*For favour of Posting*

THE HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY

## Department of Mathematics

# PHD STUDENT SEMINAR

# Private Federated Learning

**By**

## Mr. Zhicong LIANG

**Abstract**

In this seminar, we will discuss private federated learning. We will firstly provide new optimization error bounds for differential private federated learning with Laplacian Smoothing (DP-Fed-LS) and heterogeneous data. The error bounds help us better understand the influence of errors introduced by differential privacy, heterogeneity of data and variance of stochastic gradient descent over the convergence of DP-Fed-LS. For another, we will also explore how to push the limit of private federated learning by improving current gradient attack. Experiment shows that our proposed new attack can recover training data with high quality while the targeted model is untrained and when the batch size is small. Attacks on more realistic settings are to be discussed.

**Date : 29 April 2021 (Thursday)**
**Time : 10:15am**
**Zoom Meeting : https://hkust.zoom.us/j/99997376210 (Passcode: 214192)**

*All are Welcome!*