In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Computer Science and Engineering
and Department of Information Engineering

Seminar

New Privacy-Preserving Architectures for Identity-/Attribute-Based Encryption

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

Date : 15 March, 2012 (Thur.)
Time : 11:00am-12:00noon
Venue : Room 833 Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract
Security and privacy of identity-based encryption (IBE) and attribute-based encryption (ABE) are hinged on the assumption that the authority which sets up the system is honest. Our work aims to reduce this trust assumption. IBE has an inherent limitation which is key escrow. A curious key generation center (KGC) can simply generate the user's private key and decrypt a ciphertext intended for that user. However, the KGC may be unable to decrypt the ciphertext if it does not know who the intended recipient of that ciphertext is. This property is studied by formalizing the notion of KGC anonymous ciphertext indistinguishability (ACI-KGC). We propose an IBE scheme with ACI-KGC in the standard model. None of the existing practical IBE schemes achieve this level of security. We also propose a new system architecture with an anonymous secret key generation protocol which enables the KGC to issue keys to authenticated users without knowing the list of users' identities. Our proposal can be viewed as mitigating the key escrow problem in a new direction.

For ABE, it is not realistic to trust a single authority to monitor all attributes. Distributing control over many attribute-authorities is desirable, but this introduces new privacy concerns. We propose a solution which removes the trusted central authority without compromising users' privacy, thus making ABE more usable in practice.

Biography
Sherman S.M. Chow is a post-doctoral research fellow at University of Waterloo, a position he commenced after receiving his Ph.D. degree from The Courant Institute of Mathematical Sciences, New York University. He interned at NTT Research and Development (Tokyo), Microsoft Research (Redmond) and Fuji Xerox Palo Alto Laboratory, and has made research visits to U. of Maryland, U. of Calgary, U. of Hong Kong, U. of Texas, MIT and Queensland University of Technology. These visits resulted in US patent applications and also in publications at major conferences such as CCS and EUROCRYPT. He serves on the program committees of several international conferences including ASIACRYPT 2012 and ACNS 2012. Apart from foundational topics in cryptography such as leakage-resilient (yet practical) cryptosystems, he is also interested in security/privacy issues of distributed systems such as vehicular network and distributed database, and achieving seemingly conflicting requirements in applications such as anonymous credentials and e-voting. Recently, he has been working on secure cloud computing and healthcare systems.

**** ALL ARE WELCOME ****

Host: Professor Dah-Ming Chiu (Tel: 3943-8357, Email: dmchiu@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)