# Quantitative approaches to information protection

Course in Pisa, April 2014
Lecture 3

# Leakage in the min-entropy approach

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

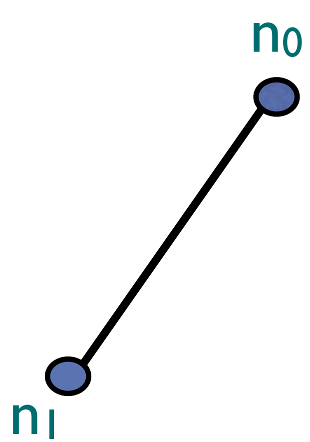
A posteriori $$H_\infty(S|O) = -\log \sum_o \max_s (p(o|s) \cdot p(s))$$

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

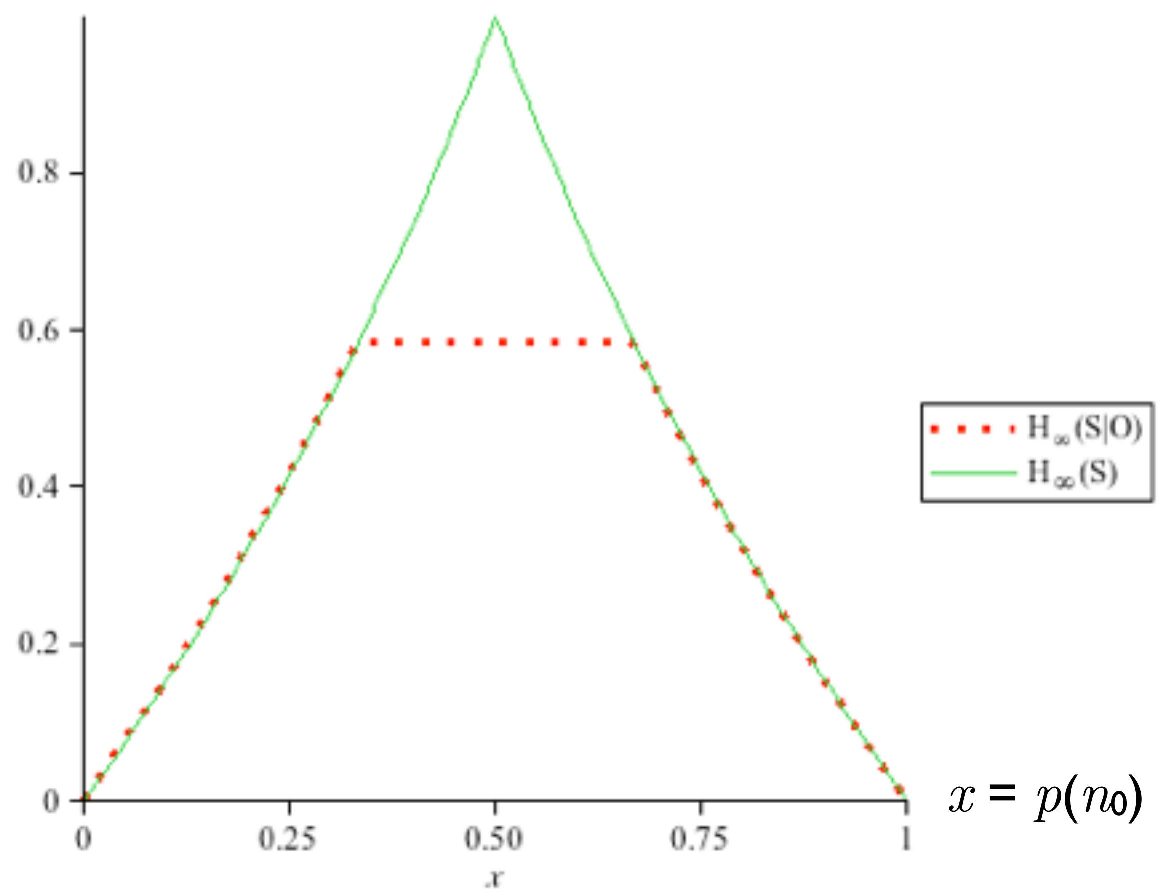
Input $S$: $n_0$ , $n_1$

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 |
|---|---|---|
| n | ⅔ | ⅓ |
| n | 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: $C_\infty =$ max $I_\infty(S;O)$ over all priors. We have:
  1. $C_\infty = 0$ if and only if all rows are the same
  2. $C_\infty$ is obtained on the uniform distribution (but, in general, there can be other distribution that give maximum leakage)
  3. $C_\infty =$ 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

- $C_\infty$ is obtained on the uniform distribution
- $C_\infty$ = 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

# Exercises

4. Prove that $I_\infty(S;O) \geq 0$
5. Prove that if all rows of the channel matrix are equal, then $I_\infty(S;O) = 0$
6. Prove that all rows of the channel matrix are equal if and only if $C_\infty = 0$
7. Compute Shannon leakage and Rényi min-leakage for the password checker (the version where the adversary can observe the execution time), assuming a uniform distribution on the passwords