

COMPUTER SCIENCE SEMINAR SERIES

Department of Computer Science
City University of Hong Kong
(Departmental Seminar Seminar 2006/2007 - No 57)

An Efficient Signcryption Scheme with Key Privacy

Mr LI Chung Ki
MPhil Student
Department of Computer Science
City University of Hong Kong

Date :

25 May 2007 (Friday)

Time :

2:30pm-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

In Information Processing Letters 2006, Tan pointed out that the anonymous signcryption scheme proposed by Yang, Wong and Deng (YWD) in ISC 2005 provides neither confidentiality nor anonymity. However, no discussion has been made on whether YWD scheme can be made secure. In this paper, we propose a modification of YWD scheme which resolves the security issues of the original scheme without sacrificing its high efficiency and simple design. Indeed, we show that our scheme achieves confidentiality, existential unforgeability and anonymity with more precise reduction bounds. In addition, our scheme further improves the efficiency when compared with YWD, with reduced number of operations for both signcryption and de-signcryption.

This paper will be presented in the 4th European PKI Workshop (EUROPKI '07), June 28-30, 2007.

Supervisor: Dr Duncan Wong (CS)

Research Interest: Signcryption

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/>.