-) $m^* \neq \{m\}$?

THM If $F = \{F_k\}$ is a PRF, then

$\text{Tag}(k, m) = F_k(m)$ is UF-CMA

(for $F(L)$).

Proof. Let $\text{GAME}^{\text{uf-cma}}_{\Pi, A}(\lambda) \equiv G(\lambda)$

and $H(\lambda)$ is the same but replace

$F_k(\cdot)$ with $R \leftarrow R(\lambda, n \to n)$.

Standard reduction to PRF security

proves $G(1^\lambda) \overset{c}{\approx} H(1^\lambda)$.

It remains to prove: $\forall$ PPT A,

$$\Pr[\underbrace{A \text{ wins on } H(1^\lambda)}_{H(1^\lambda) = 1}] \leq \text{negl}(\lambda).$$

Indeed, this $>$ prob. $\geq 2^{-n}$ for even unbounded t. ∎

The question now is: How about longer messages? How about V12?

Warm-up examples: Let $m = m_1, \dots, m_d$

- $\tau_i = \mathrm{Tog}(K, m_i)$, $\forall i \in [d]$

$$\tau = (\tau_1, \dots, \tau_d).$$

Doesn't work! Attacker can mix and match: Tog forces $m_1 \parallel m_2$ then $m_3 \parallel m_4$, forge $\tau_1 \parallel \tau_4$ on $m_1 \parallel m_4$.

- $\tau = \mathrm{Tog}(K, \bigoplus_{i=1}^{d} m_i)$

Not secure: Here is an attack. For instance query $m \| m$ for any $m \in \{0,1\}^n$; this gives $\tau = T_{eq}(K, O^n)$.

Now output: $m' \| m' = m^*$

$\tau^* = \tau$.

$m' \neq m$.

Idea: Let $\mathcal{H} = \{h_s : \{0,1\}^{mod} \to \{0,1\}^n\}_{s \in \{0,1\}^\lambda}$

Then, let $Tag(K, m) = F_K(h_s(m))$.

What property of $\mathcal{H}$ is enough ??

Clearly, it should be hard to find m, m' s.t. $m \neq m'$ and

$$h_s(m) = h_s(m')$$

A COLLISION.

DEF (AU) $\mathcal{H}$ is ε-ALMOST UNIVERSAL if $\forall\, m, m'$ s.t. $m \neq m'$

$$\Pr_s\left[h_s(m) = h_s(m') \right] \leq \varepsilon$$

$\varepsilon = 2^{-n}$ is called PERFECTLY UNIVERSAL

$\varepsilon = \text{negl}(|s|)$ is AU.

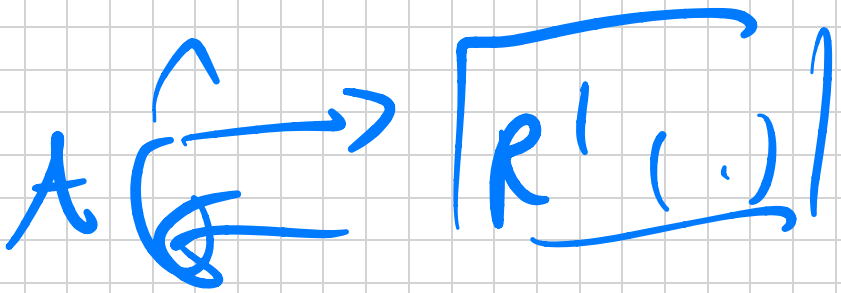
THM If F is a PRF and H is AU, then $F(H)$ is a PRF.

$$\hookrightarrow \{ F_K(h_s(\cdot)) \}$$

Proof. We consider a few experiments:

$A \longleftrightarrow \boxed{F_K(h_s(\cdot))}$ $\quad H_0(\lambda)$

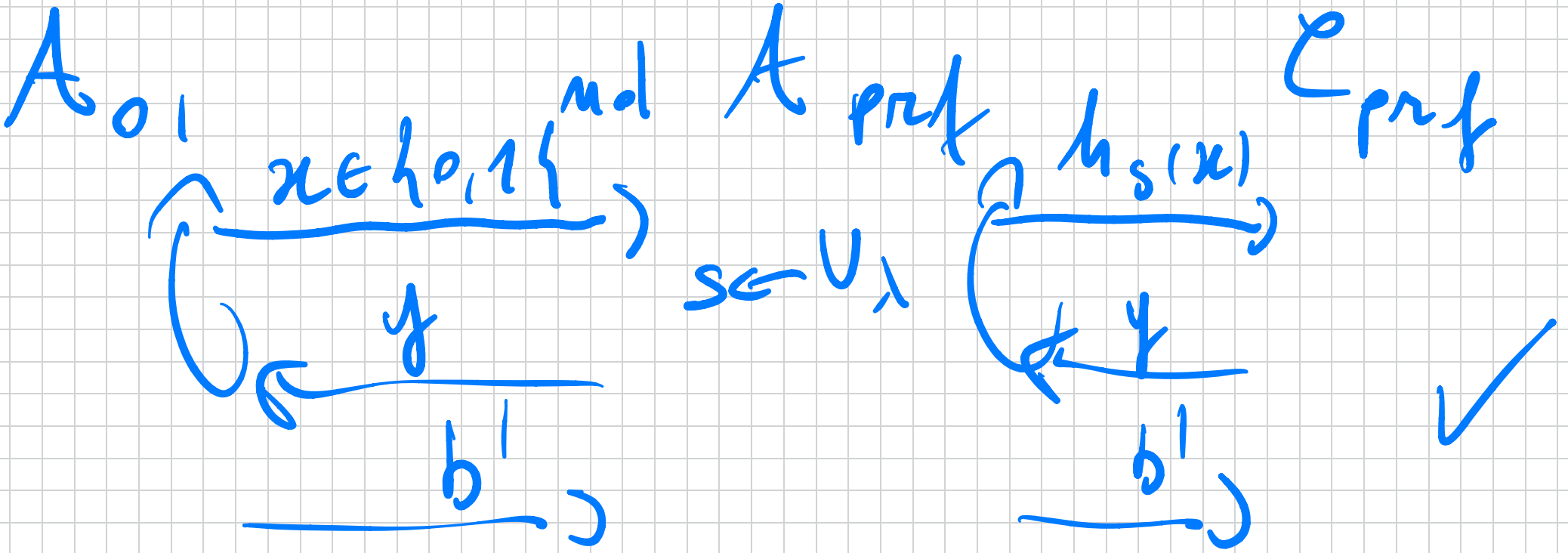
$A \longleftrightarrow \boxed{R(h_s(\cdot))}$ $\quad H_1(\lambda)$ $\quad R \leftarrow \mathcal{R}(\lambda, n \to n)$



$H_2(\lambda)$

$R^1 \leftarrow R(\lambda, md \to m)$.

Standard reduction: $H_0(\lambda) \overset{\sim}{\leftarrow}_e H_1(\lambda)$.



It remains to show: $H_1(\lambda) \approx_c H_2(\lambda)$.
We actually show they are $\approx_s$
so long as # queries $= q(\lambda) = \text{poly}(\lambda)$.
Let BAD: the event that becomes
true if $\exists\ v, i$ among $x_1, \ldots, x_q$
s.t. $v \neq i$ and $h_s(x_v) = h_s(x_i)$
Conditioning on $\overline{\text{BAD}}$, $H_1(\lambda) \equiv H_2(\lambda)$.
So, $SD(H_1; H_2) \leq Pr[\text{BAD}]$.
Subtlety! We first sample s and

then answer the queries. Whereas AU requires to fix s for the queries and then sample s.

Redefine BAD: Upon input x from A reply with U_m. At the end sample s and check if $\exists x_i$ s.t. $h_s(x_i) = h_s(x)$. Nothing changed: until BAD happens the two are identical. After

we don't care.

$$\Pr[B \wedge \bar{D}] = \Pr_s[\exists x_N, x_i, \text{ s.t. } h_s(x_N) = h_s(x_i)]$$

$$\leq \sum_{N, N \neq i} \underbrace{\Pr_s[h_s(x_N) = h_s(x_i)]}_{\Delta U}$$

$$\leq \binom{q}{2} \cdot \varepsilon = \text{negl}(\lambda). \quad \blacksquare$$

It's easy to construct AU families.
Two examples:

1) $\mathbb{F} = GF(2^n)$; $m = m_1, \dots, m_d$

$m_\nu \in GF(2^n)$

$s = (s_1 \dots, s_d) \in (GF(2^n))^d$

$$h_s(m) = \sum_{\nu=1}^{d} s_\nu \cdot m_\nu$$

$$= \langle \vec{s}, \vec{m} \rangle$$

Teil k $\quad m = (m_1, \dots, m_d)$

$m' = (m_1', \dots, m_d')$ $\qquad \delta_i := m_i' - m_i$

$m \neq m'$

$h_S(m) = h_S(m')$ (wlg. seq $s_1 \neq 0$.)

$$\iff \sum_{i=1}^{d} s_i m_i = \sum_{i=1}^{d} s_i m_i'$$

$$\iff s_1 \delta_1 = - \sum_{i=2}^{d} s_i \delta_i$$

$$\iff s_1 = \left(- \sum_{i=2}^{d} s_i \delta_i \right) / \delta_1$$

$$\Rightarrow \quad \varepsilon \leq 2^{-m} .$$

2) $IF = GF(2^m)$; $s \in IF$

$$h_s(m) = h_s(m_1, \dots, m_l) = \sum_{\nu=1}^{l} m_\nu \cdot s^{\nu-1} = q_m(s)$$

$$h_s(m) = h_s(m')$$

$$\Leftrightarrow \quad q_m(s) = q_{m'}(s)$$

$$\Leftrightarrow \quad q_{m-m'}(s) = 0$$

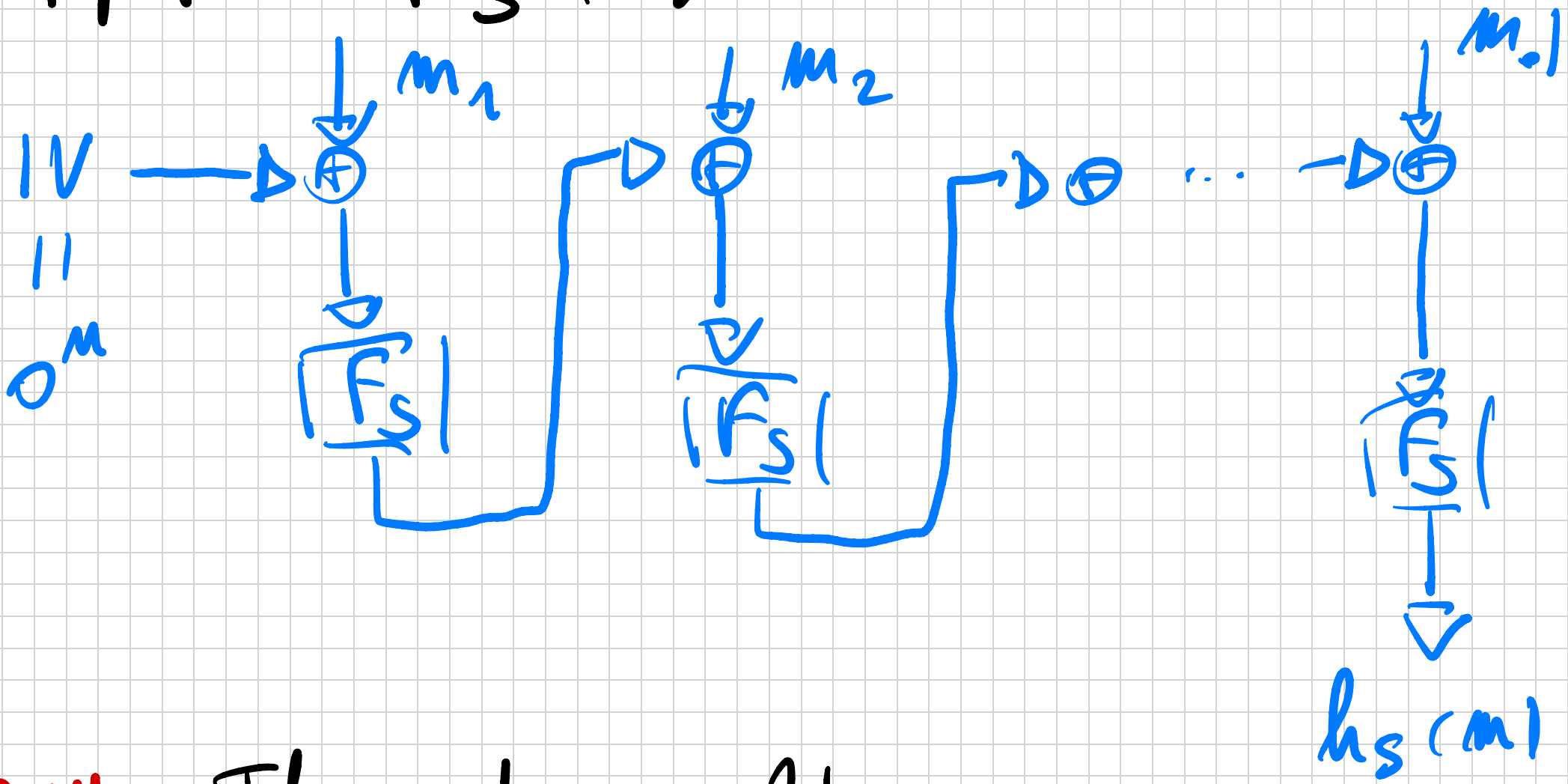
$$\Leftrightarrow \quad \sum_{\nu=1}^{d} (m_\nu - m'_\nu)\, s^{\nu-1} = 0$$

$$\Rightarrow \quad \varepsilon = (d-1)/|F| \approx d/2^n$$

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

CBC-MAC. It's just a different choice of h_s, using "error"

PRF $F_S(\cdot)$



THM The above H_{CBC} VS computationally AU essentially VS a PRF.