Yasuda, Masaya; **Yamaguchi, Junpei**; **Ooka, Michiko**; **Nakamura, Satoshi**

Development of a dual version of DeepBKZ and its application to solving the LWE challenge.

(English) Zbl 1423.94117

Joux, Antoine (ed.) et al., Progress in cryptology – AFRICACRYPT 2018. 10th international conference on cryptology in Africa, Marrakesh, Morocco, May 7–9, 2018. Proceedings. Cham: Springer. Lect. Notes Comput. Sci. 10831, 162-182 (2018).

Summary: Lattice basis reduction is a strong tool in cryptanalysis. In 2017, DeepBKZ was proposed as a new variant of BKZ [the first two authors, NuTMiC 2017, Lect. Notes Comput. Sci. 10737, 142–160 (2018; Zbl 1423.94115)], and it calls LLL with deep insertions (DeepLLL) as a subroutine alternative to LLL. In this paper, we develop a dual version of DeepBKZ (which we call "Dual-DeepBKZ"), to reduce the dual basis of an input basis. For Dual-DeepBKZ, we develop a dual version of DeepLLL, and then combine it with the dual enumeration by *D. Micciancio* and *M. Walter* [Eurocrypt 2016, Lect. Notes Comput. Sci. 9665, 820–849 (2016; Zbl 1385.94062)]. It never computes the dual basis of an input basis, and it is as efficient as the primal DeepBKZ. We also demonstrate that Dual-DeepBKZ solves several instances in the TU Darmstadt LWE challenge. We use Dual-DeepBKZ in the bounded distance decoding (BDD) approach for solving an LWE instance. Our experiments show that Dual-DeepBKZ reduces the cost of Liu-Nguyen's BDD enumeration [*M. Liu* and *P. Q. Nguyen*, CT-RSA 2013, Lect. Notes Comput. Sci. 7779, 293–309 (2013; Zbl 1312.94070)] more effectively than BKZ. For the LWE instance of $(n, \alpha) = (40, 0.015)$ (resp., $(n, \alpha) = (60, 0.005)$), our results are about 2.2 times (resp., 4.0 times) faster than *R. Xu* et al.'s results [ACNS 2017, Lect. Notes Comput. Sci. 10355, 253–272 (2017; Zbl 1366.94005)], for which they used BKZ in the fplll library and the BDD enumeration with extreme pruning while we used linear pruning in our experiments.

For the entire collection see [Zbl 1387.94004].

MSC:

94A60 Cryptography
68W30 Symbolic computation and algebraic computation

Keywords:

lattice basis reduction; dual lattices; LLL with deep insertions; BKZ; Learning With Errors (LWE)

Full Text: DOI