In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Keeping the Biggest Data Safe

by

Professor Sen-ching Samson Cheung

College of Engineering, University of Kentucky, USA

Date : 10th December, 2018 (Mon)

Time : 2:00pm – 3:00pm

Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Multidimensional streaming signals like audio, videos, and multi-spectral imagery are truly the biggest of the Big Data. Collected by sensors at the network edge, these data often contain highly sensitive information and their misuse can lead to significant invasion of privacy. For example, networks of surveillance cameras have been used by some countries in tracking their citizens, and pervasive use of IoT devices in smart homes opens door to recording private behaviors and interactions. It is highly challenging to apply traditional privacy enhancing technologies to handle these data. Cryptographic techniques like homomorphic encryption and garbled circuits are too computationally intensive for any practical applications. The more efficient differential private schemes, on the other hand, rely on additive noise and may not be able to provide adequate protection on semantic contents.

In this talk, I will discuss a number of techniques developed in my research group to process multidimensional signals while ensuring their privacy. First, I will talk about how to exploit the nature of the signals in speeding up cryptographic computation. Specifically, I will focus on the optimized design of a garble-circuit based iris-code matching algorithm where we can achieve significant speedup using a common iris mask. Second, I will present the use of secret sharing as a faster and more convenient privacy platform for distributed signal computation. Secret sharing does not require key distribution and can achieve information theoretic security without long integer fields. However, secret sharing is prone to collusion attacks. I will present a peer-to-peer computational framework that combines cryptographic and game-theoretic countermeasures to prevent such attacks. Finally, I will discuss my recent work in using generative adversarial network (GAN) and random neural networks to protect signal privacy in distributed deep learning. We use GAN to learn the statistics of sensitive facial data at local sites and generate privacy-preserving synthetic data for public centralized learning. While GAN at network edge can be computationally intensive, random neural network offers a much lighter weight privacy-enhancing protocol suitable for a broad range of IoT applications.

Biography

Sen-ching "Samson" Cheung is a Professor of Electrical and Computer Engineering and the director of Multimedia Information Laboratory (Mialab) at University of Kentucky (UKY), Lexington, KY, USA. He is the endowed Blazie Family Professor of Engineering. He has held visiting positions at Cisco Systems, University of California at Davis, and the University of Michigan-Shanghai Jiao Tong University Joint Institute. Before joining UKY in 2004, he was a postdoctoral researcher with the Sapphire Scientific Data Mining Group at Lawrence Livermore National Laboratory that won the R&D 100 Award in 2006. He received his Ph.D. degree from University of California, Berkeley in 2002. He is a senior member of both IEEE and ACM. He has the fortune of working with a team of talented students and collaborators at Mialab in a number of areas in multimedia including video surveillance, privacy protection, encrypted domain signal processing, 3D data processing, virtual and augmented reality as well as computational multimedia for autism therapy. More details about current and past research projects at Mialab can be found at http://www.mialab.net .

**** ALL ARE WELCOME ****

Host: Professor CHEN Minghua (Tel: 3943-8452, Email: minghua@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)