Yamaguchi, Junpei; **Yasuda, Masaya**

Explicit formula for Gram-Schmidt vectors in LLL with deep insertions and its applications.

(English) Zbl 1423.94115

Kaczorowski, Jerzy (ed.) et al., Number-theoretic methods in cryptology. First international conference, NuTMiC 2017, Warsaw, Poland, September 11–13, 2017. Revised selected papers. Cham: Springer. Lect. Notes Comput. Sci. 10737, 142-160 (2018).

Summary: Lattice basis reduction algorithms have been used as a strong tool for cryptanalysis. The most famous one is LLL, and its typical improvements are BKZ and LLL with deep insertions (DeepLLL). In LLL and DeepLLL, at every time to replace a lattice basis, we need to recompute the Gram-Schmidt orthogonalization (GSO) for the new basis. Compared with LLL, the form of the new GSO vectors is complicated in DeepLLL, and no formula has been known. In this paper, we give an explicit formula for GSO in DeepLLL, and also propose an efficient method to update GSO in DeepLLL. As another work, we embed DeepLLL into BKZ as a subroutine instead of LLL, which we call "DeepBKZ", in order to find a more reduced basis. By using our DeepBKZ with blocksizes up to $\beta = 50$, we have found a number of new solutions for the Darmstadt SVP challenge in dimensions from 102 to 123.

For the entire collection see [Zbl 1384.94004].

MSC:

94A60 Cryptography
68W30 Symbolic computation and algebraic computation

Cited in **2** Reviews
Cited in **4** Documents

Keywords:

lattice basis reduction; LLL with deep insertions; Shortest Vector problem (SVP)

Full Text: DOI

© 2021 FIZ Karlsruhe GmbH