“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

William Skeith

(The City College of New York)

"New Learning Problem with Applications to Cryptography."

Apr 27, 12:00am (New York Time).

Abstract:

We propose a generalization of the learning parity with noise (LPN) and learning with errors (LWE) problems to an abstract class of group-theoretic learning problems. The general formulation supports instantiations based on non-abelian groups, resulting in a new avenue for the application of combinatorial group theory to the development of cryptographic primitives. We then study a particular instantiation using relatively free groups, and construct a symmetric-key cryptosystem based upon it.

Joint work with Gilbert Baumslag, Nelly Fazio, Antonio Nicolosi, and Vladimir Shpilrain.

Next presentation: **May 11, 2011. New Algorithms for Learning in Presence of Errors**
Rong Ge (Princeton University)

Algebraic Cryptography Center