$\rightarrow h_{a,b}(x) = ax + b \mod p$

$(a,b) \in \mathbb{Z}_p^2$ is PAIRWISE INDEP.

EXERCISE Prove or disprove: The one-time pad is a statistical secure MAC. This means:

$$\text{Tag}(k, m) = k \oplus m = \tau$$

Attack: $\tau' = \tau \oplus m''$; $m' = m \oplus m''$

$$c' = (k \oplus m) \oplus m'' = k \oplus (m \oplus m'')$$
$$= k \oplus m'$$

The pair m', c' is VALID.

EXERCISE Show there exists Tag that is stat. secure but not PERFECT SECRET.

THM Let $\mathcal{H}$ be PAIRWISE INDEPENDENT, Then $\text{Tag}(k, m) = h_k(m)$ is

ε - stat. secure for $\varepsilon = 1/|\mathcal{T}|$

Proof. On the one hand: $\forall m, \forall \tau$

$$\Pr_K[\mathrm{Tag}(K, m) = \tau] = \Pr[h(K, m) = \tau]$$
$$= 1/|\mathcal{T}|$$

On the other hand, $\forall m, m'$ with $m \neq m'$, $\forall \tau, \tau'$

$$\Pr_K[\mathrm{Tag}(K, m) = \tau \wedge \mathrm{Tag}(K, m') = \tau']$$
$$= 1/|\mathcal{T}|^2$$

Made with Goodnotes

$$\Rightarrow \Pr[h(K,m') = \tau' \mid h(K,m) = \tau]$$

$$= \frac{1/|\mathcal{T}|^2}{1/|\mathcal{T}|} = 1/|\mathcal{T}| \qquad \blacksquare$$

Construction: Let p be a prime. Define:

$$\tau = h_{a,b}(x) = ax + b \bmod p \mapsto \{0, 1, \ldots, p-1\}$$

$x, \tau \in \mathbb{Z}_p \qquad (a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p$

Lemma The above $\mathcal{H}$ is pairwise indep.

So, we get $\varepsilon = 1/p$ - stat. secure MAC.

Proof. Fix $m, m' \in \mathbb{Z}_p$ and $\tau, \tau' \in \mathbb{Z}_p$
$m \neq m'$

$$\Pr_{a,b}\left[h_{a,b}(m) = \tau \wedge h_{a,b}(m') = \tau' \right]$$

$$= \Pr_{a,b}\left[\begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \tau \\ \tau' \end{pmatrix} \bmod p \right]$$

$$= \Pr_{a,b}\left[\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} \tau \\ \tau' \end{pmatrix} \bmod p \right]$$

$$= \Pr_{a,b}\left[\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} \right] = 1/p^2 \quad \blacksquare$$

c, d are fixed function of m, m', τ, τ'

We have a $2^{-\lambda}$-stat. secure MAC by choosing any λ-bit prime p.

Drawback: The key is twice as long as the message. Unfortunately:

Thm Any t-time $2^{-\lambda}$-stat. secure MAC has keys of size $(t+1)\cdot\lambda$.

We'd like to do much better: Alice and Bob share a key of length λ independent of t.

RANDOMNESS EXTRACTION

Randomness is crucial for crypto. For one, we need random keys.
But also, we'll see that even the algorithms need to be randomized.
Randomness comes from nature. Randomness in nature is IMPERFECT, while it can be "purified" it's very expensive.
Randomness extraction: How to extract UNIFORM randomness from an imperfect RANDOM source.

Example: The goal is to design some function Ext that takes some X (not uniform) and outputs something uniform.

Suppose you have a biased coin: $\Pr[B=0] = p < 1/2$. How to extract uniform randomness?

- Sample $b_1, b_2 \leftarrow B$
- If $b_1 = b_2$

  sample again

  Else

  Output 1 if $b_1 = 0, b_2 = 1$

  Output 0 if $b_1 = 1, b_2 = 0$

$$\Pr[\text{Ext outputs } 0] = \Pr[\text{Ext outputs } 1]$$
$$= p(1-p).$$

$\Pr[$No output after k trials$]$ is small.

In general, can we design a "good" Ext for any X? No. Because Ext is deterministic and X could be completely PREDICTABLE.

$\Rightarrow$ X needs to be UNPREDICTABLE.

DEF (MIN-ENTROPY). The min-entropy of X is

$$H_\infty(X) = -\log \max_x \Pr[X = x].$$

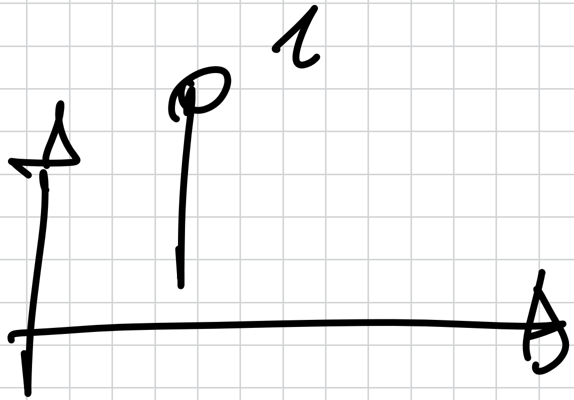
Intuition: The best probability to produce X by UNBOUNDED ADV.

Example: Let $X = U_n$ (UNIFORM over $\{0,1\}^n$)

$$H_\infty(U_n) = n$$

Let $X = 0^n$ (constant)

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



For real-world phenomena, we can get get lower bound $H_\infty(X) \geq k$. $(k < n)$

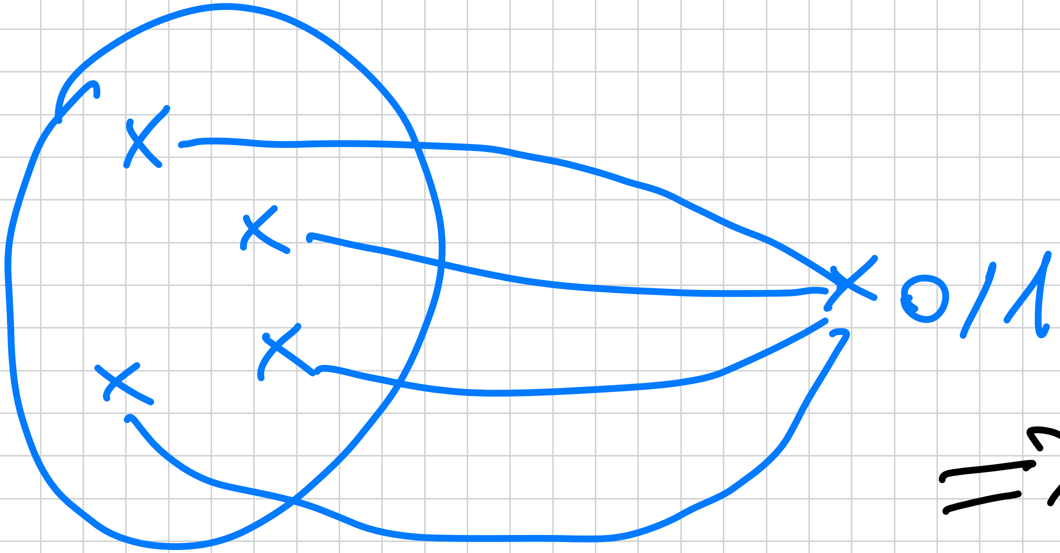
Goal: Design Ext that extracts from any X s.t. $H_\infty(X) \geq k$.

Thm. This is impossible even if $k = n-1$ and $Ext : \{0,1\}^n \to \{0,1\}$

Proof. Intuition: For every $Ext : \{0,1\}^n \to \{0,1\}$ there exists some X s.t. $H_\infty(X) = n-1$ but Ext fails on such X.

Let $b \in \{0,1\}$ be the value that maximizes $|Ext^{-1}(b)|$.

Made with Goodnotes



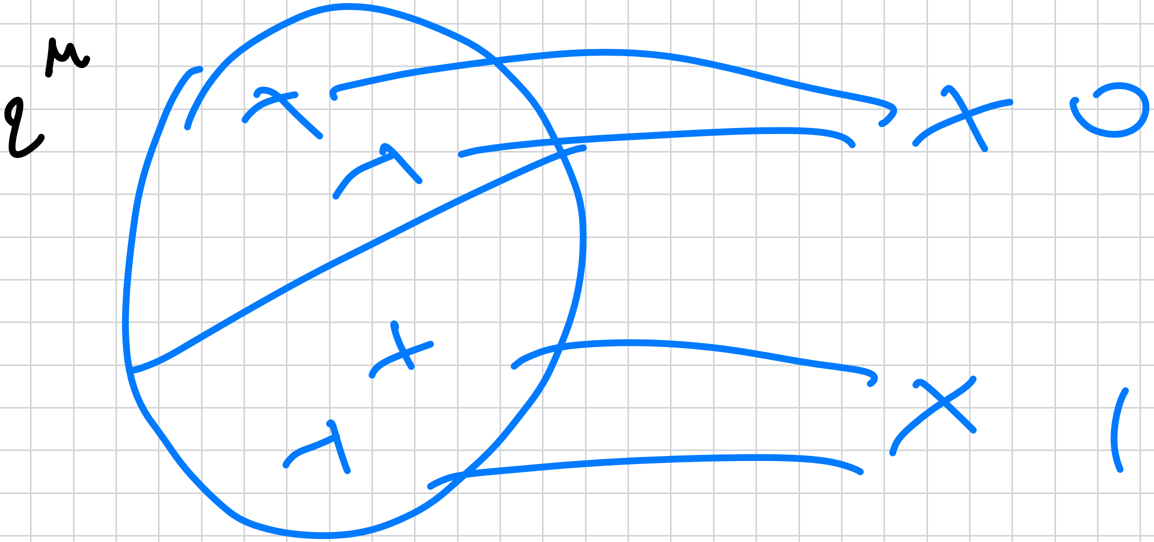
$$\Rightarrow \quad |Ext^{-1}(b)| \geq 2^{n-1}$$

Let X be uniform over $Ext^{-1}(b)$

Now:

$$H_\infty(X) \geq n-1$$

$$Ext(X) = b \quad \blacksquare$$



We need to change the model:

1) Assume independent X_1, X_2 s.t.

$H_\infty(X_1), H_\infty(X_2) \geq k$.

2) Assume the extractor is SEEDED:

$$\mathrm{Ext}(S, X)$$

$$S \in \{0,1\}^d \; ; \; X \in \{0,1\}^n$$

The seed is UNIFORM, but PUBLIC.

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

is a (k, ε)-SEEDED EXTRACTOR if

$\forall X \in \{0,1\}^n$ s.t. $H_\infty(X) \geq k$

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

where U_ℓ is UNIFORM, $S \equiv U_d$ is UNIFORM

$\approx_\varepsilon$: ε-CLOSE TO UNIFORM

$$SD(X;Y) = \frac{1}{2} \sum_{z} \left| \Pr[X = z] \right.$$

$$- \Pr[Y = z]\Big| \leq \varepsilon$$

Equivalent: An UNBOUNDED ADV can't distinguish a sample $z \leftarrow X$ from $z \leftarrow Y$ w.p. better than ε.