Cryptology ePrint Archive: Report 2011/153

Lower bounds of shortest vector lengths in random knapsack lattices and random NTRU lattices

Jingguo Bi and Qi Cheng

Abstract: Finding the shortest vector of a lattice is one of the most important problems in computational lattice theory. For a random lattice, one can estimate the length of the shortest vector using the Gaussian heuristic. However, no rigorous proof can be provided for some classes of lattices, as the Gaussian heuristic may not hold for them. In the paper we study two types of random lattices in cryptography: the knapsack lattices and the NTRU lattices. For random knapsack lattices, we prove lower bounds of shortest vector lengths, which are very close to lengths predicted by the Gaussian heuristic. For a random NTRU lattice, we prove that with a overwhelming probability, the ratio between the length of the shortest vector and the length of the target vector, which corresponds to the secret key, is at least a constant, independent of the dimension of the lattice. The main technique we use is the incompressibility method from the theory of Kolmogorov complexity.

Category / Keywords: public-key cryptography / Shortest vector problem , Kolmogorov complexity , Knapsack lattice, NTRU lattice

Date: received 28 Mar 2011

Contact author: bijingguo-001 at 163 com; qcheng@cs ou edu

Available formats: PDF | BibTeX Citation

Version: 20110329:190519 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]