In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

by

Dr. Sherman S.M. Chow
University of Waterloo
Canada

Date : 6 April, 2011 (Wed.)
Time : 2:30-3:30pm
Venue : Rm 1009, William MW Mong Engineering Building
The Chinese University of Hong Kong

Abstract
Attribute based encryption (ABE) [Eurocrypt'05, CCS'06] determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase [TCC'07] gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user.

In this talk we first describe the application of ABE for fine-grained cryptographic access control of data with collusion resistance, which covers cloud storage and decentralized social network in particular. Then we will introduce our solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users. Some related subsequent works will also be discussed.

This is a joint work with Melissa Chase appeared in CCS '09.

Biography
Sherman Chow received his B.Eng. (first class honours) and M.Phil. degrees from the University of Hong Kong, and M.S. and Ph.D. degrees from Courant Institute of Mathematical Sciences, New York University. He is now a research fellow in the Department of Combinatorics and Optimization, University of Waterloo. During his doctoral study, he has been interning at NTT Research and Development (Tokyo), Microsoft Research (Redmond) and Fuji Xerox Palo Alto Laboratory, and visited the University of Texas at Austin, Massachusetts Institute of Technology and Queensland University of Technology. His research interests are applied cryptography, privacy and distributed systems security in general. He has been serving on the program committees of several international conferences on these topics.

**** ALL ARE WELCOME ****

Host: Professor Kwok-Wai Cheung (Tel: 2609-8348, Email: kwcheung@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 2609-8385)