PSEUDORANDOM FUNCTION

We will see PRFs are enough for doing CPA-secure SKE, but also MACs.

How to build a PRF:

- Theory: OWFs or concrete assumptions (FACTORING, DL, ...)
- Practice: AES.

What is a PRF?. It's a keyed function

DETERMINISTIC $F_K : \{0,1\}^n \to \{0,1\}^n$

$K \in \{0,1\}^\lambda$ $n = 256, 512, \dots$

Security? Basically, The output of the function should be indist. from the output of TRULY RANDOM TRUTH TABLE.

INPUT	OUTPUT
$0 \cdots 0$	y_1
$0 \cdots 1$	$y_2 \in \{0,1\}^m$
$\vdots$	$\vdots$
$1 \cdots 1$	

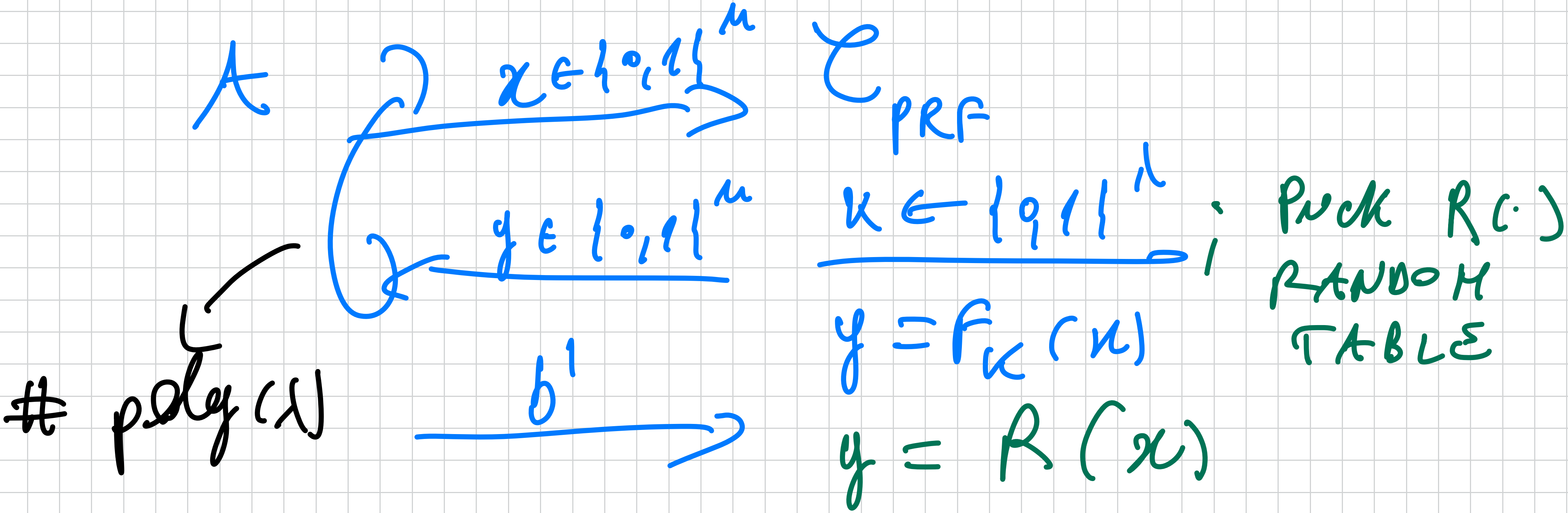
$y_1, y_2, \ldots \leftarrow \{0,1\}^m$

For RANDOM choice of $K \in \{0,1\}^\lambda$, then $F_K(\cdot)$ is COMP. IND. from RANDOM TABLE

DEF (PRF) We say that $F : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ is a PRF if:

$$\mathrm{REAL}_{A,F}(\lambda) \approx_c \mathrm{RAND}_{A,R}(\lambda)$$

$\underline{\mathrm{REAL}}_{A,F}\underline{(\lambda)}$ / $\mathrm{RAND}_{A,R}(\lambda)$


A
$x \in \{0,1\}^n$
$y \in \{0,1\}^n$
$\# \mathrm{poly}(\lambda)$
b'
$\mathcal{C}_{PRF}$
$k \leftarrow \{0,1\}^\lambda$; Pick $R(\cdot)$ RANDOM TABLE
$y = F_k(x)$
$y = R(x)$

Equivalent: $\forall$ PPT A

$$\left| \Pr[\mathrm{REAL}_{A,F}(\lambda)=1] - \Pr[\mathrm{RAND}_{A,R}(\lambda)=1 \right|$$

$$\leq \mathrm{negl}(\lambda$$

The challenger is UNBOUNDED in RAND. This is simpler to think of, but not needed as we can do LAZY SAMPLING:

- Upon $x \in \{0,1\}^n$, output $y \in \{0,1\}^n$ as long as x not called before (in which case, output previous y).

How to construct PRFs. In practice: AES (intuition and experience). Designed in early 2000, still UNBROKEN. No provable security, back then.

In theory: OWF $\Rightarrow$ PRF. Alternatively, you can use FACTORING, or DL, LWE.

Application 1: PRF $\Rightarrow$ CPA SKE for fixed input length (FIL).

Here it is: $\Pi = (\mathrm{Enc}, \mathrm{Dec})$;

- $\mathrm{Enc}(k, m)$: $r \leftarrow \{0,1\}^n$

$$c = (c_1, c_2) = (r, F_k(r) \oplus m)$$

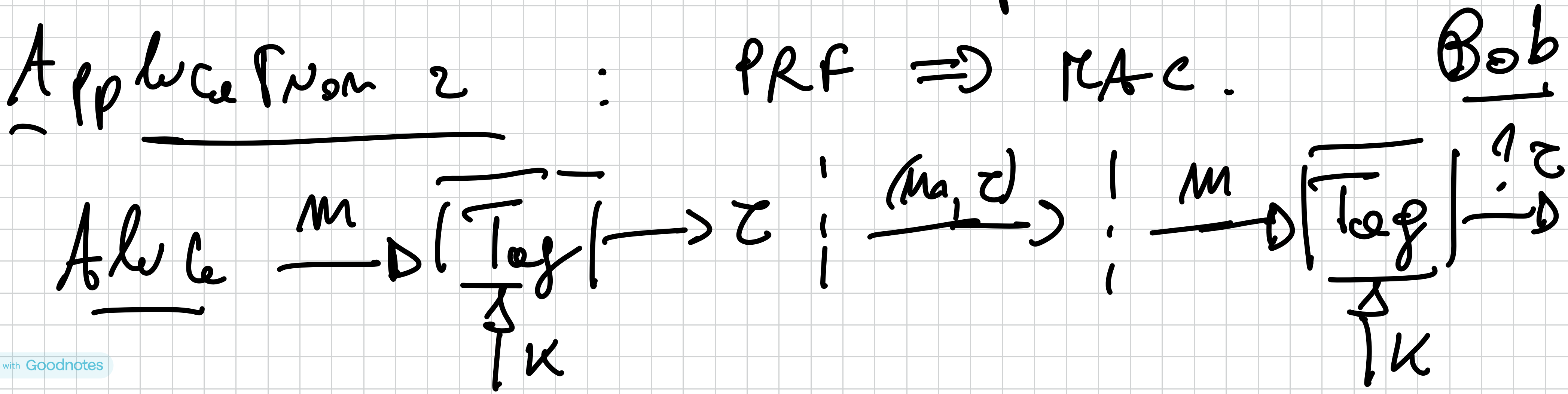
- $\mathrm{Dec}(K, (c_1, c_2))$:

$$F_K(c_1) \oplus c_2 =$$

$$= F_K(r) \oplus F_K(r) \oplus m = m \quad ✓$$

THM 1. Assuming F is a PRF, The above is CPA-secure SKE for FIL.

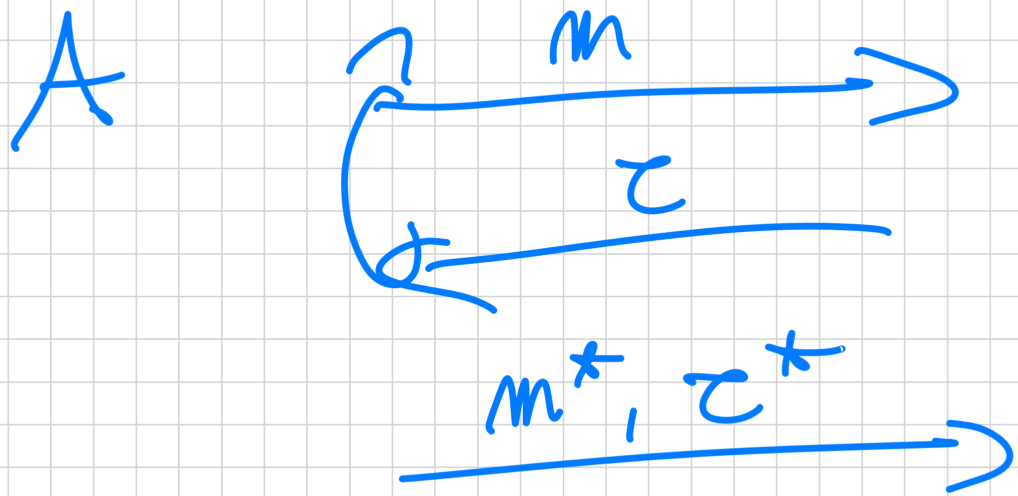
Application 2: PRF $\Rightarrow$ MAC.



Let F be a PRF; Then $\text{Tag}(K, m) = F_K(m)$.

Security? UFCMA (Universal unforgeability against chosen-message attacks)

$$\underline{\quad \text{GAME}^{\text{ufcma}}_{A,\text{Tag}}(\lambda) \quad}$$



$\mathcal{C}_{\text{ufcma}}$

$K \leftarrow \{0,1\}^\lambda$

$\tau = \text{Tag}(K, m)$

OUTPUT 1

iff $\tau^* = \text{Tag}(K, m^*)$

$m^* \notin \{m\}$