



Seminar/Talk

TCS Seminar - Unified Privacy Guarantees for Decentralized Learning via Matrix Factorization

Edwige Cyffers

ISTA

Host:

Decentralized Learning (DL) enables users to collaboratively train models without sharing raw data by iteratively averaging local updates with neighbors in a network graph. This setting is increasingly popular for its scalability and its ability to keep data local under user control. Strong privacy guarantees in DL are typically achieved through Differential Privacy (DP), with results showing that DL can even amplify privacy by disseminating noise across peer-to-peer communications. Yet in practice, the observed privacy-utility trade-off often appears worse than in centralized training, which may be due to limitations in current DP accounting methods for DL. In this paper, we show that recent advances in centralized DP accounting based on Matrix Factorization (MF) for analyzing temporal noise correlations can also be leveraged in DL. By generalizing existing MF results, we show how to cast both standard DL algorithms and common trust models into a unified formulation. This yields tighter privacy accounting for existing DP-DL algorithms and provides a principled way to develop new ones. To demonstrate the approach, we introduce MAFALDA-SGD, a gossip-based DL algorithm with user-level correlated noise that outperforms existing methods on synthetic and real-world graphs.

Tuesday, October 28, 2025 10:45am - 12:00pm

Central Bldg / O1 / Mondi 2a (I01.O1.008)



This invitation is valid as a ticket for the ISTA Shuttle from and to Heiligenstadt Station.

Please find a schedule of the ISTA Shuttle on our webpage:

<https://ista.ac.at/en/campus/how-to-get-here/> The ISTA Shuttle bus is marked ISTA Shuttle (#142) and has the Institute Logo printed on the side.