In Favour of Posting

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

Joint Seminar

Concurrent Security

by

Ms. Rachel Huijia Lin
Department of Computer Science
Cornell University
U.S.A.

Date : 21 March, 2011 (Mon.)
Time : 11:00am – 12:00noon
Venue : Room 1009, William M.W. Mong Engineering Building
The Chinese University of Hong Kong

Abstract

Cryptographic protocols have been developed for a variety of tasks, including electronic auctions, electronic voting systems, privacy preserving data mining and more. The Internet allows for the concurrent execution of cryptographic protocols. Such concurrency severely challenges their security.

In this talk we introduce a novel technique for transforming any "stand-alone" secure protocol (i.e., one whose security is only guaranteed if executed in isolation) into one that is secure under concurrent executions. Contrary to previous results in the literature, this result is established without relying on additional trusted infrastructure or cryptographic hardness assumptions.

Biography

Huijia Lin is a Ph.D. candidate in the Department of Computer Science at Cornell. Her research interests are in the field of Cryptography. She is a recipient of the Microsoft Graduate Student Fellowship.

***** ALL ARE WELCOME *****

Host: Professor Dah-Ming Chiu (Tel: 2609-8357, Email: dmchiu@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 2609-8385)