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 (II)**

Speaker: **Prof. Guangwu Xu**
Department of EE & CS
University of Wisconsin-Milwaukee, USA

Time: **3:00pm, Wednesday, July 16, 2014**

Venue: **Conference Hall 213, Science Building, Tsinghua University**

Abstract

Elliptic curve cryptography (ECC) 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.

Koblitz curves are one of the most important classes of curves in ECC. This class of curves enjoys a very efficient scalar multiplication algorithm-the window τ-NAF method. In this talk, we shall focus on the precomputation procedure of the window τ -NAF for the standard Koblitz curves. Setup of the precomputation will be introduced, a p-adic characterization of power divisibility will be presented. Finally, optimal precomputation schemes for window τ -NAF will be described and proved.

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

Brief bio: Guangwu Xu received his Ph.D. in mathematics from SUNY Buffalo. 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.