PURDUE UNIVERSITY | Elmore Family School of Electrical and Computer Engineering

Securing Collaborative Learning Systems: Deep Learning Meets Cryptography

Zahra Ghodsi
University of California San Diego

Wednesday, March 9, 2022
10:30 AM • WANG 1004

Zoom info: https://purdue-edu.zoom.us/j/98236364959 ~ Meeting ID: 982 3636 4959

Abstract
Deploying modern deep learning in real world applications comes with several challenges. Due to high data and compute demand, several parties who have access to these resources are required to collaborate during training and deployment for a successful uptake. This collaboration however, raises immediate security concerns relating to the privacy of parties' assets, the integrity or correctness of computations, and the robustness of algorithms in the presence of accidental or intentional errors. I address these challenges by providing rigorous guarantees using cryptographic protocols in deep learning systems. Striving for practicality, I demonstrate the need for re-thinking both deep learning and cryptography, and argue for their co-design.

In this talk, I will discuss my research on bridging the existing gap between deep learning and cryptography. First, I will focus on privacy-preserving inference computation, and show that naive adoption of cryptographic protocols into existing models results in unexpected overheads. With this insight, I provide several optimization avenues that re-think the design of deep learning models. Next, I will address the integrity issues in outsourced inference, and develop specialized cryptographic protocols that provide correctness guarantees while significantly slashing costs. Finally, I will discuss my future plans on building efficient collaborative learning frameworks that enable untrusted parties to participate in training and deployment of machine learning systems.

Bio
Zahra Ghodsi is currently a Postdoctoral Scholar in the Department of Electrical and Computer Engineering at University of California San Diego. Previously, she received her Ph.D. from New York University, and her B.S. from Sharif University of Technology, both in Electrical Engineering. Her research interests lie at the intersection of security, privacy, and machine learning. During her doctoral studies, she was awarded the Ernst Weber Fellowship from New York University, and the AI Fellowship from J.P. Morgan. She was a recipient of the NYU Inclusive Excellence Award, and was nominated as an MIT EECS Rising Star in 2021. She has served on the artifact evaluation committee of ASPLOS 2021 and program committee of NDSS 2022.

Host: Professor Milind Kulkarni ~ milind@purdue.edu ~ Office (765) 494-1742