Recent Advances in Metric Privacy

Catuscia Palamidessi*[1,2]

[1]Inria Saclay - Ile de France – Institut National de Recherche en Informatique et en Automatique, Institut Polytechnique de Paris – France

[2]Ecole Polytechnique – Laboratoire d'informatique de l' ecole polytechnique – France

Résumé

Metric privacy is a generalization of differential privacy that, whenever the underline data domain is provided with a metric structure, can help reduce the amount of noise necessary to protect the sensitive information. Metric privacy has been used especially in the local model, and the standard mechanisms to it are based on the Laplace and the Geometric noise. These distributions, however, are not effective in the case of isolated data points (outliers). In this talk, I will show one approach to solve the problem, based on the Blahut-Arimoto algorithm from rate distortion theory (BA mechanism). Furthermore, I will discuss the Iterative Bayesian Update (IBU), an instance of the famous Expectation-Maximization method from Statistics, that can be applied to any local mechanism to de-noise the aggregated data and help recover utility. I will show that the IBU, combined with the BA mechanism, outperforms the state-of-the-art in terms of the trade-off privacy-utility, and I will show a surprising duality between IBU and the BA mecahnism. Finally, I will discuss applications of metric privacy to the generation of synthetic data.

*Intervenant