AN AXIOMATIC APPROACH TO QUANTITATIVE INFORMATION FLOW

MARIO S. ALVIM   KOSTAS CHATZIKOKOLAKIS   ANNABELLE MCIVER
CARROLL MORGAN   CATUSCIA PALAMIDESSI   GEOFFREY SMITH

Quantitative information flow: **vulnerability** of a secret

…

Shannon entropy

…

guessing entropy

Rényi min-entropy

g-vulnerability

…

g-vulnerability

(talks by Geoffrey and Carroll)

- General: it encompasses the most used notions (Shannon, guessing, min-vulnerability,…)
- Operational interpretation: the gain functions express the gain of the adversary
- Some useful properties:
  - Min-leakage is an upper bound to g-leakage
  - The robust leakage ordering (w.r.t. all gain functions and all priors) coincides with the post-processing ordering
- but… does *g*-vulnerability represent all conceivable kinds of vulnerability ?

A principled approach

- What are the properties that any "reasonable" notion of vulnerability should have?
- Notation:
  - X , Y — random variables (secrets, observables)
  - $C : X \rightarrow Y$ — channel (system)
  - $\mathbb{V}(X)$ — prior vulnerability of X
  - $\mathbb{V}(X|Y)$ — posterior vulnerability of X given Y

Axioms of vulnerability I

Let $C : X \rightarrow Y$ and $D : Y \rightarrow Z$

- Data Processing Inequality (DPI)

  $\mathbb{V}(X \mid Z) \leqslant \mathbb{V}(X \mid Y)$

- Non-Negativity of leakage (NN)

  $\mathbb{V}(X) \leqslant \mathbb{V}(X \mid Y)$

Axioms of vulnerability II

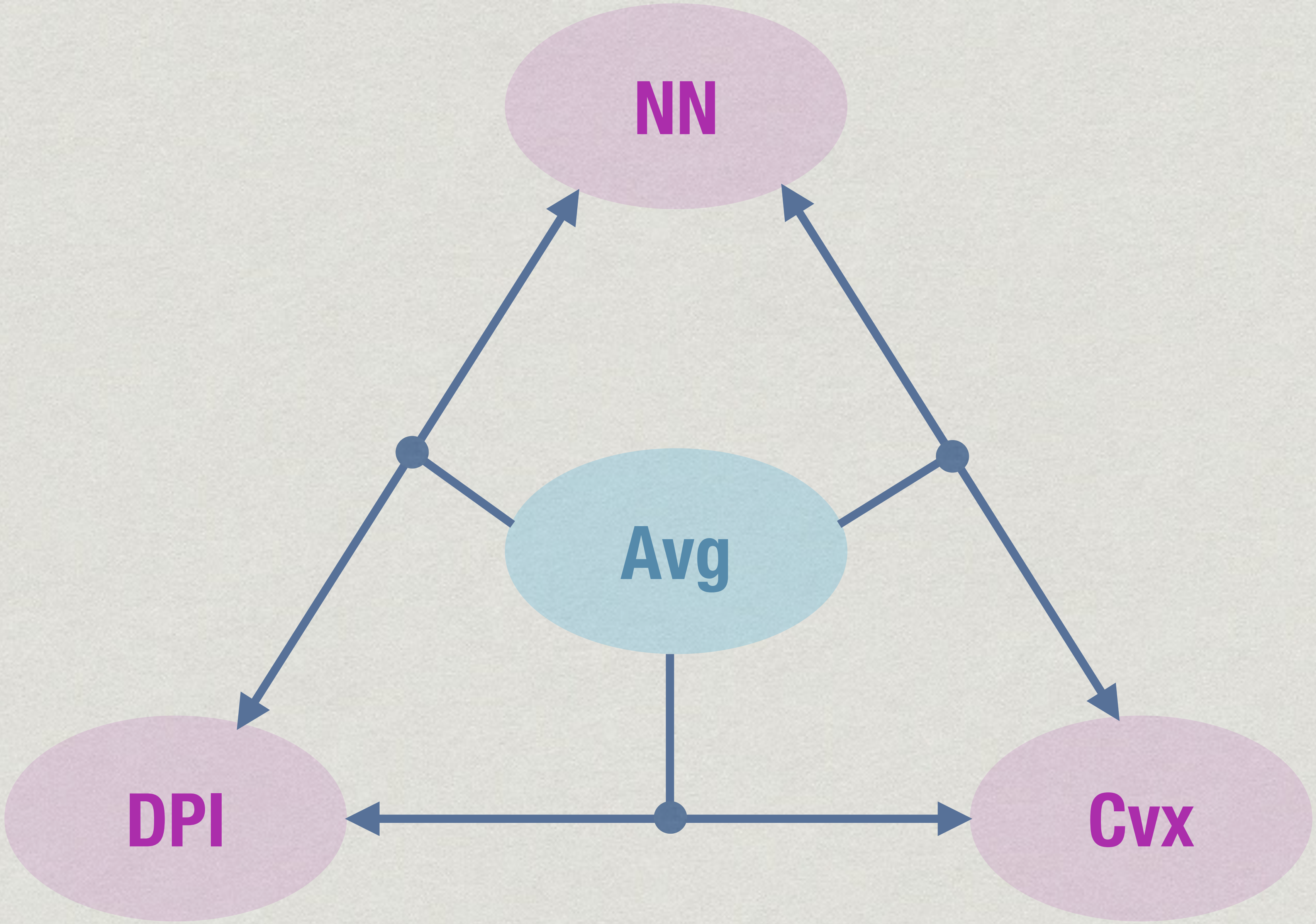
Let π be the distribution of X (prior)
and *p* be the distribution of Y (posterior)

- Convexity (Cvx)

$$\mathbb{V}(c\,\pi + (1-c)\,\pi') \leq c\,\mathbb{V}(\pi) + (1-c)\,\mathbb{V}(\pi')$$

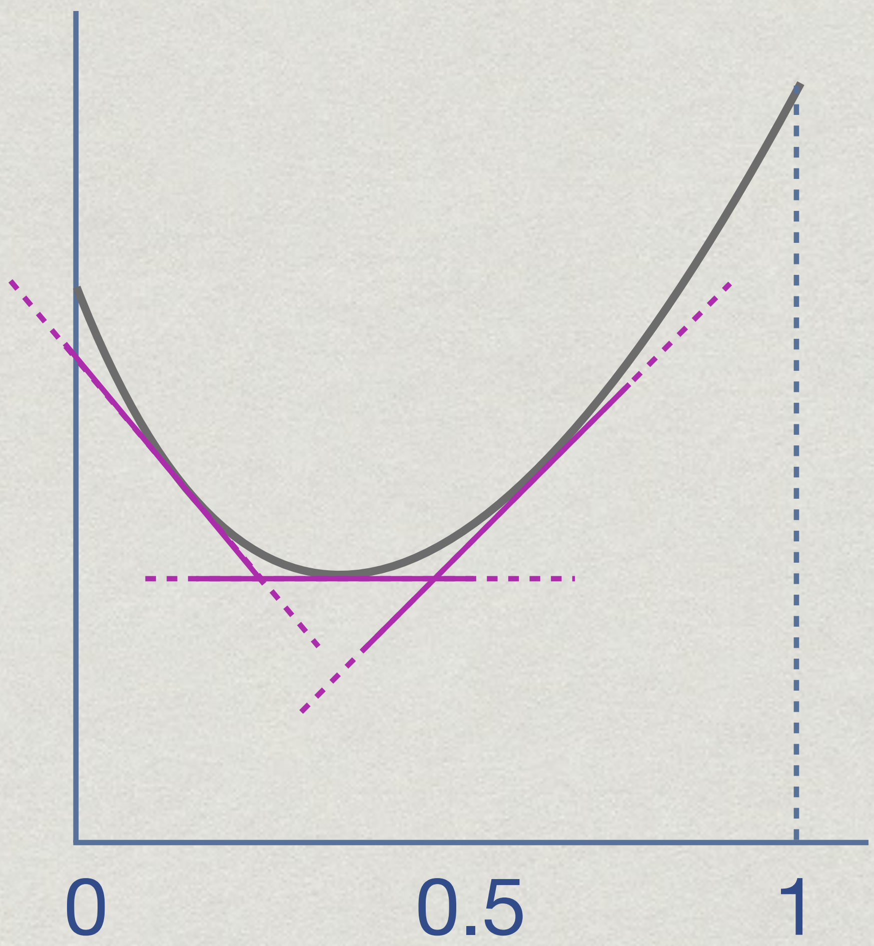
- Averaging (Avg)

$$\mathbb{V}(X \mid Y) = \sum_y p(y)\,\mathbb{V}(X \mid Y=y)$$



If we assume Avg, the other three axioms are equivalent

Convexity implies g-vulnerability



$\mathbb{V}_g(\pi) = \max_w \sum_x \pi(x)\, g(x,w)$

Posterior g-vulnerability is defined by averaging

Additional axioms to obtain Shannon entropy

Relation: $\mathbb{H}(X) = \mathbb{V}_{max}|X| - \mathbb{V}(X)$

- Symmetry:
  if the distributions of X , X′ have the same probability values, modulo permutation, then
  $\mathbb{H}(X) = \mathbb{H}(X')$

- Chain rule:
  $\mathbb{H}(X,Y) = \mathbb{H}(X \mid Y) + \mathbb{H}(Y)$

  Note that the chain rule together with symmetry imply the reversibility of information leakage (which is not valid, in general, for g-vulnerability) :

  $\mathbb{V}(X \mid Y) - \mathbb{V}(X) = \mathbb{V}(Y \mid X) - \mathbb{V}(Y)$

  typical definition of leakage

Thank you