In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

Lecture on

Elliptic Curve Cryptography

Jointly organized by Faculty of Engineering and ITCSC

March 23 – April 14, 2010

By

Prof. Rong-Jaye Chen

Professor, Computer Science Department, National Chiao Tung University, Taiwan

Mar 23, Tue	**2:30-4:30pm**	**Lecture on "Elliptic Curve Cryptography"**
Mar 31, Wed	**2:30-4:30pm**	**Tutorial class**
Apr 7, Wed	**2:30-4:30pm**	**Tutorial class**
Apr 14, Wed	**2:30-4:30pm**	**Tutorial class**
Venue:	**Room. 121, Ho Sin Hang Engineering Building, CUHK**	

Abstract:
Elliptic curve cryptography (ECC) is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was first proposed by Koblitz and Miller in 1985. Their motivation for using ECC is the fact that there is no known sub-exponential algorithm to solve the discrete logarithm problem on an elliptic curve. Cryptosystems based on elliptic curves apply the smaller key sizes to attain the same level of security as RSA. This makes them ideal for use in smart cards and other environments where resources such as storage, time, or power are limited.

Pairings in ECC are functions which map a pair of elliptic curve points to an element of the multiplicative group of a finite field. Pairings have been used to support a wide range of cryptographic applications. Pioneering works in this area are Sakai, Ohgishi, and Kasahara's pairing based key agreement and signature schemes(2000); Joux's three-party key agreement(2000); and Boneh and Franklin's identity-based encryption(2001).

In this talk, we will address how elliptic curve cryptosystems apply the smaller key sizes, how elliptic curves can be extended to hyperelliptic curves, and also various applications of pairing-based cryptography(PBC).

Biography:
Rong-Jaye Chen received the B.S. degree in mathematics from Taiwan Tsing Hua University in 1977 and the Ph.D. degree in computer science from the University of Wisconsin-Madison in 1987. He is currently a professor of computer science department at Taiwan Chiao Tung University. His research interests include elliptic curve cryptography, cryptography and security, coding theory, algorithm design, and mathematical programming.

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

Hosted by: Prof. Peter T.S.Yum Tel: 26098386
Enquiries : Institute of Theoretical Computer Science and Communications Tel: 2696 1257