Cryptology ePrint Archive: Report 2011/525

A Note on the Density of the Multiple Subset Sum Problems

Yanbin Pan and Feng Zhang

Abstract: It is well known that the general subset sum problem is NP-complete. However, almost all subset sum problems with density less than $0.9408\ldots$ can be solved in polynomial time with an oracle that can find the shortest vector in a special lattice. In this paper, we give a similar result for the multiple subset sum problems which has k subset sum problems with the same solution. Some extended versions of the multiple subset sum problems are also considered. In addition, a modified lattice is involved to make the analysis much simpler than before.

Category / Keywords: Lattice, Low-Density, Multiple Subset Sum Problem, Multiple Modular Subset Sum Problem.

Date: received 25 Sep 2011, last revised 17 Oct 2011

Contact author: panyanbin at amss ac cn

Available formats: PDF | BibTeX Citation

Version: 20111018:022234 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]