Bayesian Adversarial Privacy

A seminar by Christian Robert

Université Paris-Dauphine

Thursday 02 Apr 2026 | 14:30-15:30
Room BENVENUTI
Department of Statistical Sciences

Bayesian Adversarial Privacy

Theoretical and applied research into privacy encompasses an incredibly broad swathe of differing approaches, emphasis and aims. In a first part, we propose a novel framework for measuring privacy from a Bayesian game-theoretic perspective. This framework enables the creation of new, purpose-driven privacy definitions that are rigorously justified, while also allowing for the assessment of existing privacy guarantees through game theory. We show that pure and probabilistic differential privacy are special cases of our framework, and provide new interpretations of the post-processing inequality in this setting. Further, we demonstrate that privacy guarantees can be established for deterministic algorithms, which are overlooked by current privacy standards. In a second part, we introduce a new quantitative notion of privacy that is both contextual and specific. We argue that it provides a more meaningful notion of privacy than the widely utilised framework of differential privacy and a more explicit and rigorous formulation than what is commonly used in statistical disclosure theory. Our definition relies on concepts inherent to standard Bayesian decision theory, while departing from it in several important respects. In particular, the party controlling the release of sensitive information should make disclosure decisions from the prior viewpoint, rather than conditional on the data, even when the data is itself observed.

Joint work with James Bailie, Cameron Bell, Joshua Bon, Timothy Johnston, Antoine Luciano, and Judith Rousseau

https://arxiv.org/abs/2601.22945

https://arxiv.org/abs/2603.04199