Cryptology ePrint Archive: Report 2013/039

Creating a Challenge for Ideal Lattices

Thomas Plantard and Michael Schneider

Abstract: Lattice-based cryptography is one of the candidates in the area of post-quantum cryptography. Cryptographic schemes with security reductions to hard lattice problems (like the Shortest Vector Problem SVP) offer an alternative to recent number theory-based schemes. In order to guarantee asymptotic efficiency, most lattice-based schemes are instantiated using polynomial rings over integers. These lattices are called 'ideal lattices'. It is assumed that the hardness of lattice problems in lattices over integer rings remains the same as in regular lattices. In order to prove or disprove this assumption, we instantiate random ideal lattices that allow to test algorithms that solve SVP and its approximate version. The Ideal Lattice Challenge allows online submission of short vectors to enter a hall of fame for full comparison. We adjoin a set of first experiments and a first comparison of ideal and regular lattices.

Category / Keywords: implementation / Lattice-Based Cryptography, Ideal Lattices, Cyclotomic Rings, Lattice Challenge

Date: received 26 Jan 2013

Contact author: mischnei at cdc informatik tu-darmstadt de