“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

William Skeith

(The City College of CUNY)

″Random Self-Reducibility Properties of Learning Problems over Burnside Groups of Exponent 3.″

Sep 29, 12:00pm (New York Time).

Abstract:

In this work we investigate the hardness of a computational problem introduced in the recent work of Baumslag et al. In particular, we study the B_n-LHN problem, which is a generalized version of the learning with errors (LWE) problem, instantiated with a particular family of non-abelian groups (free Burnside groups of exponent 3). In our main result, we demonstrate a random self-reducibility property for B_n-LHN. Along the way, we also prove a sequence of lemmas regarding homomorphisms of free Burnside groups of exponent 3 that may be of independent interest.

Next presentation: Oct 13. Marcus Lohrey *(University of Leipzig). Title:* **TBA**

Algebraic
Cryptography
Center