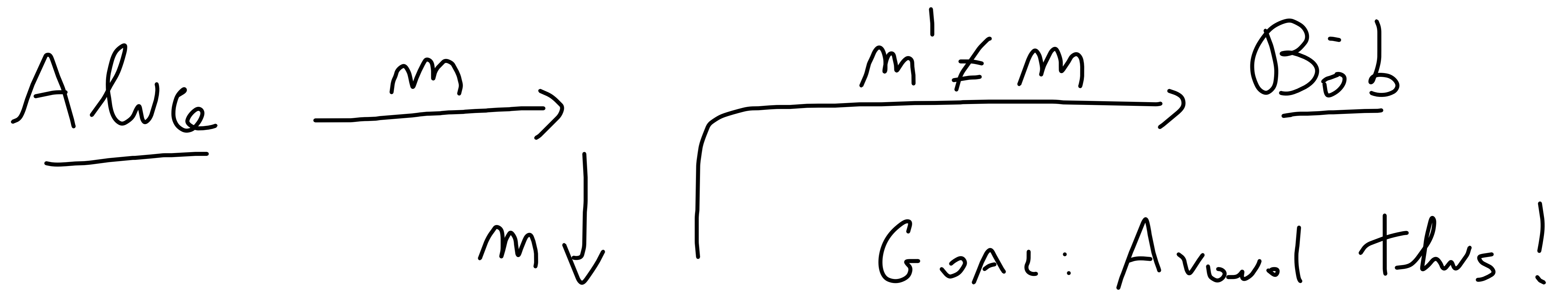
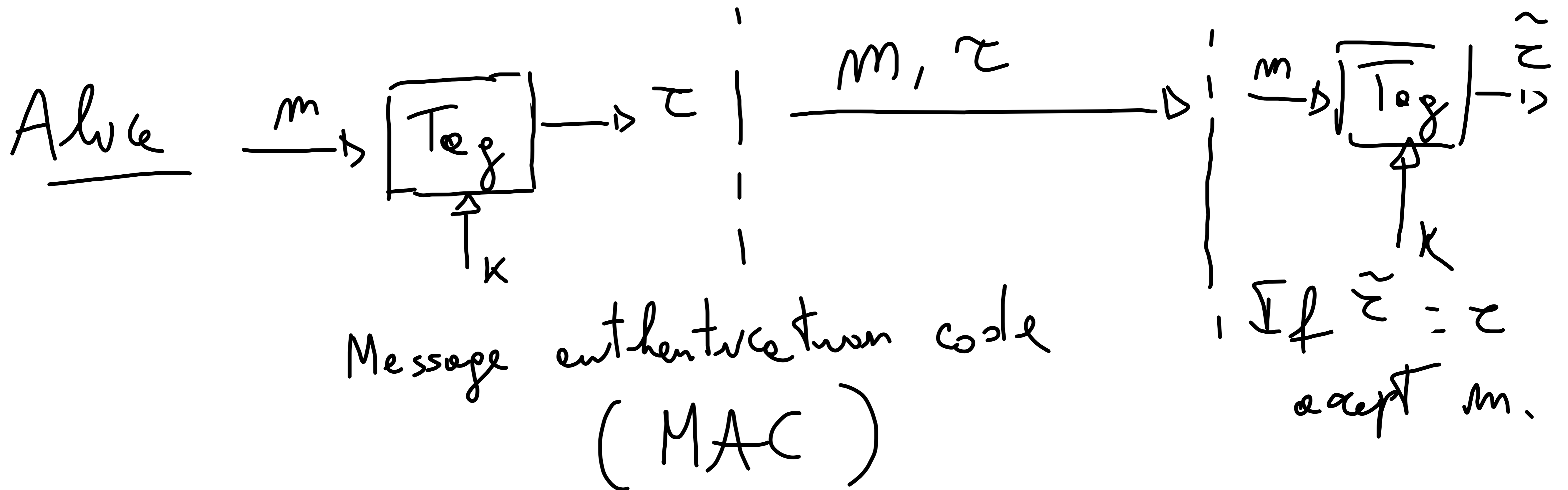


# MESSAGE AUTHENTICATION



Note:  $m$  is public



Syntax:

- $K$  Key space:  $x \leftarrow K$  (UNIFORM over  $K$ )
- Tag:  $\mathcal{M} \times K \rightarrow \Sigma$  (deterministic!)

CORRECTNESS:  $\forall k \in K, \forall m \in \mathcal{M}$  it always works!  
( $\hookrightarrow$  TRIVIAL)

SECURITY: Intuition, no  $A$  adversary can forge  
a tag  $\tau'$  on  $m' \neq m$  without the key  $k$ .  
(UNFORGEABILITY)

DEF (IT MAC)  $\Pi = \text{Tag}$  has  $\epsilon$ -statistical security if  $\forall m, m' \in \mathcal{M}$  s.t.  $m' \neq m \ \forall z, z' \in \mathcal{Z}$ :

$$\Pr_k \left[ \text{Tag}(k, m') = z' \mid \text{Tag}(k, m) = z \right] \leq \epsilon$$

EXERCISE. Is it possible to get  $\epsilon = 0$ ?

$$\epsilon = 2^{-80}, 2^{-256}, \dots$$

Note: Def. of security only ONE-TIME.

Construction: Based on a family of PAIRWISE INDEPENDENT hash functions.

DEF. A family  $\mathcal{H} = \{h_k : \mathcal{M} \rightarrow \mathcal{Z}\}_{k \in \mathcal{K}}$  is called PAIRWISE INDEPENDENT if  $\forall m, m' \in \mathcal{M}$  s.t.  $m \neq m'$  it holds that  $(h_k(m), h_k(m'))$  is UNIFORM over  $\mathcal{Z}^2$  for random  $k \leftarrow \mathcal{K}$ .

||  
 $\mathcal{Z} \times \mathcal{Z}$

THM. Let  $\Pi = \text{Tag}$  where  $\text{Tag}(k, m) = h_k(m)$  for  $h_k \in \mathcal{H}$  a PI hash family. Then  $\Pi$  has  $\epsilon$ -stat. security for  $\epsilon = 1/|\mathcal{Z}|$ .

Proof. By P1  $\forall m \in \mathcal{M}, z \in \mathcal{Z}$ :

$$P_{\kappa} [ \text{Tag}(k, m) = z ] = P_{\kappa} [ h_{\kappa}(m) = z ]$$

Moreover,  $\forall m, m' \in \mathcal{M}, m \neq m', \forall z, z' \in \mathcal{Z}$ :

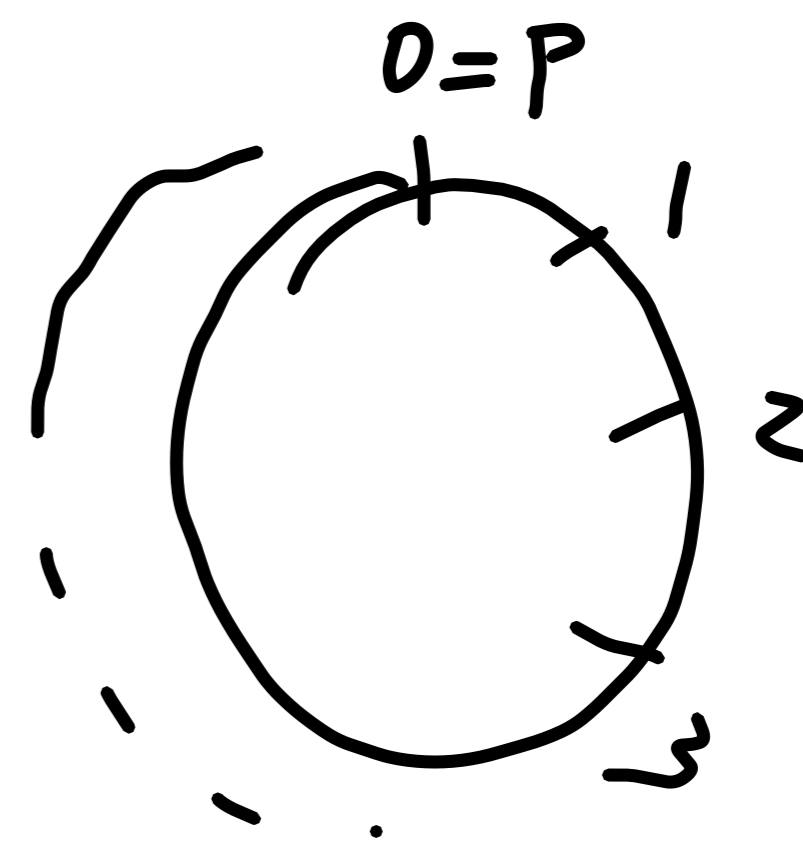
$$\begin{aligned} & P_{\kappa} [ \text{Tag}(k, m) = z \wedge \text{Tag}(k, m') = z' ] \quad (\text{P1}) \\ &= P_{\kappa} [ h_{\kappa}(m) = z \wedge h_{\kappa}(m') = z' ] = 1/|\mathcal{Z}|^2 \\ &\Rightarrow P_{\kappa} [ \text{Tag}(k, m') = z' \mid \text{Tag}(k, m) = z ] = \frac{1/|\mathcal{Z}|^2}{1/|\mathcal{Z}|} = \frac{1}{|\mathcal{Z}|} \end{aligned}$$

Now, construct  $\mathcal{H}$ . Let  $p$  a prime

$$h_{a,b}(m) = a \cdot m + b \pmod{p}$$

$$(a,b) = 1 \in \mathbb{Z}_p^2; \quad \mathcal{M} = \mathcal{Z} = \mathbb{Z}_p$$

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$$



LEMMA

Above,  $\mathcal{H}$  is PL.

Proof.  $\forall m, m' \in \mathbb{Z}_p, m \neq m', \forall z, z' \in \mathbb{Z}_p$

$$\mathcal{P}_{(a,b)} \left[ h_{a,b}(m) = z \wedge h_{a,b}(m') = z' \right]$$

$$= \prod_{a,b} \left[ a \cdot m + b = z \pmod{p} \wedge a \cdot m' + b = z' \pmod{p} \right]$$

$$= \prod_{a,b} \left[ \begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} z \\ z' \end{pmatrix} \pmod{p} \right]$$

$$= \prod_{a,b} \left[ \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} z \\ z' \end{pmatrix} \pmod{p} \right]$$

$$= \prod_{a,b} \left[ \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} z \\ z' \end{pmatrix} \pmod{p} \right] \quad \begin{array}{l} \hookrightarrow \text{Inverse exists as } m \neq m' \\ \text{for some constant } z, z'. \end{array}$$

$$= 1/p^2 \quad \square$$

Limitations:

- Def. only ONE-TIME (can be extended to  $t$ -TIME)
- Key length in actual construction ( $\mathbb{Z}_p^2$ )  
vs twice msg length ( $\mathbb{Z}_p$ ) -

THM Any  $t$ -TIME  $2^{-\lambda}$ -secure MAC has a  
Key of size  $(t+1) \cdot \lambda$  -



# RANDOMNESS EXTRACTION

We'll see: Randomness ESSENTIAL to crypto.

How to generate randomness??

Randomness comes from nature: physical phenomena.

Extract perfect randomness is very costly; it's ok if you are happy with some bits.

Maybe, we only have IMPERFECT randomness and want to purify it. Can we expend it?

Motivation example: VON NEUMANN EXTRACTOR:

Given a biased coin  $C$  s.t.  $\Pr[C=0]=p$

$\Pr[C=1]=1-p$  ;  $p \neq 1/2$ .

How to make it UNBIASED?

- Sample  $c_1 \leftarrow C$  ;  $c_2 \leftarrow C$

- If  $c_1 = c_2$   
Sample again;

- If  $c_1 = 0, c_2 = 1$  output 1

If  $c_1 = 1, c_2 = 0$  output 0

$$\Pr[C_1=0 \wedge C_2=1] = p(1-p)$$

$$\Pr[C_1=1 \wedge C_2=0] = p(1-p)$$

$$\Pr[\text{FAIL after } n \text{ turns}] = (1 - 2p(1-p))^n$$

In general, we have a source  $X$  and want  
(RV)

To design EXT s.t.  $\text{Ext}(X)$  UNIFORM.

Impossible! Question was bogus, what if

$$P_{\mathcal{X}}[X = 0] = 1$$

Then,  $X$  must be "UNPREDICTABLE"

DEF (MIN-ENTROPY) The MIN-ENTROPY of  $\mathcal{X}$  is

$$H_{\infty}(X) = -\log \max_x P_{\mathcal{X}}[X = x].$$

Examples:  $X$  constant

$$H_{\infty}(X) = -\log 1 = 0.$$

$X \equiv V_m$  uniform over  $\{0,1\}^m$

$$H_{\infty}(V_m) = \underset{\text{such}}{-\log 2^{-m}} = m.$$

Hope: Design Ext  $\gamma$  that Ext( $\mathcal{X}$ ) UNIFORM

$\forall X$  s.t.  $H_{\infty}(X) \geq k$ ;

$X \in \{0,1\}^m$  and  $0 < k < m$

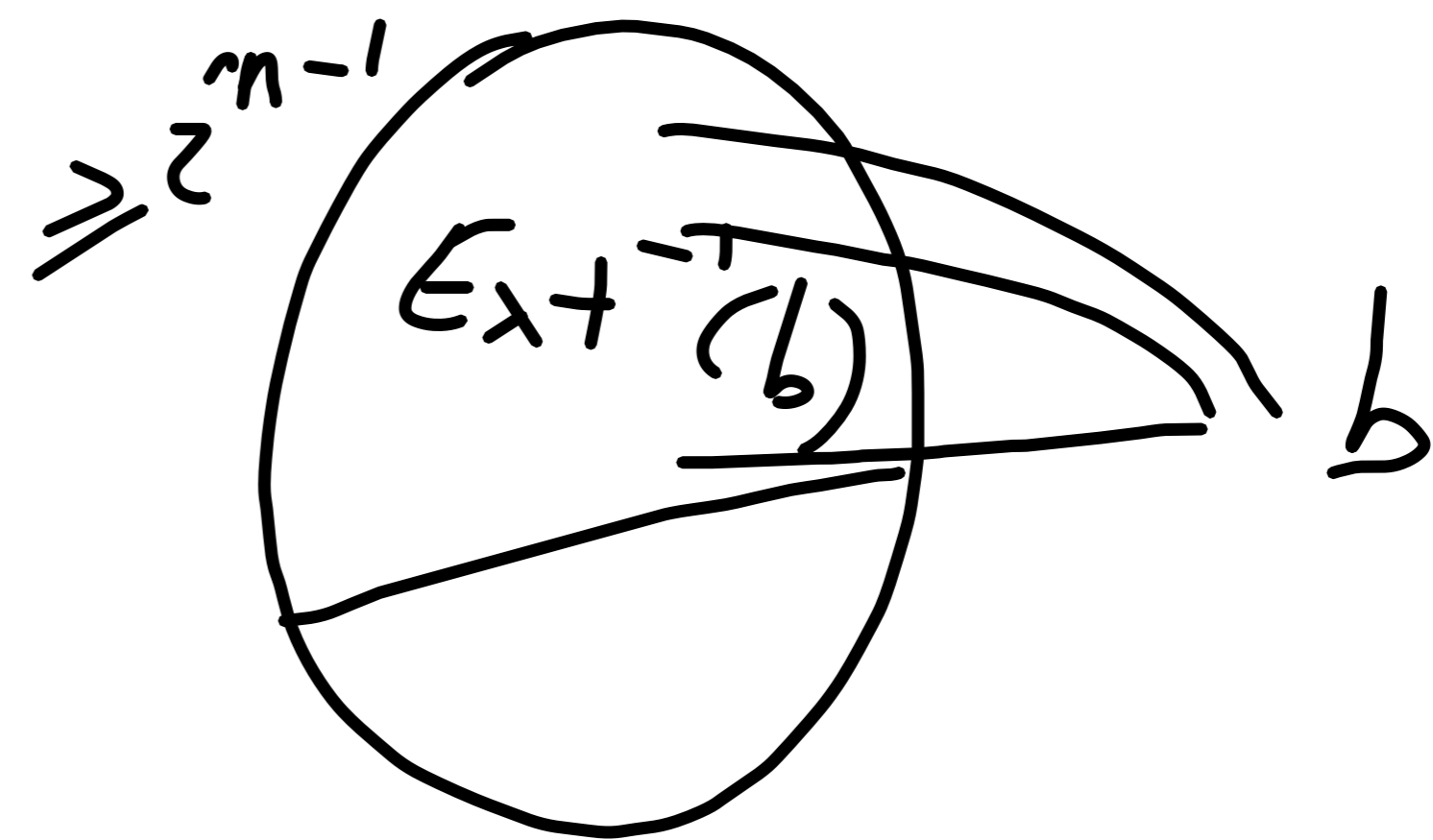
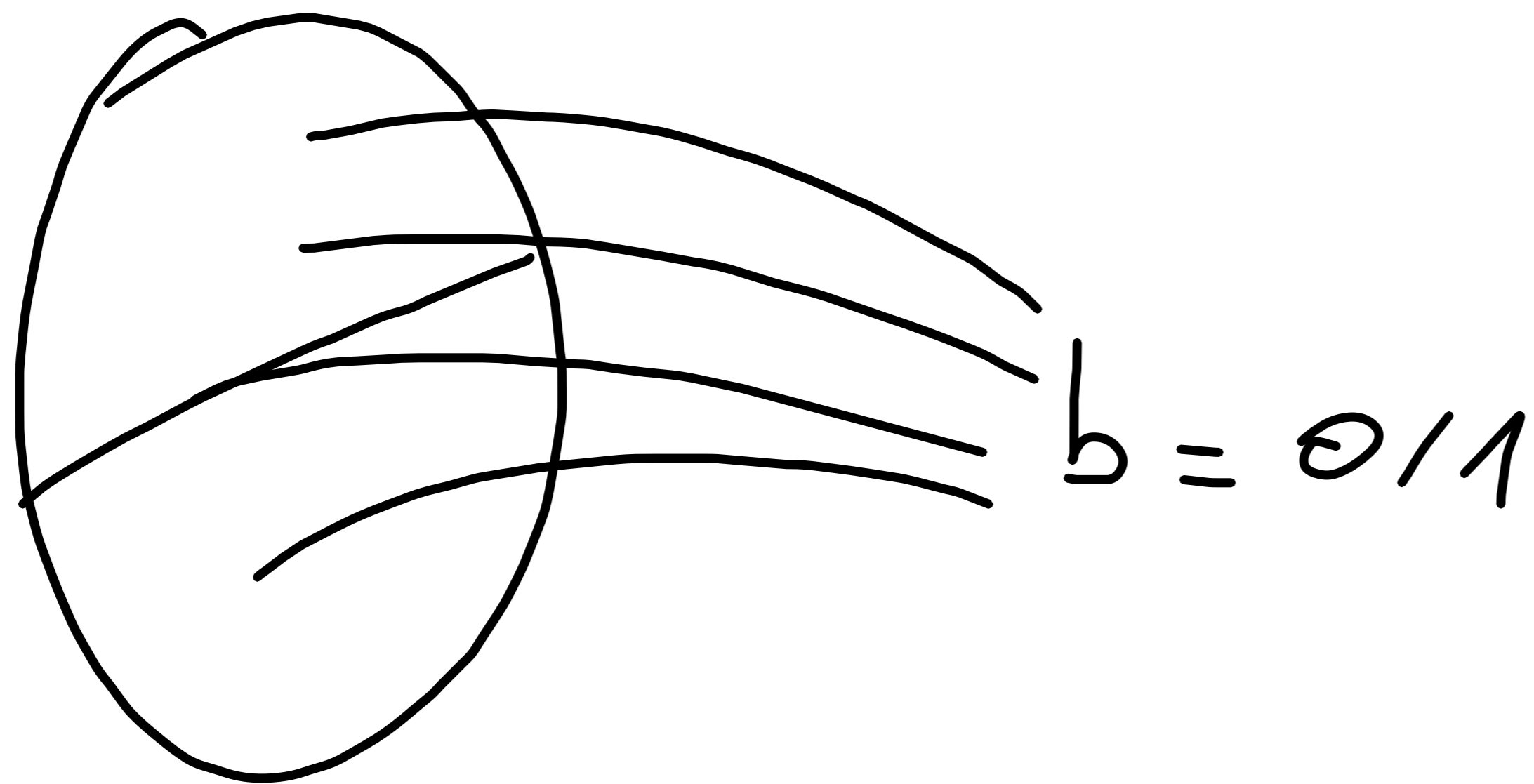
Impossible!

Even for  $k = n-1$  and  $\text{Ext} : \{0,1\}^n \rightarrow \{0,1\}$ .

Why? Take any  $\text{Ext}$  and let  $b \in \{0,1\}$

s.t.  $|\text{Ext}^{-1}(b)| \leq \text{MAX}$

$$\Rightarrow |\text{Ext}^{-1}(b)| \geq 2^{n-1}$$



The "attack": Take  $X$  to be uniform over  $\text{Ext}^{-1}(b)$

$$H_{\infty}(X) \geq n-1 ; \text{Ext}(X) = b \quad \square$$

Way out:

\* Independent sources:  $X_1, X_2$  s.t.  
-  $\checkmark$  Seeded extraction  $\left. \begin{array}{l} H_{\infty}(X_1) \geq k \\ H_{\infty}(X_2) \geq k \end{array} \right\} \underline{\text{HARD}}$

↪ Assume extractor takes as input CATALYST  
uniformly random seed  $s \in \{0, 1\}^d$

Non trivial Ext outputs  $\gg d$  bits.