EPFL-Inria
INTERNATIONAL LAB

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Inria
INVENTEURS DU MONDE NUMÉRIQUE

Workshop EPFL-Inria
15 et 16 février 2018, Paris

Aurélien Bellet, MAGNET research team, Inria

Title: « Private Algorithms for Decentralized Collaborative Machine Learning »

Abstract:
With the advent of connected devices with computation and storage capabilities, it becomes possible to run machine learning on-device to provide personalized services. However, the currently dominant approach is to centralize data from all users on an external server for batch processing, sometimes without explicit consent from users and with little oversight. This centralization poses important privacy issues in applications involving sensitive data such as speech, medical records or geolocation logs.
In this talk, I will discuss an alternative setting where many agents with local datasets collaborate to learn models by engaging in a fully decentralized peer-to-peer network. We introduce and analyze asynchronous algorithms that allow agents to improve upon their locally trained model by exchanging information with other agents that have similar objectives. I will then describe how to make such algorithms differentially private to avoid leaking information about the local datasets, and analyze the resulting privacy-utility trade-off. These results are illustrated by a set of numerical experiments.