

## Asymmetric Group Key Agreement

**Professor Yi Mu**  
Centre for Computer and Information  
Security Research,  
University of Wollongong, Australia



**Date :** 17 April 2009 (Friday)  
**Time :** 4.30 pm – 5.30 pm  
**Venue:** SPMS-Executive Classroom 1, MAS-03-06  
School of Physical and Mathematical Sciences

A group key agreement (GKA) protocol allows a set of users to establish a common secret via open networks. Observing that a major goal of GKAs for most applications is to establish a confidential channel among group members, we revisit the group key agreement definition and distinguish the conventional symmetric group key agreement from asymmetric group key agreement (ASGKA) protocols. Instead of a common secret key, only a shared encryption key is negotiated in an ASGKA protocol. This encryption key is accessible to attackers and corresponds to different decryption keys, each of which is only computable by one group member. We propose a generic construction of one-round ASGKAs based on a new primitive referred to as aggregatable signature-based broadcast (ASBB), in which the public key can be simultaneously used to verify signatures and encrypt messages while any signature can be used to decrypt cipher texts under this public key. Using bilinear pairings, we realize an efficient ASBB scheme equipped with useful properties. Following the generic construction, we instantiate a one-round ASGKA protocol tightly reduced to the decision Bilinear Diffie-Hellman Exponentiation (BDHE) assumption in the standard model.

### Speaker Biography

A/P Mu received his PhD from the Australian National University in 1994. Prior to joining the University of Wollongong, he was a senior lecturer in the Department of Computing, Macquarie University. He also worked in the Department of Computing and IT, University of Western Sydney as a lecturer. He has been with the University of Wollongong since 2003. His current research interest includes cryptography, network security, electronic payment, access control, and computer security. He has also previously worked in the areas of quantum cryptography, quantum computers, atomic computations, and quantum optics. He has published over 200 research papers. A/P Mu is the Editor-in-Chief of the International Journal of Applied Cryptography and serves as Editor or Guest Editor for many international journals. He has served in the program committees for a number of international security conferences, including ACM CCS, ACM AisaCCS, ESORICS, ACISP, CANS, EuroPKI, ICICS, ICISC, ProvSec, ISPEC etc. He is also a senior member of the IEEE and a member of the IACR.

Host: Prof. Wang Huaxiong, Division of Mathematical Sciences, School of Physical and Mathematical Sciences

Queries to: Prof. Wang Huaxiong, [hxwang@ntu.edu.sg](mailto:hxwang@ntu.edu.sg), Tel: 6513 7472

### **SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES**

NANYANG TECHNOLOGICAL UNIVERSITY

SPMS-MAS-03-01, 21 NANYANG LINK, SINGAPORE 637371

FAX: +65 6515 8213 TEL: +65 6513 7423