MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Finding a Short Nonzero Lattice Vector

Authors: Richard Lindner, Markus Rueckert, Paul Baumann, Leo Nobach

February 2011

Introduction

Lattices are regular pointsets in real vector space. They consist of all integral combinations of a given tuple of linearly independent basis vectors, which is simply called a basis.
The most studied computational problem in lattice theory is that given such a basis you are asked to find the shortest nonzero lattice vector (SVP) or a good approximation thereof.

For the context of this challenge, "ciphertext" will always be a lattice base and "plaintext" will always be nonzero lattice vectors, which are sufficiently short in the Euclidean norm.

Being able to solve SVP has a multitude of applications. It can be used to model many real world problems including several from the field of integer programming. The exact problem (without approximation) is NP-hard under randomized reductions and unlikely to be easily solvable.

Building upon a popular paper by Ajtai [Ajtai], we have constructed lattice bases for which the solution of SVP implies a solution of SVP in all lattices of a certain smaller dimension. This does not mean that one can solve all instances simultaneously, but rather that one can solve even the worst case instances. We think these lattice bases are hard instances and most fitting to test and compare modern lattice basis reduction algorithms.

The Challenge

We show how these lattice bases were constructed and prove the existence of short vectors in each of the corresponding lattices in [BLR]. We challenge everyone to try by whatever algorithm to find a nonzero short vector in the basis given in the additional file *Ciphertext.txt*. Here, the first line is the dimension of the lattice basis, the second line is the maximum norm of the searched vector and the third line is the modulus.

This challenge is only an introduction to the area of lattice problems, for more intricate challenges, please visit

`http://www.latticechallenge.org`

References

Ajtai: Generating Hard Instances of Lattice Problems, STOC 1996

http://portal.acm.org/citation.cfm?id=237838

Buchmann, Lindner, Rueckert: Explicit Hard Instances of the Shortest Vector Problem, PQCrypto 2008

http://eprint.iacr.org/2008/333