# The University of Chicago

# Department of Computer Science & Mathematics

# Combinatorics & Theoretical Seminar



PRESENTS:

**Youming Qiao**

**University of Technology, Sydney**

http://itcs.tsinghua.edu.cn/youmingqiao/

“Isometry testing of Hermitian bilinear maps via \*-algebras”

Abstract:

Let F be a finite field of odd characteristic. Suppose we are given two tuples of n by n symmetric (resp. skew-symmetric) matrices vB=(B\_1, ..., B\_m) and vC=(C\_1, ..., C\_m) over F. vB and vC are isometric, if there exists an invertible matrix A such that for every i in [m], A^tB\_iA=C\_i. We present an efficient randomized algorithm to test whether vB and vC are isometric, in time polynomial in n, m, and log |F|. This algorithm is achieved by working with the underlying \*-algebra (algebras with an anti-automorphism of order 2) of this problem.

Our algorithm breaks an authentication protocol based on 1-sided isomorphism of quadratic forms, proposed by Patarin in 1990's. It also has certain consequence on isomorphism testing of p-groups of class 2 and exponent p, where p is odd.

Joint work with Gábor Ivanyos.

**Tuesday, November 29, 2016**

**3:00 pm**

**Ryerson 251**

**Host: Prof. Laszlo Babai**

\*Refreshments during the talk\*