THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Research Seminar

How To Preserve Privacy In Learning?

Mr Di Wang
PhD Candidate
Department of Computer Science and Engineering
The State University of New York, Buffalo
USA

Date : 7 April 2020 (Tuesday)
Time : 11:00 a.m. - 12:00 noon

▶ Abstract

Recent research showed that most of the existing learning models are vulnerable to various privacy attacks. Thus, a major challenge facing the machine learning community is how to learn effectively from sensitive data. An effective way for this problem is to enforce differential privacy during the learning process. As a rigorous scheme for privacy preserving, Differential Privacy (DP) has now become a standard for private data analysis. Despite its rapid development in theory, DP's adoption to the machine learning community remains slow due to various challenges from the data, the privacy models and the learning tasks. In this talk, I will use the Empirical Risk Minimization (ERM) problem as an example and show how to overcome these challenges. Particularly, I will first talk about how to overcome the high dimensionality challenge from the data for Sparse Linear Regression in the local DP (LDP) model. Then, I will discuss the challenge from the non-interactive LDP model and show a series of results to reduce the exponential sample complexity of ERM. Next, I will present techniques on achieving DP for ERM with non-convex loss functions. Finally, I will discuss some future research along these directions.

▶ About the Speaker

Di Wang is currently a PhD student in the Department of Computer Science and Engineering at the State University of New York (SUNY) at Buffalo. Before that, he obtained his BS and MS degrees in mathematics from Shandong University and the University of Western Ontario, respectively. During his PhD studies, he has been invited as a visiting student to the University of California, Berkeley, Harvard University, and Boston University. His research areas include differentially private machine learning, adversarial machine learning, interpretable machine learning, robust estimation and optimization. He has received the SEAS Dean's Graduate Achievement Award and the Best CSE Graduate Research Award from SUNY Buffalo.

ALL are welcome!

Enquiries : Professor George Baciu
Email : csgeorge@polyu.edu.hk
Tel : 2766 7272

We drive innovation through
SMART COMPUTING