline{m_1} \rightarrow f(\overline{m_1})$

$m_1 \text{ XOR } \overline{m_1}$ $\rightarrow 1 \ldots 1 \Rightarrow b=0$

$\rightarrow \neq 1 \ldots 1 \Rightarrow b=1$

$Pr(\Pi(m_1) \text{ XOR } \Pi(\overline{m_1}) = 1 \ldots 1)$

$= 1/(2^n - 1)$

$\Pr(\text{adversarie game}) =$

$\Pr(\text{adversarie game} \mid b=0) \cdot \Pr(b=0) + \Pr(\text{adversarie game} \mid b=1) \cdot \Pr(b=1)$

$\Pr(\text{adversarie game} \mid b=0) \to 1$, $\Pr(b=0) = 1/2$

$\Pr(\text{adversarie game} \mid b=1) \to \left(1 - \frac{1}{2^n - 1}\right)$, $\Pr(b=1) = 1/2$

$$= \frac{1}{2} + \frac{1}{2} \cdot \left(1 - \frac{1}{2^n - 1}\right)$$

$n = 128$