Entropy: Alternative notions

As we argued before, there is no unique notion of vulnerability. It depends on:

- the model of attack, and
- how we measure its success

Consider again the general **model of adversary** proposed by [Köpf and Basin CCS'07] that we saw before:

- Assume an oracle that answers yes/no to questions of a certain form.
- The adversary is defined by the form of the questions and the measure of success.
- In general we consider the best strategy for the adversary, with respect to a given measure of success.

Entropy: Alternative notions

We saw that if

- the questions are of the form: "is $S \in P$?", and
- the measure of success is: the expected number of questions needed to find the value of S in the adversary's best strategy

then the natural measure of protection is Shannon's entropy

However, this model of attack does not seem so natural in security, and alternatives have been considered. In particular, the **limited-try attacks**

- The adversary has a limited number of attempts at its disposal
- The measure of success is the probability that he discovers the secret during these attempts (in his best strategy)

Obviously the best strategy for the adversary is to try first the values which have the highest probability

One try attacks: Rényi min-entropy

One-try attacks

- The questions are of the form: “is $S = s$?”
- The measure of success is: $-\log(\max_s p(s))$

The measure of success is Rényi min-entropy: $H_\infty(S) = -\log(\max_s p(s))$

Like in the case of Shannon entropy, $H_\infty(S)$ is highest when the distribution is uniform, and it is 0 when the distribution is a delta of Dirac (no uncertainty).

Towards a notion of leakage based on min-entropy

Leakage = difference between
the a priori vulnerability
and
the a posteriori vulnerability

Leakage = $H_\infty(S) - H_\infty(S \mid O)$

How should we define the conditional min-entropy $H_\infty(S \mid O)$?

Let us recall the conditional entropy in Shannon's case

$$H(S) = -\sum_s p(s)\log p(s)$$ Shannon entropy

An observable o determines a new distribution on S:

$$p(s|o) = p(s)\frac{p(o|s)}{p(o)}$$ Bayes theorem

Define the entropy of the new distribution on S, given that $O = o$, as:

$$H(S|O=o) \quad = \quad -\sum_s p(s|o)\log p(s|o)$$

Define conditional entropy as the expected value of the updated entropies:

$$\begin{aligned} H(S|O) \quad &= \quad \sum_o p(o)\; H(S|O=o) \\ &= \quad -\sum_o p(o)\sum_s p(s|o)\log p(s|o) \end{aligned}$$

Let us try to do the same for the min-entropy case

$$H_\infty(S) = -\log(\max_s p(s))$$ Rényi min-entropy

Define the entropy of the new distribution on S, given that $O = o$, as:

$$H_\infty(S|O=o) \quad = \quad -\log(\max_s p(s|o))$$

Define conditional entropy as the expected value of the updated entropies:

$$\begin{aligned} H_\infty(S|O) \quad &= \quad \sum_o p(o)\; H_\infty(S|O=o) \\ &= \quad -\sum_o p(o) \log(\max_s (s|o)) \end{aligned}$$

However this approach does not work: we would obtain negative leakage!

Conditional min-entropy

Probability of success of an attack on S, given that $O = o$:

$$\Pr_{succ}(S|O=o) \quad = \quad \max_s p(s|o)$$

The expected value of the prob. of success (aka converse of the Bayes risk):

$$\begin{aligned}\Pr_{succ}(S|O) &= \sum_o p(o)\,\Pr_{succ}(S|O=o)\\ &= \sum_o p(o)\,\max_s\, p(s|o)\\ &= \sum_o \max_s\,(p(o|s)\,p(s))\end{aligned}$$

Now define $H_\infty(S|O) = -\log \Pr_{succ}(S|O)$ [Smith 2009]

Leakage in the min-entropy approach

A priori $H_\infty(S) = -\log \max_s p(s)$

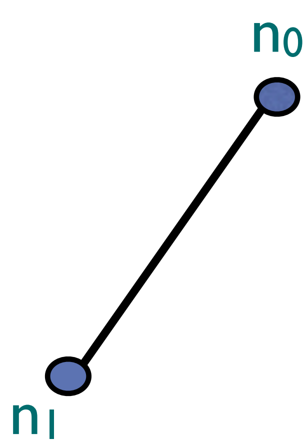
A posteriori $H_\infty(S|O) = -\log \sum_o \max_s (p(o|s) \cdot p(s))$

Leakage = min-Mutual Inf. $I_\infty(S;O) = H_\infty(S) - H_\infty(S|O)$

Example: DC nets. Ring of 2 nodes, b = 1, biased coin

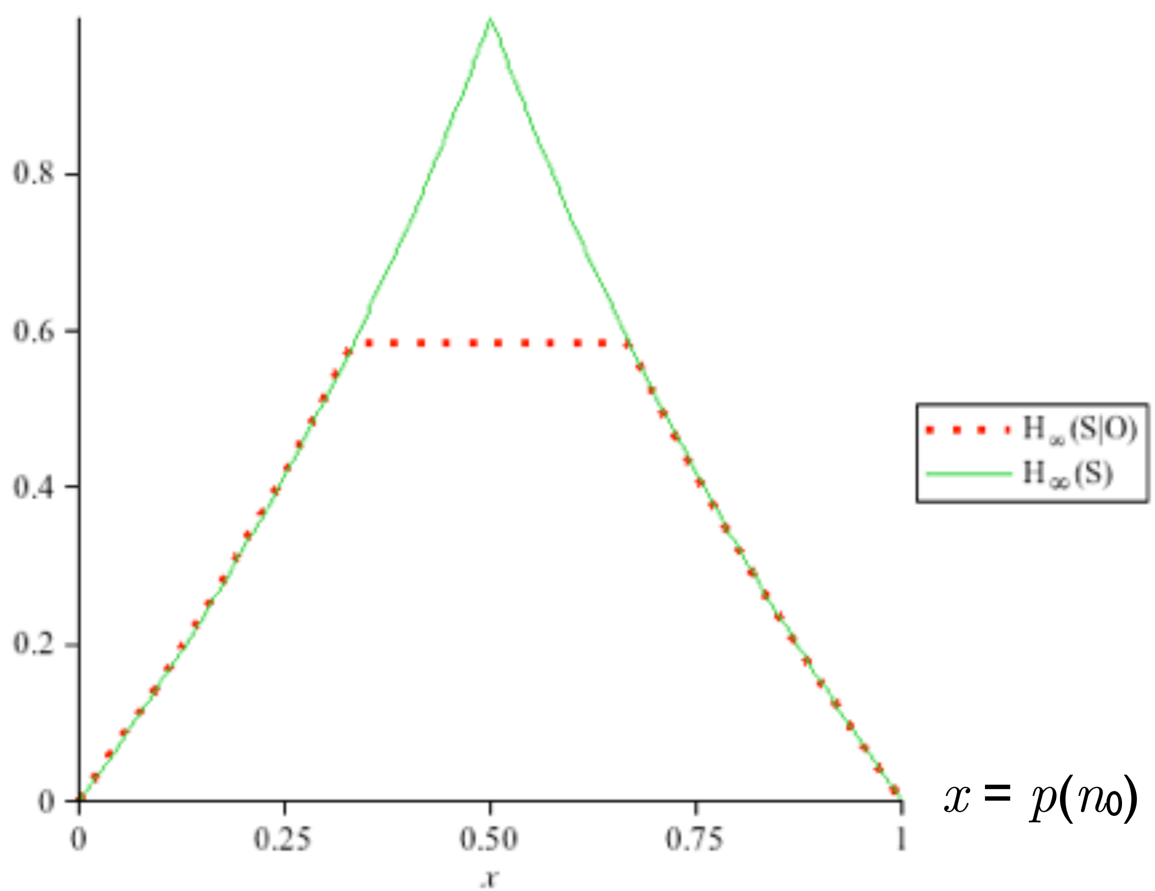
Input S: n_0 , n_1

Output O: the declarations of n_1 and n_0: $d_1 d_0 \in \{01,10\}$



Biased c.: p(0) = ⅔ p(1) = ⅓

	01	10
n0	⅔	⅓
n1	⅓	⅔



$x = p(n_0)$

Properties of the leakage in the min-entropy approach

- In general $I_\infty(S;O) \geq 0$
- $I_\infty(S;O) = 0$ if all rows are the same (but not viceversa)
- Define min-capacity: C_∞ = max $I_\infty(S;O)$ over all priors. We have:
  1. $C_\infty = 0$ if and only if all rows are the same
  2. C_∞ is obtained on the uniform distribution (but, in general, there can be other distribution that give maximum leakage)
  3. C_∞ = the log of the sum of the max of each column
  4. $C_\infty = C$ in the deterministic case
  5. $C_\infty \geq C$ in general

Leakage in the min-entropy approach

- C_∞ is obtained on the uniform distribution
- C_∞ = the sum of the max of each column

Proof (a)

$$
\begin{aligned}
I_\infty(S;O) &= H_\infty(S) - H_\infty(S|O) \\
&= -\log \max_s\ p(s) - (-\log(\sum_o \max_s (p(o|s)\, p(s)))) \\
&= \log \frac{\sum_o \max_s (p(o|s)\, p(s))}{\max_s\ p(s)} \\
&\leq \log \frac{\sum_o (\max_s\ p(o|s))\, (\max_s\ p(s))}{\max_s\ p(s)} \\
&= \log \sum_o \max_s\ p(o|s)
\end{aligned}
$$

(b) This expression is also given by $I_\infty(S;O)$ on the uniform input distribution