Micciancio, Daniele; **Mol, Petros**

Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions.
(English) Zbl 1287.94085

Rogaway, Phillip (ed.), Advances in cryptology – CRYPTO 2011. 31st annual cryptology conference, Santa Barbara, CA, USA, August 14–18, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-22791-2/pbk). Lecture Notes in Computer Science 6841, 465-484 (2011).

Summary: We study the pseudorandomness of bounded knapsack functions over arbitrary finite abelian groups. Previous works consider only specific families of finite abelian groups and 0-1 coefficients. The main technical contribution of our work is a new, general theorem that provides sufficient conditions under which pseudorandomness of bounded knapsack functions follows directly from their one-wayness. Our results generalize and substantially extend previous work of *R. Impagliazzo* and *M. Naor* [J. Cryptology 9, No. 4, 199–216 (1996; Zbl 0862.94015)].

As an application of the new theorem, we give sample preserving search-to-decision reductions for the Learning With Errors (LWE) problem, introduced by [*O. Regev*, Proc. 37th annual ACM symposium on theory of computing, STOC 2005. New York, NY: ACM Press, 84–93 (2005; Zbl 1192.94106)] and widely used in lattice-based cryptography. Concretely, we show that, for a wide range of parameters, m LWE samples can be proved indistinguishable from random just under the hypothesis that search LWE is a one-way function for the same number m of samples.

For the entire collection see [Zbl 1219.94002].

MSC:

94A60 Cryptography
62B10 Statistical aspects of information-theoretic topics

Full Text: DOI