Cryptology ePrint Archive: Report 2013/098

Learning with Rounding, Revisited: New Reduction, Properties and Applications

Joel Alwen and Stephan Krenn and Krzysztof Pietrzak and Daniel Wichs

Abstract: The learning with rounding (LWR) problem, introduced by Banerjee, Peikert and Rosen [BPR12] at EUROCRYPT '12, is a variant of learning with errors (LWE), where one replaces random errors with deterministic rounding. The LWR problem was shown to be as hard as LWE for a setting of parameters where the modulus and modulus-to-error ratio are super-polynomial. In this work we resolve the main open problem of [BPR12] and give a new reduction that works for a larger range of parameters, allowing for a polynomial modulus and modulus-to-error ratio. In particular, a smaller modulus gives us greater efficiency, and a smaller modulus-to-error ratio gives us greater security, which now follows from the worst-case hardness of GapSVP with polynomial (rather than super-polynomial) approximation factors.

As a tool in the reduction, we show that there is a ``lossy mode" for the LWR problem, in which LWR samples only reveal partial information about the secret. This property gives us several interesting new applications, including a proof that LWR remains secure with weakly random secrets of sufficient min-entropy, and very simple new constructions of deterministic encryption, lossy trapdoor functions and reusable extractors.

Our approach is inspired by a technique of Goldwasser et al. [GKPV10] from ICS '10, which implicitly showed the existence of a ``lossy mode" for LWE. By refining this technique, we also improve on the parameters of that work to only requiring a polynomial (instead of super-polynomial) modulus and modulus-to-error ratio.

Category / Keywords: foundations / Learning with Errors, Learning with Rounding, Lossy Trapdoor Functions, Deterministic Encryption

Date: received 21 Feb 2013

Contact author: wichs at ccs neu edu