# abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In this work we study the task of randomness extraction from sources which are distributed uniformly on an unknown algebraic variety. In other words, we are interested in constructing a function (an extractor) whose output is close to uniform even if the input is drawn uniformly from the set of solutions of an unknown system of low degree polynomials. This problem generalizes the problem of extraction from affine sources which has drawn a considerable amount of attention recently.

In this talk I will show two constructions of explicit extractors for varieties. The first works for varieties of any size (including one dimensional varieties, or curves) and requires field size which is exponential in the overall dimension of the space. the second extractor allows the field size to be polynomial in the degree of the equations defining the variety, but works only for varieties whose size is at least the square root of the total size of the space.