清华大学高等研究院

Institute for Advanced Study, Tsinghua University

密码学学术报告 Cryptology Seminars

Title: **RECENT DEVELOPMENTS ON TWO PROBLEMS CONCERNING MULTIPLICATIVE GROUPS OF FINITE FIELDS**

Speaker: **Prof. MING-DEH HUANG**
(UNIVERSITY OF SOUTHERN CALIFORNIA)

Time: **9:00am, Thursday, June 13, 2013**
(8:30~9:00am, Tea, Coffee, and Cookie)

Venue: **Conference Hall 322, Science Building, Tsinghua University**

Abstract

In this talk we discuss recent developments on two problems concerning multiplicative groups of finite fields Fpn where p is a prime: the discrete logarithm problem and the problem of finding primitive elements (a generator for the multiplicative group). The first part of the talk discusses a recent announcement of Joux's heuristically L(1/4) method for discrete logarithms over finite fields. In the second part we describe a deterministic algorithm for finding a primitive element for the finite field. The algorithm relies on a relation generation technique in Joux's method. Based on a heuristic assumption, the algorithm finds a primitive element in time polynomial in p and n. It can also be shown unconditionally that in time polynomial in p and n, the algorithm either outputs an element that is provably a generator or declares that it has failed in finding one.