abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

This work attempts to broaden the foundations of public-key cryptography. We construct a new public key encryption based on two □hardness on average□ assumptions:

(1) it is hard to □learn parity with noise□ for random sparse equations; and

(2) it is hard to approximate the vertex expansion of random unbalanced bipartite graphs.

Most, if not all, previous constructions of public key encryption used hardness assumptions with significant algebraic structure. Our new assumptions, positing indistinguishably from uniform of certain natural distributions on instances of NP-complete problems, seem relatively unstructured and qualitatively different from previous ones.

We give some evidence for these assumptions by studying their resistance to certain natural algorithms, and relating them to variants of more widely studied assumptions such as the hardness of the □search version□ of learning parity with noise and the planted clique problems.

Joint work with Boaz Barak and Avi Wigderson.