abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The security of several cryptosystems is based on our apparent inability to solve the following computational problem: given as input a basis B for a lattice and a target vector t , find the lattice point closest to t. This problem, referred to as the Closest Vector Problem (CVP), is not only NP-hard, it is hard to approximate to a factor better than 2^{log n/loglog n}, where n is the dimension of the lattice.
However, in several cryptographic applications, B is known in advance and can be pre-processed arbitrarily. Thus, the security of such a cryptosystem actually relies on the following pre-processing version of CVP, called CVPP: here B can be pre-processed arbitrarily and the input consists just of t. Could CVPP be much easier than CVP? For instance, one can compute the shortest vector in the lattice generated by B, a NP-hard problem, for free. Indeed, it was shown by Ahoronov and Regev how to approximate CVPP to within about \sqrt{n} factor; compare this to the best known approximation factor for CVP, which is roughly 2^n.
In this talk I will outline a result with Subhash Khot and Preyas Popat which shows that CVPP is hard to approximate to within a factor of 2^{(log n)^(1-\epsilon)} unless NP is contained in quasi-poly time. Thus, knowing the lattice in advance may not compromise the cryptosystem. A similar result is proved in the setting of error correcting codes where one wants to understand the complexity of decoding when the generator for the code is known in advance and can be pre-processed.