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: **Window τ-NAF for Koblitz Curves with Optimal Pre-Computation**

Speaker: **Prof. Guangwu Xu**
（*University of Wisconsin-Milwaukee, USA*）

Time: **9:00am, Thursday, Jan 9, 2014**

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

Abstract

Elliptic curve cryptography has the advantage of achieving the same security with smaller key sizes. It has been deployed in many important applications, e.g., Bitcoin, SSH, TLS, and smart card.

In this talk, we shall focus on the arithmetic of the standard Koblitz curves. Special attention will be given to sparse τ-adic expansion for scalar multiplication. Existence and generalization of such expansion will be discussed. Optimal precomputation for the associated scalar multiplication will be described.

(Contains joint work with I. Blake and K. Murty, and with Trost)

Brief bio: Guangwu Xu received his Ph.D. in mathematics from SUNY Buff alo. He is now with the Department of EE & CS, University of Wisconsin-Milwaukee. His research interests include cryptography and information security, computational number theory, compressed sensing, algorithms, and functional analysis.