

COMPUTER SCIENCE SEMINAR SERIES

Department of Computer Science
City University of Hong Kong
(Departmental Seminar Seminar 2006/2007 - No 61)

A More Efficient Convertible Nominative Signature

Mr LIU Yan Wang Dennis
MPhil Student
Department of Computer Science
City University of Hong Kong

Date : 18 June 2007 (Monday)

Time : 3:00pm-3:30pm

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

Abstract

Nominative signature provides an interesting share of power between a nominator and a nominee in which a nominative signature, generated jointly by the nominator and the nominee, can only be verified with the aid of the nominee. In this paper, we propose a new construction of nominative signature which has a higher network efficiency than the existing one (Liu et al., 2007). In addition, our scheme is the first one supporting nominee-only conversion. We also enhance the security model of nominative signature for capturing this new property.

This paper is to appear in the International Conference on Security and Cryptography (SECRYPT 2007).

Supervisor: Dr Duncan Wong (CS)
Research Interests: Applied Cryptography and Digital Signatures

All are welcome!

* * * * *

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