Quantitative Information Flow (QIF) **DCC/ICEx/UFMG**
Prof. Mário S. Alvim **2021/1**

PROBLEM SET

Axiomatics / The geometry of hypers, gains and losses / The Crowds protocol
(Chapters 11 / 12 / 18)

Necessary reading for this assignment:

- *The Science of Quantitative Information Flow* (Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, and Smith):
  - Chapter 11: *Axiomatics*
    - Chapter 11.1: *An axiomatic view of vulnerability*
    - Chapter 11.2: *Axiomatization of prior vulnerabilities*
    - Chapter 11.3: *Axiomatization of posterior vulnerabilities*
    - Chapter 11.4: *Applications of axiomatization to understanding leakage measures*
  - Chapter 12: *The geometry of hypers, gains and losses*
    - Chapter 12.1: *Barycentric representation of gain/loss functions*
    - Chapter 12.2: *Barycentric representation of hypers and their refinement*
  - Chapter 18: *The Crowds protocol*
    - Chapter 18.1: *Introduction to Crowds, and its purpose*
    - Chapter 18.2: *Modeling the Crowds protocol*
    - Chapter 18.3: *Bayes vulnerability and Bayes leakage*
    - Chapter 18.4: *Explanation of the paradox*
    - Chapter 18.5: *Why φ matters, even for uniform priors*
    - Chapter 18.6: *Refinement: increasing φ is always safe*
    - Chapter 18.7: *Multiple paths*

Review questions.

1. Explain in your own words what the following axioms for prior vulnerabilities mean.
   (a) Continuity (`CNTY`).
   (b) Convexity (`CVX`).
2. Explain in your own words what the following axioms for posterior vulnerabilities mean.
   (a) Noninterference (`NI`).
   (b) Data-processing inequality (`DPI`).
   (c) Monotonicity (`MONO`).
3. Explain in your own words what the following axioms relating prior and posterior vulnerabilities mean.
   (a) Averaging (`AVG`).
   (b) Maximum (`MAX`).
4. Explain in your own words the significance of the relationship among axioms depicted in Figure 11.1.

Exercises.

5. (Exercise 12.1) Explain why the first action of a channel on a prior seems to reveal more (non-negative leakage), but subsequent multiplications (by refinement/post-processing matrices) loses information (the data-processing inequality *DPI* of §4.6.2).

6. (Exercise 18.2) In §18.6 is was shown rigorously that increasing the forwarding probability φ results in a refinement of the protocol, i.e. that for any prior and gain function the effect of increasing φ cannot be to increase the adversary's gain — increasing φ can never do any harm.

   But from that it is elementary that *decreasing* φ cannot *decrease* the adversary's gain (because then increasing φ back to its original value would contradict the above). Thus decreasing φ can never do any good.

   If that reasoning is so elementary, why do we bother to prove the "only if" for Thm. 18.3?