Confidentialité différentielle

- Martin Kroll (Université de Bayreuth)

  Title: An introduction to local differential privacy in nonparametric statistics

  Abstract: This talk provides an introduction to differential privacy with an emphasis on local differential privacy. In the first part of the talk, we motivate the need for privacy-preserving data analysis and discuss several notions of privacy circulating in the research literature. We introduce the definition of differential privacy and discuss basic properties of this definition including the difference between the global and the local privacy setup. In the second part of the talk, we introduce several algorithmic buildings blocks that are usually used to generate differentially private data. In the third and last part, we discuss local differential privacy in the context of nonparametric estimation with a focus on nonparametric density estimation and nonparametric regression. For both problems we present optimal rates of convergence and show how the building blocks introduced in the second part can be used for the construction of rate optimal estimators.

- Hélène Halconruy (Telecom SudParis)

  Title: LDP drift parameter estimation for i.i.d. paths of diffusion processes

  Abstract: With the rise of large-scale sensitive data, understanding the tradeoffs between privacy and utility is crucial. Traditionally, exploring statistical inference under "local differential privacy" (LDP) has focused on N random variables without historical context, posing challenges like hypothesis testing and (non)parametric estimation.

  In the paper on which this talk is based, we address drift parameter estimation from N i.i.d. diffusion paths under LDP by proposing a contrast function using a pseudo-likelihood approach and adding suitably scaled Laplace noise to ensure privacy. Our findings provide explicit conditions for privacy, under which we establish the consistency and asymptotic normality of the estimator.

  This is a joint work with Chiara Amorino and Arnaud Gloter.

- Paul Mangold (École Polytechnique)

  Title: Differential Privacy has Bounded Impact on Fairness in Classification

  Abstract: We theoretically study the impact of differential privacy on fairness in classification. We prove that, given a class of models, popular group fairness measures are pointwise Lipschitz-continuous with respect to the parameters of the model. This result is a consequence of a more general statement on accuracy conditioned on an arbitrary event (such as membership to a sensitive group). We use this Lipschitz property to show that, given enough examples, the fairness level of private models is close to the one of their non-private counterparts.

- Karolina Klockmann (University of Vienna)

  Title: Pointwise spectral density estimation under local differential privacy

  Abstract: We propose a new interactive locally differentially private mechanism for estimating a Hölder-smooth spectral density function of a stationary Gaussian process at a fixed frequency. Anonymization is achieved through two-stage truncation and subsequent Laplace perturbation. In particular, we show that our method achieves a pointwise L2-rate with a dependency of only α^2 on the privacy parameter α. This rate stands in contrast to the results of (Kroll, 2024), who proposed a non-interactive locally differentially private mechanism for estimating the whole spectral density and showed a dependency of α^4 on the privacy parameter for the uniform L2-rate. Additionally, we show that for pointwise spectral density estimation with a non-interactive locally differentially privacy mechanism the factor α^4 is unavoidable in the convergence rate by proving the corresponding lower bounds