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: **Weil descent, last fall degree and the elliptic curve discrete logarithm problem**

Speaker: **Ming-Deh Huang (*University of Southern California*)**

Time: 2015年7月28日（周二） 下午2:00

Venue: 清华大学 高等研究院（科学馆）213 报告厅

Abstract

The elliptic curve discrete logarithm problem (ECDLP) is a computational problem that has many applications in cryptography. Its computational complexity is an interesting and important problem in its own right. After an overview of different approaches in the study of this problem we will focus our attention on the Weil descent approach. In this context we will discuss theoretical works on last fall degrees, which cast serious doubt on recent claims of heuristic subexponential Weil descent attacks on the ECDLP in finite fields of small characteristics.