*REVISED
For favour of Posting

THE HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY

Department of Mathematics

MATHEMATICS COLLOQUIUM

Theoretical Evaluation of Data Reconstruction Error and Induced Optimal Defenses

By

Prof. Qi Lei
New York University

Abstract

Data reconstruction attacks and defenses are crucial for understanding data leakage in machine learning and federated learning. However, previous research has largely focused on empirical observations of gradient inversion attacks, lacking a theoretical framework for quantitatively analyzing reconstruction errors based on model architecture and defense methods. In this talk, we propose framing the problem as an inverse problem, enabling a theoretical and systematic evaluation of data reconstruction attacks. For various defense methods, we derive the algorithmic upper bounds and matching information-theoretical lower bounds on reconstruction error for two-layer neural networks, accounting for feature and architecture dimensions as well as defense strength. We further propose two defense strategies — Optimal Gradient Noise and Optimal Gradient Pruning — that maximize reconstruction error while maintaining model performance.

Bio: *Qi Lei is an assistant professor of Mathematics and Data Science at the Courant Institute of Mathematical Sciences and the Center for Data Science at NYU. Previously she was an associate research scholar at the ECE department of Princeton University. She received her Ph.D. from Oden Institute for Computational Engineering & Sciences at UT Austin. She visited the Institute for Advanced Study (IAS)/Princeton for the Theoretical Machine Learning Program. Before that, she was a research fellow at Simons Institute for the Foundations of Deep Learning Program. Her research aims to develop mathematical groundings for trustworthy and (sample- and computationally) efficient machine learning algorithms. Qi has received several awards/recognitions, including Rising Stars in Machine Learning, in EECS, and in Statistics and Data Science, the Outstanding Dissertation Award, Computing Innovative Fellowship, and Simons-Berkeley Research Fellowship.*

Date : 07 February 2025 (Fri)
***Time : 10:30a.m. – 11:30a.m.**
***Venue : Room 3598 (Lifts 25/26)**
All Are Welcome!