Cryptology ePrint Archive: Report 2013/164

Provably Secure LWE-Encryption with Uniform Secret

Daniel Cabarcas and Florian Göpfert and Patrick Weiden

Abstract: In this paper we present the (to the best of our knowledge) first LWE-based encryption scheme that removes the need of Gaussian sampling for the error, i.e. the discrete Gaussian distribution is replaced by the uniform distribution on a (small) set, which at the same time preserves the underlying worst-case hardness. This shows that provable security and efficiency do not necessarily have to mutually exclude each other. We give an asymptotic parameter instantiation for our scheme, as well as some hardness results for LWE which might be of independent interest.

Category / Keywords: public-key cryptography / LWE, Encryption, Lattice-Based Cryptography

Date: received 21 Mar 2013

Contact author: pweiden at cdc informatik tu-darmstadt de