# Cryptology ePrint Archive: Report 2011/398

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

*Nelly Fazio and Kevin Iga and Antonio Nicolosi and Ludovic Perret and William E. Skeith III*

**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.

**Category / Keywords:** foundations / Random self-reducibility. Learning with errors. Post-quantum cryptography. Non-commutative cryptography. Burnside groups.

**Date:** received 25 Jul 2011, last revised 3 Feb 2012

**Contact author:** wes at cs ccny cuny edu

**Available formats:** PDF | BibTeX Citation

**Version:** 20120203:224135 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

[ Cryptology ePrint archive ]