

PSEUDORANDOM FUNCTIONS

We have seen that the previous SKE is insecure when multiple msg are encrypted.

To overcome this, we introduce a new tool.

What is a PRF? It is a family of functions:

$$\mathcal{F} = \{ F_K : \{0,1\}^M \rightarrow \{0,1\}^m \}_{K \in \{0,1\}^\lambda}$$

Security? For uniform choice of $K \leftarrow \mathcal{V}_\lambda$, no efficient A can tell apart samples from $F_K(\cdot)$ from sample of a uniformly random function $R: \{0,1\}^M \rightarrow \{0,1\}^m$.

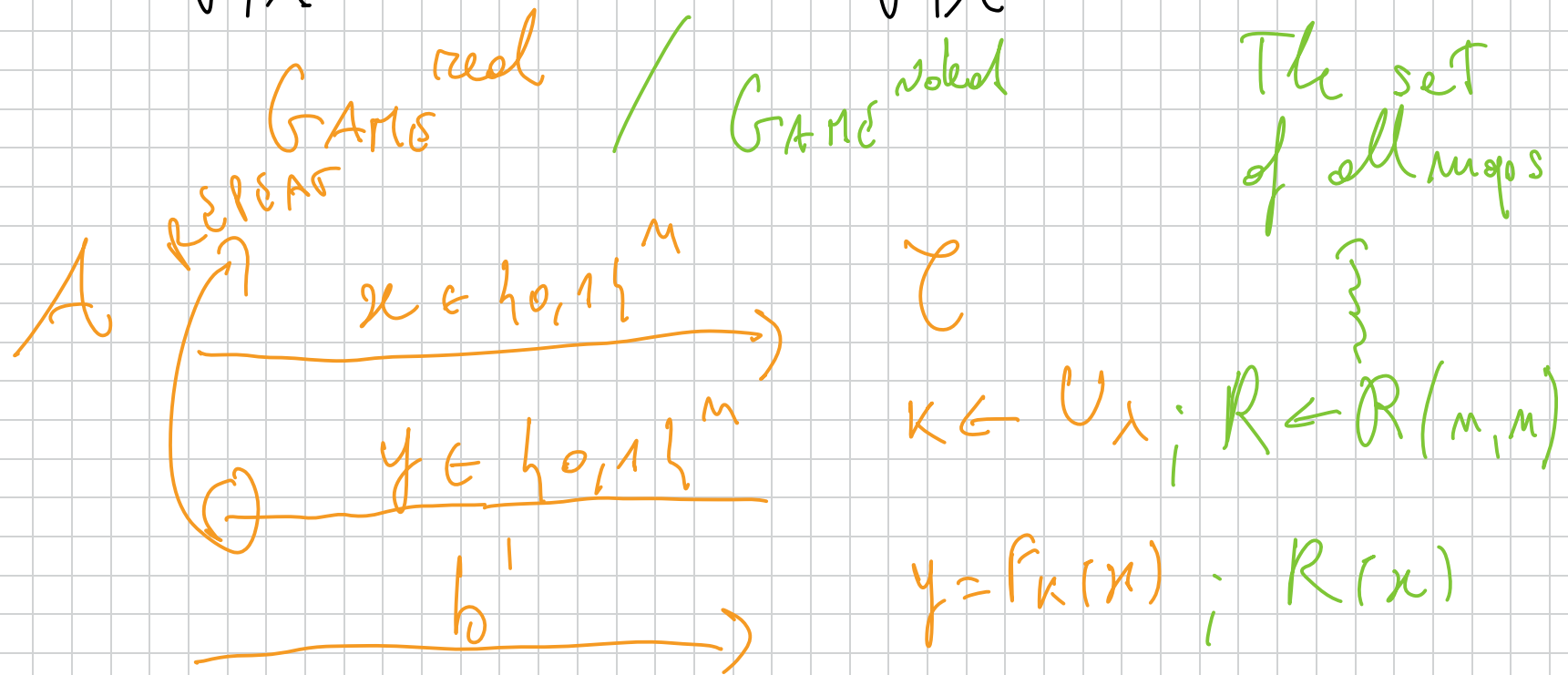
($\hookrightarrow$) R is still DETERMINISTIC
but
picked randomly among all possible

maps from $\{0,1\}^m \rightarrow \{0,1\}^m$

DEF

$\mathcal{F}$ as above is a PRF family if:

$$\text{GAME}_{\mathcal{F}, A}^{\text{real}}(\lambda) \approx_c \text{GAME}_{\mathcal{F}, A}^{\text{ideal}}(\lambda)$$



REMARK: The green game takes exp time.
(i.e., $\mathcal{T}$ is UNBOUNDED)

EXERCISE: No F is a PRF against n BOON =
DED ADVERSARIES!

How do we build PRFs?

- In practice: AES; DES; ANY BLOCKCIPHER
Nobody knows how to prove AES is a PRF.

- In theory: OWFs (not practical); or
some assumptions as public-key crypto
(factoring, discrete log, lattices)
practical and efficient (still less
efficient than AES).

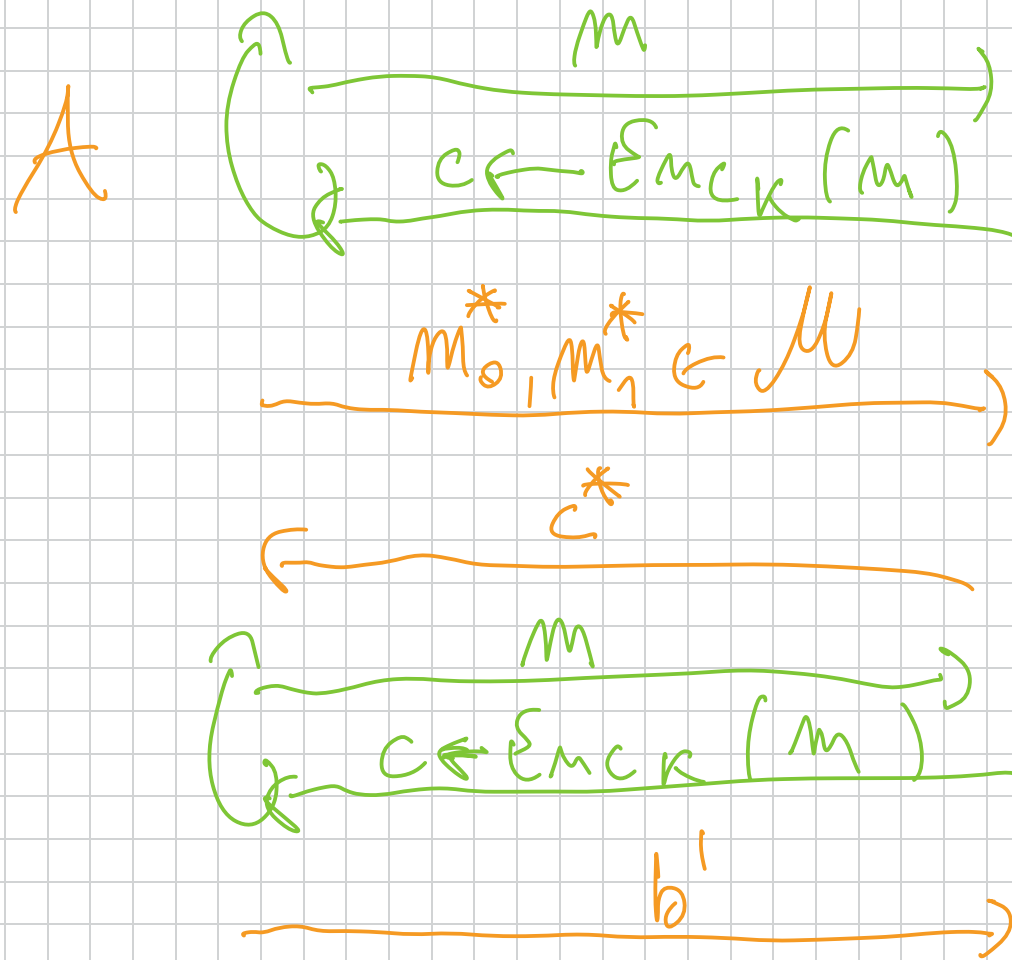
Let's first apply PRFs to broadcast protocol
SKE (one key, short, many msg).

We start by defining SKE secure for many
msg (i.e. CPA-secure SKE).

DEF. We say $\Pi = (\text{Enc}, \text{Dec})$ is CPA
secure if:

$$\text{GAME}_{\Pi, A}^{\text{cpa}}(\lambda, 0) \approx_c \text{GAME}_{\Pi, A}^{\text{cpa}}(\lambda, 1)$$

$$\underline{\text{GAME}_{\Pi, A}^{\text{cpa}}(\lambda, b \in \{0, 1\})}$$



$\mathcal{C}$
 $K \leftarrow \mathcal{K}$

$c^* \leftarrow E_{mc_K}(m_b^*)$

REMARK : $E_{mc_K}(\cdot)$ must be RANDOMIZED.

$c \leftarrow E_{mc_K}(m) \quad \equiv \quad c = E_{mc_K}(m; r)$
 $r \leftarrow \mathcal{R} \quad (\text{RANDOMIZED SPACE})$

Usually $\text{Dec}_K(\cdot)$ still deterministic.

Let's build it from ANY PRF!

$$\text{Enc}(K, m) = (c_1, c_2)$$

$$c_2 = F_K(\pi) \oplus m$$

$$\pi \leftarrow U_m$$

$$c_1 = \pi$$

$$\text{Dec}(K, (c_1, c_2)) = F_K(c_1) \oplus c_2 = m$$

THM Assuming $\mathcal{F}$ is a PRF family, Then
 The above SKE $\Pi = (\text{Enc}, \text{Dec})$ is CPA-secure.
 Proof. First, let $G(\lambda, b) \equiv \text{Gar}_{N, A}^{\text{CPA}}(\lambda, b)$.

We need to show: $G(\lambda, 0) \approx_c G(\lambda, 1)$.

Consider, $H(\lambda, b)$: The same as $G(\lambda, b)$
 except we use $R \leftarrow \mathcal{R}(n, n)$ instead of F_K .

$$\underline{G(\lambda, b) / H(\lambda, b)}$$

A

$$\begin{array}{l} \xrightarrow{m} \\ \text{Enc} \quad C = (C_1, C_2) \\ \xrightarrow{m_0^*, m_1^*} \\ \text{Dec} \quad C^* = (C_1^*, C_2^*) \end{array}$$

$\mathcal{C}$

$$K \leftarrow \mathcal{U}_A; R \leftarrow \mathcal{R}(n, n)$$

$$C_1 = \pi \leftarrow \mathcal{U}_m$$

$$C_2 = F_K(\pi) \oplus m$$

$$\begin{array}{c} \uparrow \\ \text{---} M \text{---} \rightarrow \\ \oplus \text{---} c = (c_1, c_2) \text{---} \\ \downarrow \\ \text{---} b' \text{---} \end{array}$$

$$c_1^* = \pi^* \leftarrow U_M$$

$$c_2^* = f_K(\pi^*)$$

$$\oplus M_b^*$$

$$c_1 = \pi \leftarrow U_M$$

$$c_2 = R(\pi) \oplus M$$

$$c_1^* = \pi^* \leftarrow U_M$$

$$c_2^* = R(\pi^*) \oplus M_b^*$$

LEMMA $G(\lambda, b) \approx_c H(\lambda, b)$, $\forall b \in \{0, 1\}$.

Proof. By reduction to PRF security.

A

"START"

M

$C = (C_1, C_2)$

B

$\pi \in U_M$

z

$\mathcal{C}$

$F_K(\pi)$

$R(\pi)$

$$C_1 = \pi$$

$$C_2 = z \oplus M$$

M_0^*, M_n^*

$C^* = (C_1^*, C_2^*)$

π^*

z^*

$$C_1^* = \pi^*, C_2^* = z^* \oplus M_b^*$$

$\vdots$

b^1

$\vdots$

b^1

Perfect REDUCTION.



LEMMA

$H(\lambda, 0) \approx_s H(\lambda, 1)$ so long
as the (UNBOUNDED) ATTACKER makes
at most $q(\lambda) = \text{poly}(\lambda)$ queries
 $(\Rightarrow H(\lambda, 0) \approx_c H(\lambda, 1))$

Proof. The intuition is: Assume first
no encryption queries. Then, upon
 m_0^*, m_1^* , the challenge is $r^*, R(r^*) \oplus m_b^*$
with $r^* \leftarrow U_n$. Because R is a
RANDOM table, this is the same as

$$C^* = (\pi^*, z^* \oplus m_b^*)$$

$$\pi^*, z^* \leftarrow U_n$$

However, A can make encryption queries. This could be problematic because what if A queries $m = 0^n$ and $\mathcal{E}$ picks again π^* same as in challenge. Then:

$$C = (\pi^*, R(\pi^*) \oplus 0^n)$$

But this event only happens with negligible probability.

In general, let BAD be the event that π^* collides with any of the π 's on encryption queries.

Conditional on $\overline{\text{BAD}}$ we have $H(\lambda, 0) \equiv H(\lambda, 1)$ because we can replace $R(\pi^*)$ with uniform z^* independent of everything.

On the other hand:

$$\begin{aligned} \Pr[\text{BAD}] &\leq \Pr[\exists i, j : \pi_i = \pi_j] \\ &\leq \sum_{\substack{i, j=1 \\ i \neq j}}^q \Pr[\pi_i = \pi_j]. \end{aligned}$$

$$= \sum_{i=1}^M \text{Col}(V_i)$$

$$\leq \begin{pmatrix} 9 \\ 2 \end{pmatrix} \cdot 2^{-M}$$

$$M = M(\lambda) \\ = \text{poly}(\lambda).$$

$$= \text{poly}(\lambda) \cdot \text{negl}(\lambda) = \text{negl}(\lambda).$$

One can show that the above two facts imply

$$SD(H(\lambda, 0); H(\lambda, 1)) \leq \Pr[BAD]$$

$$= \text{negl}(\lambda)$$

