

# COMPUTER SCIENCE SEMINAR SERIES

Department of Computer Science  
City University of Hong Kong  
(Departmental Seminar Seminar 2006/2007 - No 67)

## Nominative Signature from Ring Signature

Miss CHANG Shuang  
MPhil Student  
Department of Computer Science  
City University of Hong Kong

**Date :** 13 July 2007 (Friday)

**Time :** 2:00pm-3:00pm

**Venue :** CS Seminar Room, Rm Y6405, 6th Floor Yellow Zone, Academic Building, City University of Hong Kong, Tat Chee Avenue, Kowloon Tong.

### Abstract

A nominative signature (NS) involves three parties: nominator A, nominee B and verifier C. The nominator arbitrarily chooses a message and works jointly with the nominee to produce a signature called nominative signature. The validity of the signature can only be verified by B and if it is valid, B can convince the verifier C the validity of the signature using a confirmation protocol; otherwise, B can convince C the invalidity of it using a disavowal protocol. Due to the special property of NS that the nominator cannot convince anyone about the validity of a nominative signature while only the nominee can, NS has been found to be very useful for implementing user certification systems.

There have been a handful of schemes proposed and almost all of them have been found flawed. The only one which is secure requires multi-round of communications between the nominator and the nominee for signature generation.

So in this presentation, I will briefly introduce nominative signature and its application, and then present our novel construction derived from ring signature which is efficient and requires only one-move communication for signature generation. At the end I will analyze its security and performance.

This paper will be presented in the 2nd International Workshop on Security (IWSEC2007), October 29-31, 2007.

Supervisor: Dr Duncan Wong (CS)  
Research Interests: Applied cryptography, information security

**All are welcome!**

\* \* \* \* \*

*In case of questions, please contact Dr Duncan Wong at Tel: 2788 8020, E-mail: [duncan@cityu.edu.hk](mailto:duncan@cityu.edu.hk), or visit the CS Departmental Seminar Web at <http://www.cs.cityu.edu.hk/>.*