“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Christopher J Peikert

(Georgia Institute of Technology)

“The Geometry of Rings.”

Nov 1, 12:00pm (New York Time).

Abstract:

Recent years have seen many exciting developments in lattice cryptography, including the development of schemes whose efficiency is comparable to that of traditional number-theoretic ones, and the construction of fully homomorphic encryption. Both of these developments have centrally relied on algebraically structured "ideal lattices" in polynomial rings.

A key technical challenge in the design of any lattice-based scheme (especially homomorphic encryption) is to bound the growth of (small) "noise" terms under operations like addition, multiplication, and round-off. Unfortunately, in many important rings the most obvious ways of doing this gives very loose bounds, which significantly harms security and efficiency.

In this talk I will discuss an alternative way of viewing rings geometrically, using classical tools from algebraic number theory. This view lends itself to simple, tight bounds on noise growth, along with some unexpected gains in algorithmic simplicity and computational efficiency.

Next presentation: **TBA**

Algebraic Cryptography Center