Cryptology ePrint Archive: Report 2011/521

Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions

Daniele Micciancio and Petros Mol

Abstract: We study under what conditions the conjectured one-wayness of the knapsack function (with polynomially bounded inputs) over an arbitrary finite abelian group implies that the output of the function is pseudorandom, i.e., computationally indistinguishable from a uniformly chosen group element. Previous work of Impagliazzo and Naor (J. Cryptology 9(4):199-216, 1996) considers only specific families of finite abelian groups and uniformly chosen random \emph{binary} inputs. Our work substantially extends previous results and provides a much more general reduction that applies to arbitrary finite abelian groups and input distributions with polynomially bounded coefficients. As an application of the new result, we give \emph{sample preserving} search-to-decision reductions for the Learning With Errors (LWE) problem, introduced by Regev (J. ACM 56(6):34, 2009) and widely used in lattice-based cryptography.

Category / Keywords: foundations /

Publication Info: A preliminary version of this work appears in the Proceedings of CRYPTO 2011. This is the full version of the paper.

Date: received 23 Sep 2011, last revised 26 Sep 2011

Contact author: pmol at cs ucsd edu