“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Andrej Bogdanov

(The Chinese University of Hong Kong)

”Homomorphic encryption from codes.″

Feb 09, 9:00am (New York Time).

Abstract:

I will talk about a proposal of a new cryptographic system (from joint work with Chin Ho Lee) that supports (layered) homomorphic circuit evaluation. The security of this system is based on the hardness of decoding under random noise in certain families of codes.

Our design achieves "proto-homomorphic" properties in an elementary manner: message addition and multiplication are emulated by pointwise addition and multiplication of the ciphertext vectors. Moreover, the extremely simple nature of our decryption makes the scheme easily amenable to bootstrapping. However, some complications are caused by the inherent presence of noticeable encryption error. If time permits, I will describe some techniques we developed to handle this error in the homomorphic evaluation process, which is the main technical contribution of our work.

Next presentation: **Feb 23, 2012.** Algebraic methods to solve lattice problems
Jintai Ding (University of Cincinnati)

Algebraic Cryptography Center