abstract

COMPUTER SCIENCE/DISCRETE MATH, I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

I will talk about a family of graphs which originally arose in cryptography, in studying the difficulty of the discrete logarithm problem on elliptic curves.

These graphs can be shown to be expanders, assuming the generalized Riemann hypothesis (GRH) for Hecke's grossencharacter L-functions. From this one can deduce a random reducibility result for the discrete logarithm problem on the types of elliptic curves that are used in cryptographic applications. The rapid mixing of the random walk on these graphs had previously been assumed in a number of recent attacks on elliptic curve cryptosystems. One application of our estimates of the graph eigenvalues is to give useful, explicit bounds for these mixing times. The graphs themselves represent a new (conditional) construction of expanders, which can be used for other applications. (Joint work with Ramarathnam Venkatesan and David Jao, Microsoft Research Cryptography and Anti-Piracy Group.)