THM Any family $\mathcal{H}$ of pairwise indep. hash functions directly gives a $\varepsilon = 1/|\mathcal{C}| - \text{secure MAC}$.

Proof. Fix any $m \in \mathcal{M}$, $\tau \in \mathcal{C}$:

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

$$\Pr_K[h(K, m) = \tau] = 1/|\mathcal{C}|$$

by PAIRWISE IN DEP.

Symmetrically, for any m, m' s.t. $m \neq m'$
$\tau, \tau' \in \mathcal{T}$.

$$\Pr_K[\mathrm{Tag}(K, m) = \tau \wedge \mathrm{Tag}(K, m') = \tau']$$

$$= \Pr_K[h(K, m) = \tau \wedge h(K, m') = \tau']$$

$$= 1/|\mathcal{T}|^2.$$

By Bayes':

$$\Pr[\mathrm{Tag}(k, m') = \tau' \mid \mathrm{Tag}(k, m) = \tau]$$

$$= \Pr[h(k, m') = \tau' \wedge h(k, m) = \tau]$$

$$\Pr[h(k, m) = \tau]$$

$$= \frac{1/|\tau|^2}{1/|\tau|} = \frac{1}{|\tau|}$$

■

Now, we universal hash. Here is a construction: Let p be a prime.

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

$$K = (a, b) \in \mathbb{Z}_p^2 = K$$

$$\mathbb{Z}_p = M = T$$

LEMMA The above H is pairwise indep.

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

$$\Pr_{(a,b)\in \mathbb{Z}_p^2}\left[h_{a,b}(m) = \tau \wedge h_{a,b}(m') = \tau' \right]$$

$$\begin{cases} a \cdot m + b = \tau \\ a \cdot m' + b = \tau' \end{cases}$$

$$\Pr_{(a,b)\in \mathbb{Z}_p^2}\left[\begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \tau \\ \tau' \end{pmatrix} \right]$$

$$\Pr_{(a,b)\in \mathbb{Z}_p^2}\left[\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} \tau \\ \tau' \end{pmatrix} \right]$$

$\det(\cdot) \neq 0$ dunque è invertibile

$$= \frac{1}{p^2} = \frac{1}{|\mathbb{Z}_p|^2} = \frac{1}{|C|^2}$$ ∎

Exercise: Show that the above scheme would not be 2-time secret, secure.

Exercise: Construct a 3-wise indep. hash family.

RANDOMNESS EXTRACTION

Alice and Bob need a RANDOM key.

How do they generate it?

As we will see later, randomness will be CRUCIAL for secure crypto.

There are two components in ANY randomness generator (Fortuna, /dev/random):

- Randomness extraction: By measuring physical quantities we can get an

UNPREDICTABLE sequence of bits

(Not necessarily UNIFORM!
Expensive to generate!)

From this, extract RANDOM Y
which is short (256 bits)

- Expand it to any amount ("polynomial")
using a pseudorandom generator
(PRG) — requires computational
assumptions!

We want randomness: how to extract from UNPREDICTABLE source X.

Example: Von Neumann Extractor. Assume $B \in \{0,1\}$ s.t. $\Pr[B=0] = p < 1/2$.

- Sample $b_1 \leftarrow B$, $b_2 \leftarrow B$
- If $b_1 = b_2$
  Resample
- Else output 1 iff $b_1 = 0, b_2 = 1$
  0 iff $b_1 = 1, b_2 = 0$

Assuming all outputs something. This will be 2.

$$Pr[\text{Output} = 1] = Pr[\text{Output} = 1]$$

$$\geq p \cdot (1-p)$$

$$Pr[\text{No output of the } n \text{ runs}]$$

$$= (1 - 2p(1-p))^n$$

becomes small for large enough n.

We want to generalize this question.

DREAM: Design Ext taking RV X and outputting (UNIFORM $Ext(X)$).

Impossible! ↳ DETERMINISTIC.

The source must be UNPREDICTABLE!

DEF (MIN-ENTROPY) The min-entropy of X is $H_\infty(X) = -\log_2 \max_x \Pr[X=x]$

EXAMPLE: Let $X \equiv U_n$ UNIFORM ON $\{0,1\}^n$. $H_\infty(X) = n$.

Let X be constant:

$$H_\infty(X) = 0$$

Next best thing: Design Ext that extracts uniform $Y = Ext(X)$ for every X s.t. $H_\infty(X) \geq k$

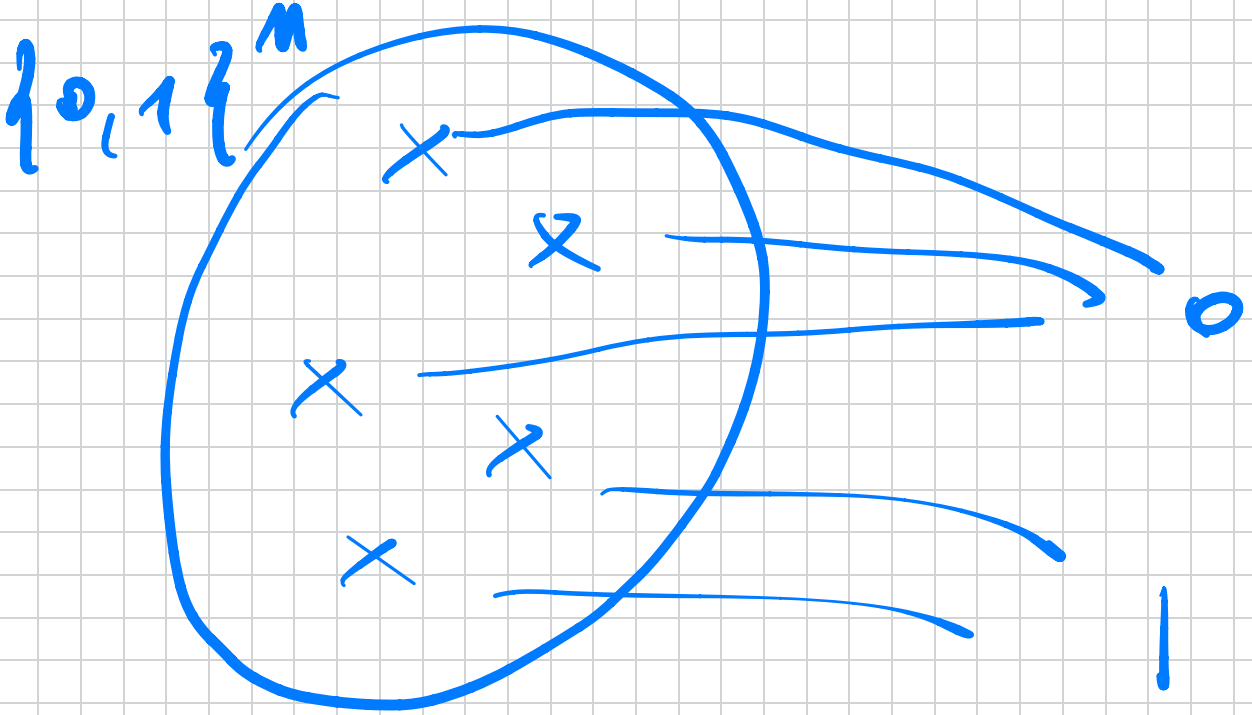
Also IMPOSSIBLE: Even if

$$Ext(X) = b \in \{0,1\}$$

$$K = N - 1$$

$$X \in \{0,1\}^N$$

Here is why: For any $Ext : \{0,1\}^N \to \{0,1\}$ and let $b \in \{0,1\}$ be the output maximizing $|Ext^{-1}(b)|$



$|Ext^{-1}(b)|$

$\geq 2^{n-1}$

$= 2^n/2$

The bad X: Define X to be UNIFORM over $Ext^{-1}(b)$. Since it is uniform: $H_\infty(X) \geq n-1$

But $Ext(X) = b$ so NOT UNIFORM.

Solution: Swap the quantifiers.

Def (SEEDED EXTRACTOR). A function

$$Ext : \{0,1\}^d \times \{0,1\}^n \to \{0,1\}^\ell$$

is a (k, ε)- extractor if

for all X s.t. $H_\infty(X) \geq k$:

$$(S, Ext(S, X)) \approx_\varepsilon (S, U_\ell)$$

for $S \equiv U_d$ (uniform over $\{0,1\}^d$).

(Note that $(S, U_\ell) \equiv U_{\ell+d}$.)

What does it mean? There is a STANDARD WAY to measure distance between distributions:

$$Z \approx_\varepsilon Z' \iff$$

$$SD(Z; Z') \leq \varepsilon$$

$$SD(Z; Z') = \frac{1}{2} \sum_z \left| Pr[Z = z] - Pr[Z' = z] \right|$$

Thus we equivalent: $\forall$ UNBOUNDED ADV. A:

$$\left| \Pr[A(z)=1 : z \leftarrow Z] - \Pr[A(z)=1 : z \leftarrow Z'] \right| \leq \epsilon$$

THM (LEFTOVER HASH LEMMA). Let $\mathcal{H} = \{ h_s : \{0,1\}^n \to \{0,1\}^\ell \}_{s \in \{0,1\}^d}$

be a PAIRWISE INDEP. family. Then,
$Ext(s,x) = h(s,x)$ is a (k,ε)-
extractor for $k \geq l + 2\log(1/\varepsilon) - 2$.

LEMMA. Let Y be a RV over $\mathcal{Y}$, such that:

$$Col(Y) = \sum_{y \in \mathcal{Y}} Pr[Y=y]^2$$

$$\leq \frac{1}{|\mathcal{Y}|} \cdot (1+4\varepsilon^2)$$

Then, $SD(Y; U) \leq \varepsilon$.