MESSAGE AUTHENTICATION

$\text{Tag}: \mathcal{K} \times \mathcal{M} \to \mathcal{T}$; $\tau = \text{Tag}(k, m)$

$$\underset{k}{\text{Alice}} \xrightarrow{m,\ \tau} \underset{k}{\text{Bob}}$$

Recall: In the IT setting $|k| \geq 2|m|$ (one-time only).

Q: Can we do better assuming OWFs?

DEF (UF-CMA). We say $\text{Tag} = \Pi$ is UF-CMA if $\forall$ PPT A: $\Pr[\text{GAME}^{\text{ufcma}}_{\Pi, A}(\lambda) = 1] \leq \text{negl}(\lambda)$.

$$\mathrm{GAME}^{\mathrm{ufcma}}_{\Pi, A}(\lambda)$$

$$\begin{array}{ccc}
A & & C \\
 & \text{poly} & k \leftarrow\!\$\ \mathcal{K} \\
 & \xrightarrow{\quad m \quad} & \\
 & \xleftarrow{\quad \tau \quad} & \tau = \mathrm{Tag}(k, m). \\
 & \xrightarrow{\quad m^*, \tau^* \quad} & \text{Output } 1 \text{ iff} \\
 & & \mathrm{Tag}(k, m^*) = \tau^* \\
 & & m^* \notin \{m\}. \ (\text{FRESH } m^*)
\end{array}$$

Two cases:

- FIL ✓
- VIL

THM. Let $\mathcal{F} = \{F_k\}$ be a PRF, and $\mathrm{Tag}(k, m) = F_k(m)$. Then Tag is UF-CMA secure (as long as the output length $n = n(\lambda)$ of F_k satisfies $n(\lambda) = \omega(\log(\lambda))$.).

Proof. We start with:

$\underline{\mathrm{GAME}(\lambda)}$ & $\underline{\mathrm{HYB}(\lambda)}$

$$\mathcal{A} \quad \begin{array}{c} \xrightarrow{\quad m \quad} \\ \xleftarrow{\quad \tau \quad} \\ \xrightarrow{\quad m^*,\tau^* \quad} \end{array}$$

$k \leftarrow\$ \{0,1\}^\lambda$; $R \leftarrow\$ \mathcal{R}(\lambda, n, m)$

$\tau = F_k(m)$; $\tau = R(m)$

Output 1 if:

(i) $\tau^* = F_k(m^*)$; $\tau^* = R(m^*)$

(ii) $m^* \notin \{m\}$.

LEMMA $\mathrm{GAME}(\lambda) \approx_c \mathrm{HYB}(\lambda)$.

Proof. Standard reduction to PRF security.

LEMMA For all adversaries, $\Pr[HYB(\lambda)=1] \leq negl(\lambda)$.

Proof. To win, A needs to guess the random string $R(m^*)$ for a fresh row m^*. Because the rows are independent, even unbounded A succeeds w.p. $\leq 2^{-m(\lambda)}$. When $m(\lambda) = \omega(\log(\lambda))$, $2^{-m(\lambda)} = negl(\lambda)$. ∎

Q: What about long $m = (m_1, \dots, m_d)$ where $d \in \mathbb{N}$ and $|m_i| = n(\lambda)$.

What about VIL?

Constructions that DO NOT work:

- $\tau = \mathrm{Tag}_k\left(\bigoplus_i m_i\right)$. $\quad m \neq 0^n$

$$\underset{m_1}{m = 0^{256}} \,\|\, \underset{m_2}{0^{256}} \,\|\, \underset{m_3}{1^{256}} \qquad A, A, B$$

$$0, 0, B$$

$$\bigoplus m_i = 1^{256}$$

$$\tau = AES_k(1^{256})$$

$$m^* = (0^{255}1 \,\|\, 0^{255}1 \,\|\, 1^{256})$$

$\mathcal{A}$ $\xrightarrow{m \| m \| m'}$ $\mathcal{C}$

$\xleftarrow{\tau}$ $\quad \tau = \mathrm{Tag}_k(m \oplus m \oplus m')$

$\xrightarrow{0 \| 0 \| m', \tau}$

$$\bigoplus_i m_i = 1^{256}$$

- $\tau_i = \mathrm{Tag}_K(m_i) \quad \forall\, i = 1, \dots, d$

$m_1 \neq m_2 \qquad \tau = (\tau_1, \dots, \tau_d)$.

$m = (m_1, m_2)\ ; \quad \tau = (\tau_1, \tau_2)$

$m^* = (m_2, m_1)\ ; \quad \tau^* = (\tau_2, \tau_1)$

- $\tau_i = \mathrm{Tag}_K(i \| m_i) \quad \forall\, i = 1, \dots, d.$

$\tau_2 = \mathrm{Tag}_K(2 \| B)$

$M \quad A, B \qquad (\tau_1, \tau_2)$

$m^{*'} \quad B, C \qquad (\tau_1', \tau_2')$

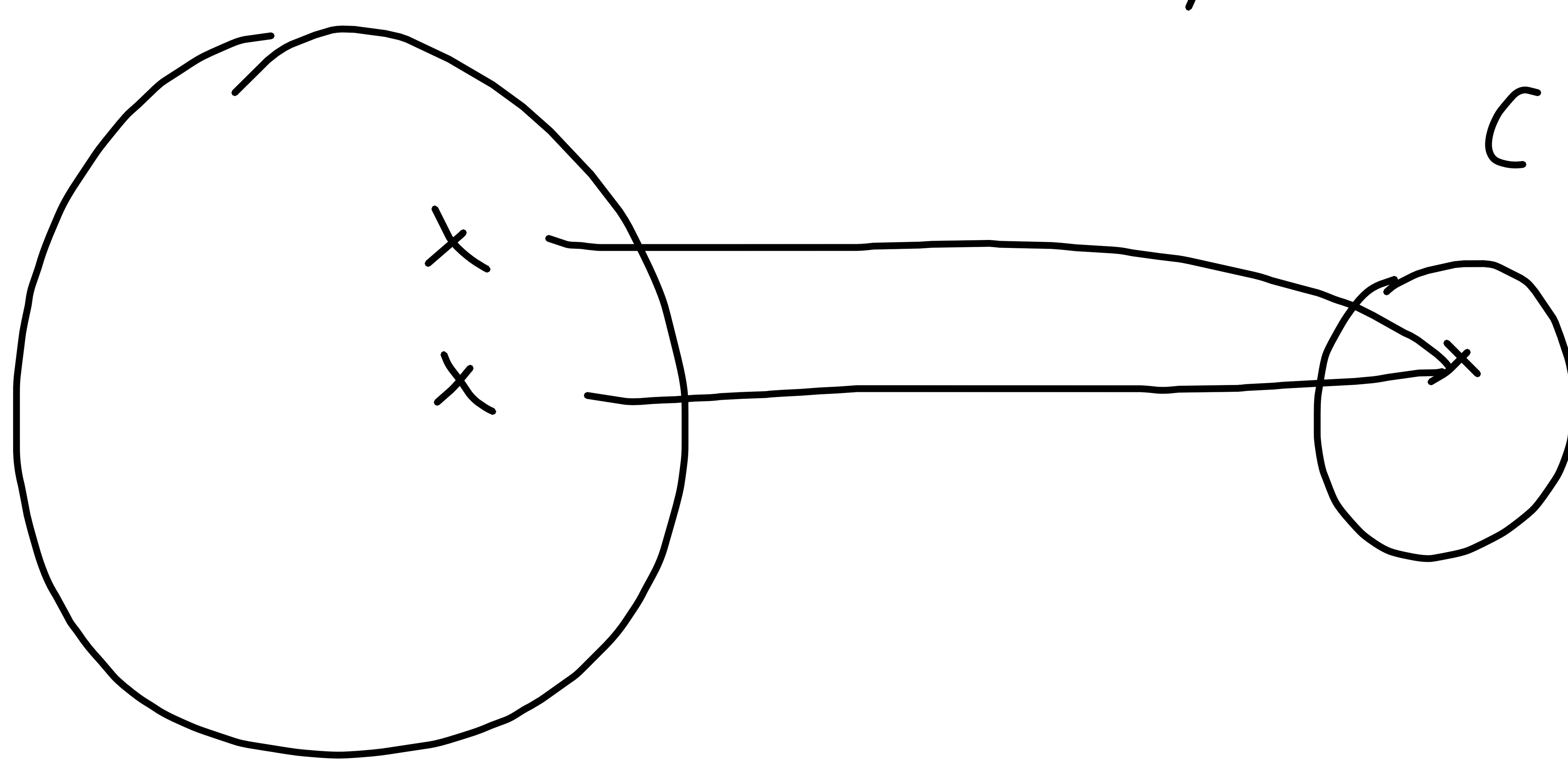
$B \| B\ ; \quad \tau_1' \| \tau_2$

$\hookrightarrow \tau_2 \overset{?}{=} \mathrm{Tag}_K(1 \| B)$

Better approach: Design some input-shrinking function $h_s : \{0,1\}^{n \cdot d} \to \{0,1\}^{n}$; $s \in \{0,1\}^{\lambda}$

$$\mathrm{Tag}_{k'}(m) = F_k(h_s(m))$$

$$k' = (k, s) \; ; \; m = (m_1, \dots, m_d)$$



COLLISION

If I can find $m^* \neq m$ s.t. $h_s(m^*) = h_s(m)$

I'm lost!

Two approaches:

- Let s be PUBLIC (COLLISION-RESISTANT HASH, i.e. SHA-3, MD-5).
- Let s be SECRET.

DEF. (ALMOST UNIVERSAL) $\mathcal{H} = \{h_s : \{0,1\}^N \to \{0,1\}^n\}_{s \in \{0,1\}^\lambda}$ is ε-AU if: $\forall x, x' \in \{0,1\}^N$ s.t. $x' \neq x$

$$\Pr_{s \leftarrow\$ \{0,1\}^\lambda}\left[h_s(x) = h_s(x') \right] \leq \varepsilon(\lambda)$$

THM * Let $\mathcal{F}$ be a PRF and $\mathcal{H}$ be AU.

Then $\mathcal{F}' = \mathcal{F}(\mathcal{H}) = \{ F'_{k'} : \{0,1\}^N \to \{0,1\}^n \}$

$$F'_{k'}(x) = F_k(h_s(x)) \qquad k' = (k, s)$$

is a PRF.

COR. $Tag_{k'}(m) = F'_{k'}(m)$ is UF-CMA for msg length $N(\lambda)$.

Proof. First use PRF security to switch $F_k(\cdot)$ with $R(\cdot)$.

$\mathrm{GAME}^{prf}_{F',\mathcal{A}}(\lambda,0)$

$\mathcal{A} \qquad\qquad\qquad\qquad \mathcal{C}$

$\xrightarrow{x \in \{0,1\}^N}$ $\qquad k \leftarrow\$ \{0,1\}^\lambda; \; s \leftarrow\$ \{0,1\}^\lambda$

$\xleftarrow{\;y\;}$ $\qquad y = F_k(h_s(x)) = F'_{k'}(x)$

$\xrightarrow{\;b'\;}$

$\approx_c$

↪ By PRF security.

$\mathrm{HYB}(\lambda)$

$\mathcal{A} \qquad\qquad\qquad\qquad \mathcal{C}$ $\qquad R \leftarrow\$ \mathcal{R}(\lambda, n, m); \; s \leftarrow\$ \{0,1\}^\lambda$

$\xrightarrow{\;x\;}$

$\xleftarrow{\;y\;}$ $\qquad y = R(h_s(x))$

$\mathrm{GAME}^{prf}_{F',\mathcal{A}}(\lambda,1)$

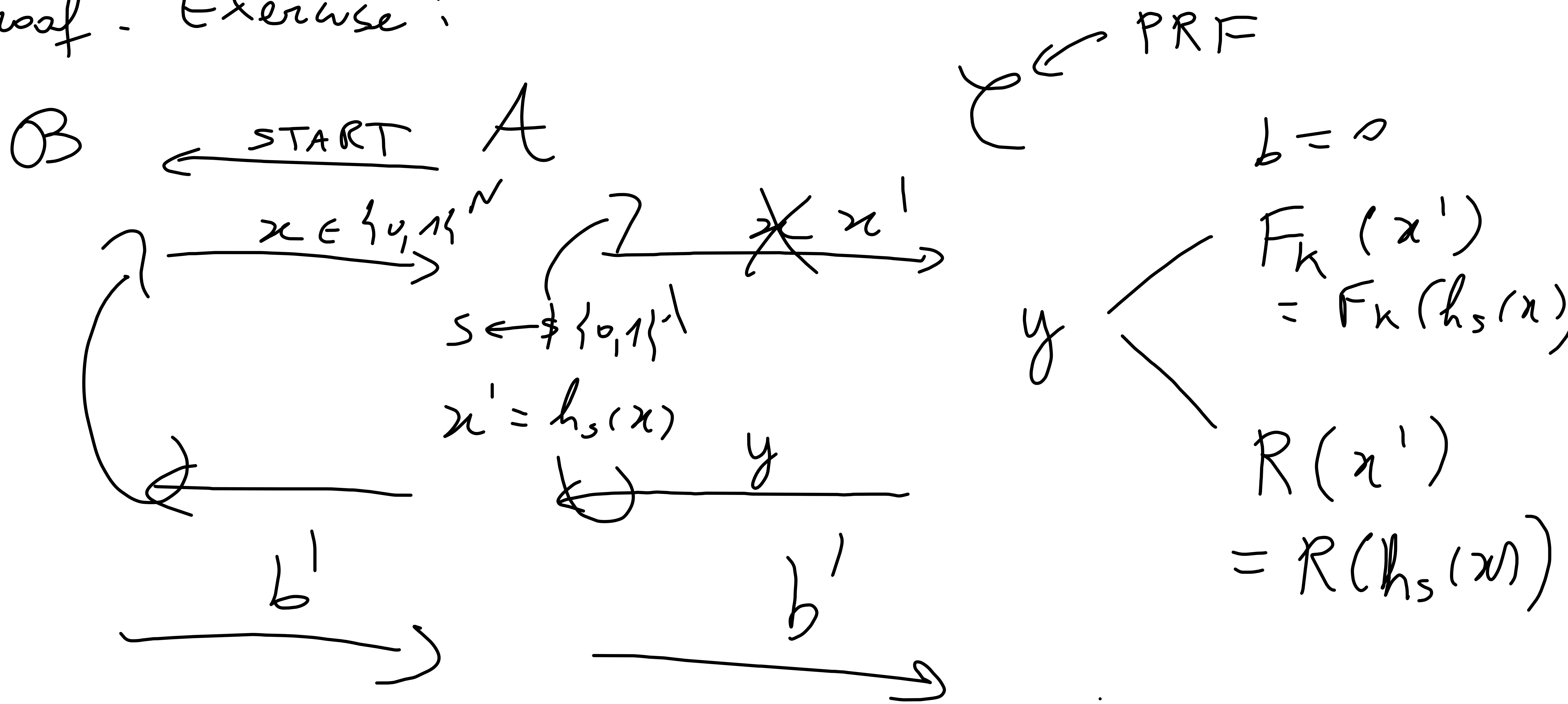
$\mathcal{A} \qquad\qquad\qquad\qquad \mathcal{C}$ $\qquad R' \leftarrow\$ \mathcal{R}(\lambda, N, m)$

$\xrightarrow{\;x\;}$

$\xleftarrow{\;y\;}$ $\qquad y = R'(x)$

LEMMA. $\mathrm{GAME}(\lambda, 0) \approx_c \mathrm{HYB}(\lambda)$.

Proof. Exercise:



LEMMA $HYB(\lambda) \approx_s GAME(\lambda, 1)$.

$\hookrightarrow$ but only $q = poly(\lambda)$ queries.

Proof. Use almost universal property of $\mathcal{H}$.

Let BAD be the event that for some $i, j \in [q]$

$h_s(x_i) = h_s(x_j)$ $\quad x_i \neq x_j$, $i \neq j$.

If $\overline{\text{BAD}}$, then $GAME(\lambda,1) \equiv HYB(\lambda)$ because we look up the table R in q distinct rows.

By the fundamental lemma of game playing we just need to prove $\Pr[\text{BAD}] \leq \text{negl}(\lambda)$. Consider modified experiment where we answer all the q queries $x_1, \ldots, x_q$ randomly. At the end we sample $s \leftarrow \$ \{0,1\}^\lambda$ and check if BAD happened. This does not change the $\Pr[\text{BAD}]$, because until BAD does not happen A only sees random values.

By AU:

$$\Pr[\text{BAD}] \leq \sum_{i,i} \Pr_s[h_s(x_i) = h_s(x_i)]$$

$$\leq q^2 \cdot \underline{\varepsilon(\lambda)} = negl(\lambda). \quad \square$$