Cryptology ePrint Archive: Report 2011/357

Generalized Learning Problems and Applications to Non-Commutative Cryptography

Gilbert Baumslag and Nelly Fazio and Antonio R. Nicolosi and Vladimir Shpilrain and William E. Skeith III

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 that we term _learning homomorphisms from noise_ (LHN). This class of problems contains LPN and LWE as special cases, but is much more general. It allows, for example, 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 cryptosystem based upon it.

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

Date: received 3 Jul 2011

Contact author: fazio at cs ccny cuny edu

Available formats: PDF | BibTeX Citation

Version: 20110704:062133 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]