Cryptology ePrint Archive: Report 2012/714

Sampling Discrete Gaussians Efficiently and Obliviously

Shweta Agrawal and Craig Gentry and Shai Halevi and Amit Sahai

Abstract: In this work we construct an algorithm for sampling Discrete Gaussians efficiently and obliviously. Previously discrete Gaussian samplers have been constructed in \cite{GPV08, Pei10}, where the algorithms take as input a ``high quality'' basis and produce an output whose quality depends on the input basis quality. Our algorithm produces a discrete Gaussian of somewhat worse quality than \cite{GPV08,Pei10} but with the advantage that it does not require access to an explicit description of the underlying lattice, for example it suffices for our purposes to have encryptions of lattice vectors under an additively homomorphic encryption scheme. At the heart of our work is the fundamental question {\it how do sums of discrete Gaussians behave?} Unlike their continuous counterparts, discrete Gaussians are not that well understood. We believe that our work fills in some important gaps of this understanding. Our results are already important in enabling the exciting new work on multilinear maps \cite{GGH12}, and since the questions we resolve arise naturally, we believe that our work will find application in other areas as well.

Category / Keywords: public-key cryptography / discrete Gaussians, sampling algorithm, lattices

Date: received 20 Dec 2012, last revised 25 Dec 2012

Contact author: shweta at cs ucla edu