

*Department of Mathematics,
University of California, San Diego*

Math 295 - Mathematics Colloquium

Kristin Lauter

Microsoft Research

Applications of Ramanujan graphs in Cryptography.

Abstract:

This talk will explain a new construction of secure cryptographic hash functions from Ramanujan graphs. First we will explain cryptographic hash functions and the importance of the collision-resistance property. After a brief overview of expander graphs, we will give a construction of provable collision resistant hash functions from expander graphs in which finding cycles is hard.

As an example, we give a family of optimal expander graphs for provable collision resistant hash function constructions: the family of Ramanujan graphs constructed by Pizer. Pizer described a family of Ramanujan graphs, where the nodes of the graph are isomorphism classes of supersingular elliptic curves over F_p^2 , and the edges are n -isogenies, n a prime different from p . When the hash function is constructed from one of Pizer's Ramanujan graphs, then collision resistance follows from hardness of computing isogenies between supersingular elliptic curves.

Joint work with Denis Charles and Eyal Goren

Host: AWM

Monday, May 12, 2008

4:00 PM

AP&M 6402
