



THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Towards Verifiable Third-Party Computation

by

Professor Yong Guan
Department of Electrical and Computer Engineering
Information Assurance Center
Iowa State University
U.S.A.

Date : 24 April, 2015 (Friday)
Time : 3:30 – 4:30pm
Venue : Room 833 Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

The surging popularity of the cloud computing paradigm has rendered a new type of service: computation as a commodity (via outsourcing). While outsourcing computation brings appealing benefits, it introduces critical and challenging security and privacy issues. One such issue is that there is no guarantee on the correctness of the results returned by the 3rd-party server, which may be error-prone or otherwise not entirely trustworthy. Thus an immediate need for result assurance naturally arises. In the last couple of years, this need motivates a quickly growing and exciting body of research on verifiable computation, and in particular, works focused on the design of verification protocols for general-purpose computation, such as systems based on Interactive Proof (IP), Probabilistically Checkable Proof (PCP), and Quadratic Arithmetic Program (QAP). In this talk, we will go over the major recent results in the literature, present our recent work in distributed verification and dealing with repeated substructures, and conclude with future directions. Through this talk, we hope to stimulate more interests and potential collaborations on solid work in verifiable computing as well as other security and privacy, and digital forensics research.

Biography

Dr. Yong Guan is an Associate Professor of Electrical and Computer Engineering, and Associate Director for Research, Information Assurance Center at Iowa State University. He is also an Ames Lab associate for Midwest Forensics Resource Center at U.S. DoE's Ames Lab. He received his Ph.D. degree in Computer Science from Texas A&M University in 2002, MS and BS degrees in Computer Science from Peking University in 1996 and 1990, respectively. With the support of NSF, IARPA, ARO, and Boeing, his research focuses on security, privacy, and digital forensics. He served as the general chair of 2008 IEEE Symposium on Security and Privacy, co-organizer for ARO Workshop on Digital Forensics, General/Program Chairs for digital forensics workshops/conferences, and coordinator of Digital Forensics WG at NSA/DHS CAE IA Principals Meetings, and editor of IEEE Transactions on Information Forensics and Security and IEEE Transactions on Wireless Communication (Security area). Dr. Guan has been recognized by ISU Award for Early Achievement in Research, Litton Industries Professorship, NSF Career Award, and Outstanding Community Service Award of IEEE Technical Committee on Security and Privacy.

**** ALL ARE WELCOME ****