THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering
Seminar

Secure Computations with Homomorphic Encryption and Multiparty Computation
by
Dr. Peizhao HU
Department of Computer Science, Rochester Institute of Technology (RIT), USA

Date : **15th August, 2018 (Wed)**
Time : **3:00pm – 4:00pm**
Venue : **Room 1009, William M.W. Mong Engineering Building**
            The Chinese University of Hong Kong

Abstract

Outsourcing data analytics tasks to the cloud is becoming more economical. But, concerns of data privacy limit what we can be computed in untrusted computing environments. Privacy-preserving techniques such as homomorphic encryption (HE) and secure multiparty computation (MPC) have attracted interests for supporting secure computations in various application scenarios, including credit assessment, genomic data analysis. Yet, using these techniques to develop practical systems requires careful designs. For example, in the case of HE we need to develop new methods to support evaluation of functions over ciphertexts encrypted under different keys. Or in the case of MPC we need methods to support the changing number of computing parties or joint evaluation over datasets that have been shared among different computing parties. This talk gives a brief overview of these problems and discusses some initial ideas toward these problems.

Biography

Peizhao Hu is an assistant professor in the department of computer science at Rochester Institute of Technology (RIT), NY, USA. Dr. Hu completed his PhD in computer science at the University of Queensland, Australia. Before joining RIT, he was a senior research engineer at NICTA, Australia (Now Data61 within CSIRO Australia). His research interests include techniques for secure computations (homomorphic encryption, secure multiparty computation), distributed systems (blockchain), pervasive computing, wireless networks.

** ALL ARE WELCOME **

Host: Sherman S.M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)

Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)