PURDUE UNIVERSITY | Elmore Family School of Electrical and Computer Engineering

Advances in Machine Learning over Encrypted Data and Beyond

Sherman Chow
Chinese University of Hong Kong

Monday, January 31, 2022
9:30 A.M. • Virtual

Zoom Meeting ~ https://purdue-edu.zoom.us/j/93167017860 ~ Meeting ID: 931 6701 7860

Abstract
Machine learning often involves sensitive data. It is desirable to preserve the privacy of all stakeholders, namely, querying clients, model owner, and training data contributors. State-of-the-art cryptographic solutions are still orders of magnitudes slower than plaintext inference and training. This talk shares new ideas targeting specific root causes of the problem. Beyond machine learning, we also briefly discuss their potentials in other pragmatic tasks involving fuzzy private computation.

Bio
Sherman Chow is an Associate Professor at The Chinese University of Hong Kong. He received the Early Career Award 2013/14 from the Hong Kong Research Grants Council. He was a research fellow at the Department of Combinatorics and Optimization, University of Waterloo, a position he commenced after receiving his Ph.D. degree from the Courant Institute of Mathematical Sciences, New York University. During his study, he interned at NTT Research and Development (Tokyo), Microsoft Research (Redmond), and Fuji Xerox Palo Alto Laboratory.

His main interests are Cryptography, Security, and Privacy, with publications in AsiaCrypt, CCS, EuroCrypt, ITCS, NDSS, S&P, and Usenix Security. He is a Deputy Editor of IET Information Security. He currently serves on the editorial boards of ACM Distributed Ledger Technologies and IEEE TDSC, and IEEE TIFS for 2015-19. He is a senior program committee member of PETS this year, a PC member of AsiaCrypt for 2012-17, and 200+ other conferences, including CCS, Crypto, Financial Crypt, Infocom, TheWeb, and Usenix Security.

Host: Professor Saurabh Bagchi, sbagchi@purdue.edu, 765-494-1741