Yasuda, Masaya; **Nakamura, Satoshi**; **Yamaguchi, Junpei**
Analysis of DeepBKZ reduction for finding short lattice vectors. (English) Zbl 1465.11236
Des. Codes Cryptography 88, No. 10, 2077-2100 (2020).

Summary: Lattice basis reduction is a mandatory tool for solving lattice problems such as the shortest vector problem. The Lenstra-Lenstra-Lovász reduction algorithm (LLL) is the most famous, and its typical improvements are the block Korkine-Zolotarev algorithm and LLL with deep insertions (DeepLLL), both proposed by Schnorr and Euchner. In BKZ with blocksize β, LLL is called many times to reduce a lattice basis before enumeration to find a shortest non-zero vector in every block lattice of dimension β. Recently, "DeepBKZ" was proposed as a mathematical improvement of BKZ, in which DeepLLL is called as a subroutine alternative to LLL. In this paper, we analyze the output quality of DeepBKZ in both theory and practice. Specifically, we give provable upper bounds specific to DeepBKZ. We also develop "DeepBKZ 2.0", an improvement of DeepBKZ like BKZ 2.0, and show experimental results that it finds shorter lattice vectors than BKZ 2.0 in practice.

MSC:

11Y16 Number-theoretic algorithms; complexity
68W30 Symbolic computation and algebraic computation
68R01 General topics of discrete mathematics in relation to computer science

Keywords:

lattice basis reduction; SVP; BKZ; deep insertions

Software:

DeepLLL; PotLLL; NTL; fpLLL; BKZ; GitHub

Full Text: DOI

References:

[1] Albrecht, M., Ducas, L., Herold, G., Kirshanova, E., Postlethwaite, E.W., Stevens, M.: The general sieve kernel and new records in lattice reduction. In: Advances in Cryptology—EUROCRYPT 2019. Lecture Notes in Computer Science, vol. 11477, pp. 717-746. Springer, Berline (2019) · Zbl 07164014

[2] Albrecht, M.R., Curtis, B.R., Deo, A., Davidson, A., Player, R., Postlethwaite, E.W., Virdia, F., Wunderer, T.: Estimate all the LWE, NTRU schemes! In: Security and Cryptography for Networks (SCN 2018). Lecture Notes in Computer Science, vol. 11035, pp. 351-367 (2018) · Zbl 06957562

[3] Aono, Y., Wang, Y., Hayashi, T., Takagi, T.: Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator. In: Advances in Cryptology—EUROCRYPT 2016. Lecture Notes in Computer Science, vol. 9665, pp. 789-819. Springer, New York (2016). Progressive BKZ library is available from https://www2.nict.go.jp/security/pbkzcode/. · Zbl 1385.94007

[4] Bremner, MR, Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications (2011), Boca Raton: CRC Press, Boca Raton

[5] Chen, Y.: Réduction de réseau et sécurité concrete du chiffrement completement homomorphe. Ph.D. thesis, Paris 7 (2013)

[6] Chen, Y., Nguyen, P.Q.: BKZ 2.0: better lattice security estimates. In: Advances in Cryptology—ASIACRYPT 2011. Lecture Notes in Computer Science, vol. 7073, pp. 1-20. Springer, New York (2011) · Zbl 1227.94037

[7] Cohen, H., A Course in Computational Algebraic Number Theory, Graduate Texts in Math (1993), Berlin, Heidelberg: Springer-Verlag, Berlin, Heidelberg · Zbl 0786.11071

[8] Ding, J., Kim, S., Takagi, T., Wang, Y.: LLL and stochastic sandpile models. arXiv:1804.03285v3 (2018).

[9] Ducas, L.: Shortest vector from lattice sieving: a few dimensions for free. In: Advances in Cryptology—EUROCRYPT 2018. Lecture Notes in Computer Science, vol. 10820, pp. 125-145. Springer, New York (2018) · Zbl 1423.94069

[10] Fontein, F.; Schneider, M.; Wagner, U., PotLLL: a polynomial time version of LLL with deep insertions, Designs Codes Cryptogr., 73, 2, 355-368 (2014) · Zbl 1297.94067 · doi:10.1007/s10623-014-9918-8

[11] Galbraith, SD, Mathematics of Public Key Cryptography (2012), Cambridge: Cambridge University Press, Cambridge

[12] Gama, N., Nguyen, P.Q.: Predicting lattice reduction. In: Advances in Cryptology—EUROCRYPT 2008. Lecture Notes in

Computer Science, vol. 4965, pp. 31-51. Springer, New York (2008) · Zbl 1149.94314

[13] Gama, N., Nguyen, P.Q., Regev, O.: Lattice enumeration using extreme pruning. In: Advances in Cryptology—EUROCRYPT 2010. Lecture Notes in Computer Science, vol. 6110, pp. 257-278. Springer, New York (2010) · Zbl 1280.94056

[14] Hanrot, G., Pujol, X., Stehlé, D.: Analyzing blockwise lattice algorithms using dynamical systems. In: Advances in Cryptology—CRYPTO 2011. Lecture Notes in Computer Science, vol. 6841, pp. 447-464. Springer, New York (2011) · Zbl 1287.94072

[15] Lenstra, AK; Lenstra, HW; Lovász, L., Factoring polynomials with rational coefficients, Math. Ann., 261, 4, 515-534 (1982) · Zbl 0488.12001 · doi:10.1007/BF01457454

[16] Li, J.: On the smallest ratio problem of lattice bases. IACR ePrint 2016/847 (2016)

[17] Martinet, J.: Perfect lattices in Euclidean spaces. Comprehensive Studies in Mathematics, vol. 327. Springer Science \& Business Media, New York (2013) · Zbl 1017.11031

[18] Micciancio, D.; Goldwasser, S., Complexity of Lattice Problems: A Cryptographic Perspective (2012), Berlin: Springer Science \& Business Media, Berlin

[19] Micciancio, D., Walter, M.: Practical, predictable lattice basis reduction. In: Advances in Cryptology—EUROCRYPT 2016. Lecture Notes in Computer Science, vol. 9665, pp. 820-849. Springer, New York (2016) · Zbl 1385.94062

[20] Milnor, JW; Husemoller, D., Symmetric Bilinear Forms (1973), New York: Springer, New York

[21] Nguyen, P.Q.: Hermite's constant and lattice algorithms. In: The LLL Algorithm, pp. 19-69. Springer, New York (2009) · Zbl 1230.11155

[22] Pohst, M., A modification of the LLL reduction algorithm, J. Symbol. Comput., 4, 1, 123-127 (1987) · Zbl 0629.10001 · doi:10.1016/S0747-7171(87)80061-5

[23] Schnorr, CP, A hierarchy of polynomial time lattice basis reduction algorithms, Theoret Comput. Sci., 53, 2-3, 201-224 (1987) · Zbl 0642.10030 · doi:10.1016/0304-3975(87)90064-8

[24] Schnorr, C.P.: Block Korkin-Zolotarev bases and successive minima. International Computer Science Institute (1992)

[25] Schnorr, C.P.: Lattice reduction by random sampling and birthday methods. In: Symposium on Theoretical Aspects of Computer Science-STACS 2003. Lecture Notes in Computer Science, vol. 2607, pp. 145-156. Springer, New York (2003) · Zbl 1035.68113

[26] Schnorr, CP; Euchner, M., Lattice basis reduction: improved practical algorithms and solving subset sum problems, Math. Program., 66, 181-199 (1994) · Zbl 0829.90099 · doi:10.1007/BF01581144

[27] Shoup, V.: NTL: A Library for Doing Number Theory. http://www.shoup.net/ntl/.

[28] The FPLLL development team: FPLLL, a lattice reduction library (2016). https://github.com/fplll/fplll

[29] TU Darmstadt: SVP challenge. https://www.latticechallenge.org/svp-challenge/.

[30] Yamaguchi, J., Yasuda, M.: Explicit formula for Gram-Schmidt vectors in LLL with deep insertions and its applications. In: International Conference on Number-Theoretic Methods in Cryptology—NuTMiC 2017. Lecture Notes in Computer Science, vol. 10737, pp. 142-160. Springer, Berlin (2017) · Zbl 1423.94115

[31] Yasuda, M.: Self-dual DeepBKZ for finding short lattice vectors. To appear in a MathCrypt special issue of J. Math. Cryptol. · Zbl 1448.94235

[32] Yasuda, M.; Yamaguchi, J., A new polynomial-time variant of LLL with deep insertions for decreasing the squared-sum of Gram-Schmidt lengths, Designs Codes Cryptogr., 87, 2489-2505 (2019) · Zbl 1431.68084 · doi:10.1007/s10623-019-00634-9

[33] Yasuda, M., Yamaguchi, J., Ooka, M., Nakamura, S.: Development of a dual version of DeepBKZ and its application to solving the LWE challenge. In: Progress in Cryptology—AFRICACRYPT 2018. Lecture Notes in Computer Science, vol. 10831, pp. 162-182. Springer, New York (2018) · Zbl 1423.94117

[34] Yasuda, M.; Yokoyama, K.; Shimoyama, T.; Kogure, J.; Koshiba, T., Analysis of decreasing squared-sum of Gram-Schmidt lengths for short lattice vectors, J. Math. Cryptol., 11, 1, 1-24 (2017) · Zbl 1391.65099 · doi:10.1515/jmc-2016-0008