For favour of Posting

AMENDMENT**

THE HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY

Department of Mathematics

PHD STUDENT SEMINAR

Exploring Private Federated Learning with Laplacian Smoothing

By

Mr. Zhicong LIANG

Abstract

Federated learning aims to protect data privacy by collaboratively learning a model without sharing private data among users. However, an adversary may still be able to infer the private training data by attacking the released model. Differential privacy (DP) provides a statistical guarantee against such attacks, at a privacy of possibly degenerating the accuracy or utility of the trained models. In this paper, we apply a utility enhancement scheme based on Laplacian smoothing for differentially-private federated learning (DP-Fed-LS), where the parameter aggregation with injected Gaussian noise is improved in statistical precision. We provide tight closed-form privacy bounds for both uniform and Poisson subsampling and derive corresponding DP guarantees for differential private federated learning, with or without Laplacian smoothing. Experiments over MNIST, SVHN and Shakespeare datasets show that the proposed method can improve model accuracy with DP-guarantee under both subsampling mechanisms.

****Date : 14 May 2020 (Thursday)**

****Time : 11:00am – 12:00noon**

Zoom Meeting : https://hkust.zoom.us/j/91364836963

All are Welcome!