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: **An Exponential Sum for Coset: Refinements and Applications**

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

Time: **9:00am, Tuesday, July 2, 2013**
(8:30~9:00am, Tea, Coffee, and Cookie)

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

Abstract

For a nontrivial multiplicative character over a finite field, Katz established an upper bound for the magnitude of summation of the character values over a special coset of the base field (as an additive subgroup of the field in consideration). In the first part of the talk, we shall describe a refinement of the Katz' estimation by showing that either the upper bound is achieved or the character sum is -1, for quadratic extension. The second part discusses how to use Katz' estimation to construct partial Fourier matrices that are well behaved compressed sensing matrices, in a deterministic manner. Finally, we shall use our refinement to the construction of sparse representation of signals in a union of orthonormal bases which has been a topic of some studies. This construction produces an approximately mutually unbiased bases which is of particular interest in quantum information theory.

(This talk contains joint work with Zhiqiang Xu)