Lattice cryptography: isomorphisms & dual attacks

Pulles, L.N.

Bibliography

[AS64] Milton Abramowitz and Irene A. Stegun. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, volume 55 of *National Bureau of Standards Applied Mathematics Series*. U.S. Government Printing Office, 1964. URL: https://archive.org/details/AandS-mono600. Cited on pages 26, 123, and 124.

[AKSY22] Shweta Agrawal, Elena Kirshanova, Damien Stehlé, and Anshu Yadav. Practical, round-optimal lattice-based blind signatures. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *ACM CCS 2022*, pages 39–53. ACM Press, November 2022. DOI: 10.1145/3548606.3560650. Cited on page 148.

[ASY22] Shweta Agrawal, Damien Stehlé, and Anshu Yadav. Round-optimal lattice-based threshold signatures, revisited. In Mikolaj Bojanczyk, Emanuela Merelli, and David P. Woodruff, editors, *ICALP 2022*, volume 229 of *LIPIcs*, pages 8:1–8:20. Schloss Dagstuhl, July 2022. DOI: 10.4230/LIPIcs.ICALP.2022.8. Cited on page 150.

[AR04] Dorit Aharonov and Oded Regev. Lattice problems in $\mathsf{NP} \cap \mathsf{coNP}$. In *45th FOCS*, pages 362–371. IEEE Computer Society Press, October 2004. DOI: 10.1109/FOCS.2004.35. Cited on pages 86, 87, 90, 92, 96, and 117.

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th ACM STOC*, pages 99–108.

ACM Press, May 1996. DOI: 10.1145/237814.237838. Cited on page 39.

[Ajt98] Miklós Ajtai. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In *30th ACM STOC*, pages 10–19. ACM Press, May 1998. DOI: 10.1145/276698.276705. Cited on pages 14 and 41.

[Ajt99] Miklós Ajtai. Generating hard instances of the short basis problem. In Jirí Wiedermann, Peter van Emde Boas, and Mogens Nielsen, editors, *ICALP 99*, volume 1644 of *LNCS*, pages 1–9. Springer, Berlin, Heidelberg, July 1999. DOI: 10.1007/3-540-48523-6_1. Cited on pages 39 and 190.

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *33rd ACM STOC*, pages 601–610. ACM Press, July 2001. DOI: 10.1145/380752.380857. Cited on page 76.

[AAC+22] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. Status report on the third round of the NIST post-quantum cryptography standardization process. Technical report, National Institute of Standards and Technology, July 2022. Update 1 (2022-09-26). DOI: 10.6028/NIST.IR.8413-upd1. Cited on pages 8, 10, and 146.

[ABC+26] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, and Noah Waller. Status report on the second round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process. Technical report, National Institute of Standards and Technology, May 2026. DOI: 10.6028/NIST.IR.8610. Cited on page 11.

[Alb17] Martin R. Albrecht. On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL.

In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 103–129. Springer, Cham, April / May 2017. DOI: 10.1007/978-3-319-56614-6_4. Cited on pages 86 and 87.

[AD21] Martin R. Albrecht and Léo Ducas. *Lattice Attacks on NTRU and LWE: A History of Refinements*, pages 15–40. London Mathematical Society Lecture Note Series. Cambridge University Press, 2021. DOI: 10.1017/9781108854207.004. Cited on pages 79, 158, and 213.

[ADH+19] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. The general sieve kernel and new records in lattice reduction. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part II*, volume 11477 of *LNCS*, pages 717–746. Springer, Cham, May 2019. DOI: 10.1007/978-3-030-17656-3_25. Cited on pages 81, 89, 111, 122, 134, and 251.

[AGVW17] Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving uSVP and applications to LWE. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 297–322. Springer, Cham, December 2017. DOI: 10.1007/978-3-319-70694-8_11. Cited on page 213.

[AS23] Martin R. Albrecht and Yixin Shen. Quantum augmented dual attack, 2023. arXiv:2205.13983. Cited on pages 87, 88, 116, and 117.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange — a new hope. In Thorsten Holz and Stefan Savage, editors, *25th USENIX Security Symposium*, pages 327–343, Austin, TX, USA, August 2016. USENIX Association. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim. Cited on pages 15, 86, 87, 95, 116, 213, and 214.

[APvW25] Bill Allombert, Alice Pellet-Mary, and Wessel P.J. van Woerden. Cryptanalysis of rank-2 module-LIP: A single real embedding is all it takes. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part II*, volume 15602 of *LNCS*, pages 184–212. Springer, Cham, May 2025. DOI: 10.1007/978-3-031-91124-8_7. Cited on page 206.

[AEN19] Yoshinori Aono, Thomas Espitau, and Phong Q. Nguyen. Random lattices: Theory and practice. Preprint, 2019. URL: https://espitau.github.io/bin/random_lattice.pdf. Cited on page 39.

[AGLL94] Derek Atkins, Michael Graff, Arjen K. Lenstra, and Paul C. Leyland. The magic words are squeamish ossifrage. In Josef Pieprzyk and Reihaneh Safavi-Naini, editors, *ASIACRYPT'94*, volume 917 of *LNCS*, pages 263–277. Springer, Berlin, Heidelberg, November / December 1994. DOI: 10.1007/BFb0000440. Cited on pages 5 and 6.

[ADM+24] Thomas Aulbach, Samed Düzlü, Michael Meyer, Patrick Struck, and Maximiliane Weishäupl. Hash your keys before signing - BUFF security of the additional NIST PQC signatures. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *PQCrypto 2024, Part II*, pages 301–335. Springer, Cham, June 2024. DOI: 10.1007/978-3-031-62746-0_13. Cited on page 175.

[Bab86] László Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986. DOI: 10.1007/BF02579403. Cited on pages 59, 60, 148, 154, and 175.

[BG14] Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary LWE. In Willy Susilo and Yi Mu, editors, *ACISP 14*, volume 8544 of *LNCS*, pages 322–337. Springer, Cham, July 2014. DOI: 10.1007/978-3-319-08344-5_21. Cited on page 38.

[BLS16] Shi Bai, Thijs Laarhoven, and Damien Stehlé. Tuple lattice sieving. *LMS Journal of Computation and Mathematics*,

19(A):146–162, 2016. DOI: 10.1112/S1461157016000292. Cited on pages 80 and 202.

[BLR+18] Shi Bai, Tancrède Lepoint, Adeline Roux-Langlois, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. *Journal of Cryptology*, 31(2):610–640, April 2018. DOI: 10.1007/s00145-017-9265-9. Cited on page 26.

[BSW18] Shi Bai, Damien Stehlé, and Weiqiang Wen. Measuring, simulating and exploiting the head concavity phenomenon in BKZ. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 369–404. Springer, Cham, December 2018. DOI: 10.1007/978-3-030-03326-2_13. Cited on pages 79, 80, 158, and 214.

[BN24] Henry Bambury and Phong Q. Nguyen. Improved provable reduction of NTRU and hypercubic lattices. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *PQCrypto 2024, Part I*, pages 343–370. Springer, Cham, June 2024. DOI: 10.1007/978-3-031-62743-9_12. Cited on page 206.

[Ban93] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Math. Ann.*, 296(1):625–635, 1993. DOI: 10.1007/BF01445125. Cited on page 57.

[BGMN05] Franck Barthe, Olivier Guédon, Shahar Mendelson, and Assaf Naor. A probabilistic approach to the geometry of the ℓ_p^n-ball. *Annals of Probability*, 33(2):480–513, 2005. DOI: 10.1214/009117904000000874. Cited on pages 127 and 134.

[BW25] Kaveh Bashiri and Andreas Wiemers. On the independence heuristic in the dual attack. *Journal of Mathematical Cryptology*, 19(1), 2025. DOI: 10.1515/jmc-2024-0028. Cited on page 122.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In Robert Krauthgamer, editor, *27th SODA*, pages 10–24. ACM-SIAM, January 2016. DOI: 10.1137/1.9781611974331.ch2. Cited on pages 80, 81, 86, 91, 105, and 121.

[BGPS23] Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 252–281. Springer, Cham, April 2023. DOI: 10.1007/978-3-031-30589-4_9. Cited on pages 146, 162, and 206.

[Ber08] Daniel J. Bernstein. ChaCha, a variant of Salsa20. In Christophe De Cannière and Orr Dunkelman, editors, *State of the Art of Stream Ciphers*, SASC, pages 273–278, Lausanne, Switzerland, February 13–14, 2008. URL: https://cr.yp.to/chacha/chacha-20080128.pdf. Cited on page 170.

[BS16] Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In Robert Krauthgamer, editor, *27th SODA*, pages 893–902. ACM-SIAM, January 2016. DOI: 10.1137/1.9781611974331.ch64. Cited on page 19.

[BM21] Tamar Lichter Blanks and Stephen D. Miller. Generating cryptographically-strong random lattice bases and recognizing rotations of $\mathbb{Z}^n$. In Jung Hee Cheon and Jean-Pierre Tillich, editors, *PQCrypto 2021*, pages 319–338. Springer, Cham, 2021. DOI: 10.1007/978-3-030-81293-5_17. Cited on page 206.

[Bli29] Hans Frederick Blichfeldt. The minimum value of quadratic forms, and the closest packing of spheres. *Math. Ann.*, 101:605–608, 1929. DOI: 10.1007/BF01454863. Cited on page 31.

[Bli35] Hans Frederick Blichfeldt. The minimum values of positive quadratic forms in six, seven and eight variables. *Mathematische Zeitschrift*, 39:1–15, 1935. DOI: 10.1007/BF01201341. Cited on page 31.

[BBD+23] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. HAWK. Technical report, National Institute of Standards and Technology, 2023. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures. Cited on pages 21 and 175.

[BBD+24] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. HAWK. Technical report, National Institute of Standards and Technology, 2024. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures. Cited on pages 175 and 207.

[BBD+26] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. HAWK. Technical report, National Institute of Standards and Technology, 2026. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-3-additional-signatures. Cited on pages xvi, 21, 145, and 208.

[BM18] Leif Both and Alexander May. Decoding linear codes with high error rate and its impact for LPN security. In Tanja Lange and Rainer Steinwandt, editors, *PQCrypto 2018*, pages 25–46. Springer, Cham, 2018. DOI: 10.1007/978-3-319-79063-3_2. Cited on page 89.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 575–584. ACM Press, June 2013. DOI: 10.1145/2488608.2488680. Cited on page 57.

[CGS14] Peter Campbell, Michael Groves, and Dan Shepherd. Soliloquy: a cautionary tale. ETSI 2nd Quantum-Safe Crypto Workshop, October 2014. URL: https://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf. Cited on page 19.

[CDMT22] Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. Statistical decoding 2.0: Reducing decoding to LPN. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 477–507. Springer, Cham, December 2022. DOI: 10.1007/978-3-031-22972-5_17. Cited on page 89.

[CDMT24] Kévin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. Reduction from sparse LPN to LPN, dual attack 3.0. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part VII*, volume 14657 of *LNCS*, pages 286–315. Springer, Cham, May 2024. DOI: 10.1007/978-3-031-58754-2_11. Cited on page 122.

[CST22] Kevin Carrier, Yixin Shen, and Jean-Pierre Tillich. Faster dual lattice attacks by using coding theory. Cryptology ePrint Archive, Report 2022/1750, 2022. Version dated 2022-12-20. URL: https://eprint.iacr.org/archive/2022/1750/20221220:184709. Cited on pages 87, 88, 116, and 117.

[Cas96] John William Scott Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer, Berlin, Heidelberg, 1996. DOI: 10.1007/978-3-642-62035-5. Cited on pages 28 and 30.

[CSV12] Xiao-Wen Chang, Damien Stehlé, and Gilles Villard. Perturbation analysis of the QR factor R in the context of LLL lattice basis reduction. *Mathematics of Computation*, 81(279):1487–1511, 2012. DOI: 10.1090/S0025-5718-2012-02545-2. Cited on page 75.

[Che13] Yuanmi Chen. *Réduction de réseau et sécurité concrete du chiffrement completement homomorphe*. PhD thesis, Université Paris Diderot, November 13, 2013. URL: https://archive.org/details/PhDChen13. Cited on pages 40 and 78.

[CN11] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 1–20. Springer, Berlin, Heidelberg, December 2011. DOI: 10.1007/978-3-642-25385-0_1. Cited on pages 79, 80, 100, 158, 159, and 214.

[CFS25] Clémence Chevignard, Pierre-Alain Fouque, and André Schrottenloher. Reducing the number of qubits in quantum factoring. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part II*, volume 16001 of *LNCS*, pages 384–415. Springer, Cham, August 2025. DOI: 10.1007/978-3-032-01878-6_13. Cited on page 6.

[CME+25] Clémence Chevignard, Guilhem Mureau, Thomas Espitau, Alice Pellet-Mary, Heorhii Pliatsok, and Alexandre Wallet. A reduction from hawk to the principal ideal problem in a quaternion algebra. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part II*, volume 15602 of *LNCS*, pages 154–183. Springer, Cham, May 2025. DOI: 10.1007/978-3-031-91124-8_6. Cited on page 206.

[CK09] Henry Cohn and Abhinav Kumar. Optimality and uniqueness of the Leech lattice among lattices. *Annals of Mathematics*, 170(3):1003–1050, 2009. DOI: 10.4007/annals.2009.170.1003. Cited on page 31.

[CKM+17] Henry Cohn, Abhinav Kumar, Stephen D. Miller, Danylo Radchenko, and Maryna Viazovska. The sphere packing problem in dimension 24. *Annals of Mathematics*, 185(3):1017–1033, 2017. DOI: 10.4007/annals.2017.185.3.8. Cited on page 31.

[CS98] John H. Conway and Neil J.A. Sloane. *Sphere Packings, Lattices and Groups*, volume 3 of *Grundlehren der mathe-*

matischen Wissenschaften. Springer, New York, 1998. DOI: 10.1007/978-1-4757-6568-7. Cited on page 30.

[Cor00] Jean-Sébastien Coron. On the exact security of full domain hash. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 229–235. Springer, Berlin, Heidelberg, August 2000. DOI: 10.1007/3-540-44598-6_14. Cited on page 10.

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 559–585. Springer, Berlin, Heidelberg, May 2016. DOI: 10.1007/978-3-662-49896-5_20. Cited on page 19.

[CDW17] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-SVP. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 324–348. Springer, Cham, April / May 2017. DOI: 10.1007/978-3-319-56620-7_12. Cited on page 19.

[CDF+21] Cas Cremers, Samed Düzlü, Rune Fiedler, Marc Fischlin, and Christian Janson. BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures. In *2021 IEEE Symposium on Security and Privacy*, pages 1696–1714. IEEE Computer Society Press, May 2021. DOI: 10.1109/SP40001.2021.00093. Cited on page 175.

[DDGR20] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. LWE with side information: Attacks and concrete security estimation. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 329–358. Springer, Cham, August 2020. DOI: 10.1007/978-3-030-56880-1_12. Cited on pages 80, 158, 159, 160, 162, 163, 164, 213, and 214.

[DADRT23] Thomas Debris-Alazard, Léo Ducas, Nicolas Resch, and Jean-Pierre Tillich. Smoothing codes and lattices: Sys-

tematic study and new bounds. *IEEE Transactions on Information Theory*, 69(9):6006–6027, 2023. DOI: 10.1109/TIT.2023.3276921. Cited on pages 88, 101, and 104.

[Duc18] Léo Ducas. Shortest vector from lattice sieving: A few dimensions for free. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 125–145. Springer, Cham, April / May 2018. DOI: 10.1007/978-3-319-78381-9_5. Cited on page 110.

[Duc24] Léo Ducas. Provable lattice reduction of $\mathbb{Z}^n$ with blocksize n/2. *DCC*, 92(4):909–916, 2024. DOI: 10.1007/s10623-023-01320-7. Cited on pages 206, 208, 209, and 213.

[DDLL13] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal Gaussians. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 40–56. Springer, Berlin, Heidelberg, August 2013. DOI: 10.1007/978-3-642-40041-4_3. Cited on page 146.

[DN12a] Léo Ducas and Phong Q. Nguyen. Faster Gaussian lattice sampling using lazy floating-point arithmetic. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 415–432. Springer, Berlin, Heidelberg, December 2012. DOI: 10.1007/978-3-642-34961-4_26. Cited on page 146.

[DN12b] Léo Ducas and Phong Q. Nguyen. Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 433–450. Springer, Berlin, Heidelberg, December 2012. DOI: 10.1007/978-3-642-34961-4_27. Cited on pages 156, 191, 203, and 206.

[DPPvW22a] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 65–94. Springer,

Cham, December 2022. DOI: 10.1007/978-3-031-22972-5_3. Cited on pages xv, 21, 145, 175, 206, 207, 209, and 213.

[DPPvW22b] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. Cryptology ePrint Archive, Report 2022/1155, 2022. URL: https://eprint.iacr.org/2022/1155. Cited on pages 164, 188, 189, and 200.

[DP16] Léo Ducas and Thomas Prest. Fast Fourier orthogonalization. In *2016 International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 191–198, Waterloo, ON, Canada, July 20–22, 2016. ACM Press, New York. DOI: 10.1145/2930889.2930923. Cited on pages 146, 152, 153, 174, and 251.

[DP23a] Léo Ducas and Ludo Pulles. Does the dual-sieve attack on learning with errors even work? Cryptology ePrint Archive, Report 2023/302, 2023. URL: https://eprint.iacr.org/2023/302. Cited on pages 95, 101, 110, 112, and 141.

[DP23b] Léo Ducas and Ludo N. Pulles. Accurate score prediction for dual-sieve attacks. Cryptology ePrint Archive, Report 2023/1850, 2023. URL: https://eprint.iacr.org/2023/1850. Cited on pages 20, 119, and 122.

[DP23c] Léo Ducas and Ludo N. Pulles. Does the dual-sieve attack on learning with errors even work? In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part III*, volume 14083 of *LNCS*, pages 37–69. Springer, Cham, August 2023. DOI: 10.1007/978-3-031-38548-3_2. Cited on pages xv, 20, 85, and 119.

[DP26] Léo Ducas and Ludo N. Pulles. Accurate score prediction for Dual-Sieve attacks. *Journal of Cryptology*, 39(8), 2026. DOI: 10.1007/s00145-025-09560-7. Cited on pages xv, 20, and 119.

[DPS25] Léo Ducas, Ludo N. Pulles, and Marc Stevens. Towards a modern LLL implementation. In Goichiro Hanaoka

and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part III*, volume 16247 of *LNCS*, pages 65–99. Springer, Singapore, December 2025. DOI: 10.1007/978-981-95-5099-9_3. Cited on pages xvi, 65, and 75.

[DSvW21] Léo Ducas, Marc Stevens, and Wessel P. J. van Woerden. Advanced lattice sieving on GPUs, with tensor cores. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 249–279. Springer, Cham, October 2021. DOI: 10.1007/978-3-030-77886-6_9. Cited on page 81.

[DvW22] Léo Ducas and Wessel P. J. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 643–673. Springer, Cham, May / June 2022. DOI: 10.1007/978-3-031-07082-2_23. Cited on pages 146, 147, 150, 158, 159, 188, 206, 213, and 252.

[Dud14] Jarek Duda. Asymmetric numeral systems: entropy coding combining speed of huffman coding with compression rate of arithmetic coding, 2014. arXiv:1311.2540. Cited on page 168.

[DTGD15] Jarek Duda, Khalid Tahboub, Neeraj J. Gadgil, and Edward J. Delp. The use of asymmetric numeral systems as an accurate replacement for huffman coding. In *2015 Picture Coding Symposium (PCS)*, pages 65–69, 2015. DOI: 10.1109/PCS.2015.7170048. Cited on page 168.

[DV90] Pierre Duhamel and Martin Vetterli. Fast Fourier transforms: a tutorial review and a state of the art. *Signal processing*, 19(4):259–299, 1990. URL: https://infoscience.epfl.ch/record/59946. Cited on page 56.

[DHVvW20] Mathieu Dutour Sikirić, Anna Haensch, John Voight, and Wessel P.J. van Woerden. A canonical form for positive definite matrices. In Steven D. Galbraith, editor, *ANTS*

XIV, volume 4 of *Open Book Series*, pages 179–195, Auckland, New Zealand, June 29 – July 4, 2020. Mathematical Sciences Publishers. DOI: 10.2140/obs.2020.4.179. Cited on page 17.

[DvW25] Mathieu Dutour Sikirić and Wessel van Woerden. The lattice packing problem in dimension 9 by Voronoi's algorithm, 2025. arXiv:2508.20719. Cited on page 31.

[vEB81] Peter van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical report, April 1981. URL: https://staff.fnwi.uva.nl/p.vanemdeboas/vectors/mi8104c.html. Cited on page 41.

[vEH14] Tim van Erven and Peter Harremoës. Rényi divergence and Kullback–Leibler divergence. *IEEE Transactions on Information Theory*, 60(7):3797–3820, 2014. DOI: 10.1109/TIT.2014.2320500. Cited on page 26.

[EFG+22] Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu. Mitaka: A simpler, parallelizable, maskable variant of falcon. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 222–253. Springer, Cham, May / June 2022. DOI: 10.1007/978-3-031-07082-2_9. Cited on pages 149 and 150.

[EJK20] Thomas Espitau, Antoine Joux, and Natalia Kharchenko. On a dual/hybrid approach to small secret LWE - A dual/enumeration technique for learning with errors and application to security estimates of FHE schemes. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *INDOCRYPT 2020*, volume 12578 of *LNCS*, pages 440–462. Springer, Cham, December 2020. DOI: 10.1007/978-3-030-65277-7_20. Cited on pages 86, 87, 88, 91, 95, 109, and 116.

[ETWY22] Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu. Shorter hash-and-sign lattice-based signa-

tures. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 245–275. Springer, Cham, August 2022. DOI: 10.1007/978-3-031-15979-4_9. Cited on page 168.

[FH23] Serge Fehr and Yu-Hsuan Huang. On the quantum security of HAWK. In Thomas Johansson and Daniel Smith-Tone, editors, *PQCrypto 2023*, pages 405–416. Springer, Cham, August 2023. DOI: 10.1007/978-3-031-40003-2_15. Cited on pages 200 and 201.

[Fis13] Daniel Fischer. Fourier transform of the indicator of the unit ball. Mathematics Stack Exchange, 2013. Version: 2013-09-12. URL: https://math.stackexchange.com/a/492055. Cited on page 124.

[FPL24] The FPLLL development team. fplll, a lattice reduction library, Version: 5.5.0, November 2024. URL: https://github.com/fplll/fplll. Cited on page 159.

[FPL25] The FPLLL development team. fpylll, a Python wrapper for the fplll lattice reduction library, Version: 0.6.3, January 2025. URL: https://github.com/fplll/fpylll. Cited on pages 89 and 122.

[Gal62] Robert Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1):21–28, 1962. DOI: 10.1109/TIT.1962.1057683. Cited on pages 86, 89, and 90.

[GHN06] Nicolas Gama, Nick Howgrave-Graham, and Phong Q. Nguyen. Symplectic lattice reduction and NTRU. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 233–253. Springer, Berlin, Heidelberg, May / June 2006. DOI: 10.1007/11761679_15. Cited on page 195.

[GN08] Nicolas Gama and Phong Q. Nguyen. Predicting lattice reduction. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 31–51. Springer, Berlin, Heidelberg, April 2008. DOI: 10.1007/978-3-540-78967-3_3. Cited on pages 78 and 79.

[GNR10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. Lattice enumeration using extreme pruning. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 257–278. Springer, Berlin, Heidelberg, May / June 2010. DOI: 10.1007/978-3-642-13190-5_13. Cited on pages 76 and 79.

[Gar77] Martin Gardner. Mathematical games: A new kind of cipher that would take millions of years to break. *Scientific American*, 237(2):120–124, August 1977. DOI: 10.1038/scientificamerican0877-120. Cited on pages 3, 4, and 5.

[GS64] Israel Moiseevich Gel'fand [Ізраїль Мойсейович Гельфанд] and Georgi Evgen'evich Shilov [Георгий Евгеньевич Шилов]. *Generalized functions. Volume I: Properties and operations*. Academic Press, New York and London, 1964. Translated by Eugene Saletan. DOI: 10.1016/C2013-0-12223-4. Cited on page 126.

[GM18] Nicholas Genise and Daniele Micciancio. Faster Gaussian sampling for trapdoor lattices with arbitrary modulus. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 174–203. Springer, Cham, April / May 2018. DOI: 10.1007/978-3-319-78381-9_7. Cited on page 146.

[vGP25] Daniël M.H. van Gent and Ludo N. Pulles. HAWK: Having automorphisms weakens key. *IACR Communications in Cryptology*, 2(2), 2025. DOI: 10.62056/a3qjp2w9p. Cited on pages xv, 21, and 205.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008. DOI: 10.1145/1374376.1374407. Cited on pages 14, 58, 146, 176, 183, 190, 191, 206, and 252.

[GS02] Craig Gentry and Michael Szydlo. Cryptanalysis of the revised NTRU signature scheme. In Lars R. Knudsen,

editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 299–320. Springer, Berlin, Heidelberg, April / May 2002. DOI: 10.1007/3-540-46035-7_20. Cited on pages 147, 184, and 206.

[Gid25] Craig Gidney. How to factor 2048 bit RSA integers with less than a million noisy qubits, 2025. arXiv:2505.15917. Cited on pages 6 and 7.

[GE21] Craig Gidney and Martin Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, 2021. DOI: 10.22331/q-2021-04-15-433. Cited on page 6.

[GM03] Daniel Goldstein and Andrew Mayer. On the equidistribution of hecke points. *Forum Mathematicum*, 15(2):165–189, 2003. DOI: 10.1515/form.2003.009. Cited on pages 36 and 37.

[Gol66] Solomon W. Golomb. Run-length encodings (corresp.). *IEEE Transactions on Information Theory*, 12(3):399–401, 1966. DOI: 10.1109/TIT.1966.1053907. Cited on page 167.

[GJ21] Qian Guo and Thomas Johansson. Faster dual lattice attacks for solving LWE with applications to CRYSTALS. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part IV*, volume 13093 of *LNCS*, pages 33–62. Springer, Cham, December 2021. DOI: 10.1007/978-3-030-92068-5_2. Cited on pages 20, 81, 85, 87, 88, 91, 92, 95, 96, 97, 99, 101, 102, 105, 108, 109, 110, 112, 116, 117, 120, and 141.

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 447–464. Springer, Berlin, Heidelberg, August 2011. DOI: 10.1007/978-3-642-22792-9_25. Cited on pages 76 and 79.

[Hås88] Johan Håstad. Dual vectors and lower bounds for the nearest lattice point problem. *Combinatorica*, 8(1):75–81,

1988. DOI: 10.1007/BF02122554. Cited on pages 86, 87, 90, and 96.

[HR14] Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In Chandra Chekuri, editor, *25th SODA*, pages 391–404. ACM-SIAM, January 2014. DOI: 10.1137/1.9781611973402.29. Cited on page 17.

[Hea17] D.R. Heath-Brown. Iteration of quadratic polynomials over finite fields. *Mathematika*, 63(3):1041–1059, 2017. DOI: 10.1112/S0025579317000328. Cited on page 5.

[Her1850] Charles Hermite. Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres. (continuation). *J. Reine Angew. Math.*, 1850(40):279–315, 1850. DOI: 10.1515/crll.1850.40.279. Cited on page 80.

[HK17] Gottfried Herold and Elena Kirshanova. Improved algorithms for the approximate k-list problem in euclidean norm. In Serge Fehr, editor, *PKC 2017, Part I*, volume 10174 of *LNCS*, pages 16–40. Springer, Berlin, Heidelberg, March 2017. DOI: 10.1007/978-3-662-54365-8_2. Cited on page 202.

[Hig02] Nicholas J. Higham. *Accuracy and Stability of Numerical Algorithms*. SIAM, second edition, August 1, 2002. DOI: 10.1137/1.9780898718027. Cited on pages 46 and 47.

[vH02] Mark van Hoeij. Factoring polynomials and the knapsack problem. *Journal of Number Theory*, 95(2):167–189, 2002. DOI: 10.1006/jnth.2001.2763. Cited on page 71.

[HHP+03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. NTRUSIGN: Digital signatures using the NTRU lattice. In Marc Joye, editor, *CT-RSA 2003*, volume 2612 of *LNCS*, pages 122–140. Springer, Berlin, Heidelberg, April 2003. DOI: 10.1007/3-540-36563-X_9. Cited on page 147.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe P.

Buhler, editor, *Algorithmic Number Theory*, ANTS '98, pages 267–288, Portland, OR, USA, June 21–25, 1998. Springer, Berlin, Heidelberg. DOI: 10.1007/BFb0054868. Cited on pages 17 and 19.

[How07] Nick Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 150–169. Springer, Berlin, Heidelberg, August 2007. DOI: 10.1007/978-3-540-74143-5_9. Cited on page 109.

[HBD+22] Andreas Hülsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS+. Technical report, National Institute of Standards and Technology, 2022. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. Cited on page 146.

[AlJ01] A.Kh. Al Jabri. A statistical decoding algorithm for general linear block codes. In Bahram Honary, editor, *8th IMA International Conference on Cryptography and Coding*, volume 2260 of *LNCS*, pages 1–8. Springer, Berlin, Heidelberg, December 2001. DOI: 10.1007/3-540-45325-3_1. Cited on pages 89 and 90.

[Jaq25] Sam Jaques. Landscape of quantum computing – 2025 update, 2025. Accessed: 2026-01-22. URL: https://sam-jaques.appspot.com/quantum_landscape. Cited on page 7.

[JWL+23] Kaijie Jiang, Anyu Wang, Hengyi Luo, Guoxiao Liu, Yang Yu, and Xiaoyun Wang. Exploiting the symmetry of $\mathbb{Z}^n$: Randomization and the automorphism problem. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part IV*, volume 14441 of *LNCS*, pages 167–200. Springer,

Singapore, December 2023. DOI: 10.1007/978-981-99-8730-6_6. Cited on pages 208, 209, 214, and 215.

[Kan83] Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In *15th ACM STOC*, pages 193–206. ACM Press, April 1983. DOI: 10.1145/800061.808749. Cited on page 32.

[KKN+26] Alexander Karenin, Elena Kirshanova, Julian Nowakowski, Eamonn W. Postlethwaite, Ludo N. Pulles, Fernando Virdia, and Paul Vié. Cool + cruel = dual, and new benchmarks for sparse LWE. In Joan Daemen and Emmanuel Thomé, editors, *EUROCRYPT 2026, Part IV*, volume 16544 of *LNCS*, pages 304–333. Springer, Cham, May 2026. DOI: 10.1007/978-3-032-25327-9_11. Cited on page xvi.

[Kir16] Paul Kirchner. Algorithms on ideal over complex multiplication order. Cryptology ePrint Archive, Report 2016/220, 2016. URL: https://eprint.iacr.org/2016/220. Cited on page 184.

[KEF21] Paul Kirchner, Thomas Espitau, and Pierre-Alain Fouque. Towards faster polynomial-time lattice reduction. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part II*, volume 12826 of *LNCS*, pages 760–790, Virtual Event, August 2021. Springer, Cham. DOI: 10.1007/978-3-030-84245-1_26. Cited on pages 65 and 75.

[Kle00] Philip N. Klein. Finding the closest lattice vector when it's unusually close. In David B. Shmoys, editor, *11th SODA*, pages 937–941. ACM-SIAM, January 2000. Cited on page 146.

[Klü10] Jürgen Klüners. The van Hoeij algorithm for factoring polynomials. In Nguyen and Vallée [NV10], pages 283–291. DOI: 10.1007/978-3-642-02295-1. Cited on page 71.

[Knu97] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison–Wesley, third edition, 1997. Cited on page 5.

[KZ1873] Aleksandr Nikolaevich Korkine [Александр Николаевич Коркин] and Egor Ivanovich Zolotarev [Егор Иванович Золотарёв]. Sur les formes quadratiques. *Math. Ann.*, 6(4):366–389, 1873. DOI: 10.1007/BF01442795. Cited on page 80.

[KS01a] Henrik Koy and Claus-Peter Schnorr. Segment LLL-reduction of lattice bases. In Joseph H. Silverman, editor, *Cryptography and Lattices*, pages 67–80. Springer, 2001. DOI: 10.1007/3-540-44670-2_7. Cited on page 75.

[KS01b] Henrik Koy and Claus-Peter Schnorr. Segment LLL-reduction with floating point orthogonalization. In Joseph H. Silverman, editor, *Cryptography and Lattices*, pages 81–96. Springer, Berlin, Heidelberg, 2001. DOI: 10.1007/3-540-44670-2_8. Cited on page 75.

[Laa21] Thijs Laarhoven. Approximate Voronoi cells for lattices, revisited. *Journal of Mathematical Cryptology*, 15(1):60–71, 2021. DOI: 10.1515/jmc-2020-0074. Cited on page 121.

[LW21] Thijs Laarhoven and Michael Walter. Dual lattice attacks for closest vector problems (with preprocessing). In Kenneth G. Paterson, editor, *CT-RSA 2021*, volume 12704 of *LNCS*, pages 478–502. Springer, Cham, May 2021. DOI: 10.1007/978-3-030-75539-3_20. Cited on pages 86, 87, 88, 90, 91, 92, 93, 94, 95, 96, 101, 102, 104, 115, 117, 120, and 126.

[LO83] J. C. Lagarias and Andrew M. Odlyzko. Solving low-density subset sum problems. In *24th FOCS*, pages 1–10. IEEE Computer Society Press, November 1983. DOI: 10.1109/SFCS.1983.70. Cited on page 71.

[LS15] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *DCC*, 75(3):565–599, 2015. DOI: 10.1007/s10623-014-9938-4. Cited on page 19.

[LM00] B. Laurent and P. Massart. Adaptive estimation of a quadratic functional by model selection. *Annals of Statis-*

tics, 28(5):1302–1338, 2000. DOI: 10.1214/aos/1015957395. Cited on page 182.

[LL93] Arjen K. Lenstra and Hendrik W. Lenstra, Jr. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer, Berlin, Heidelberg, 1993. DOI: 10.1007/BFb0091534. Cited on pages 6 and 252.

[LLL82] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982. DOI: 10.1007/BF01457454. Cited on pages 14, 59, 60, 70, 71, 72, 73, 159, 252, and 255.

[Len83] Hendrik W. Lenstra, Jr. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8(4):538–548, 1983. DOI: 10.1287/moor.8.4.538. Cited on page 60.

[LS17] Hendrik W. Lenstra, Jr. and Alice Silverberg. Lattices with symmetry. *Journal of Cryptology*, 30(3):760–804, July 2017. DOI: 10.1007/s00145-016-9235-7. Cited on pages 147, 184, and 206.

[LS19] Hendrik W. Lenstra, Jr. and Alice Silverberg. Testing isomorphism of lattices over CM-Orders. *SIAM Journal on Computing*, 48(4):1300–1334, 2019. DOI: 10.1137/17M115390X. Cited on page 206.

[LF06] Éric Levieil and Pierre-Alain Fouque. An improved LPN algorithm. In Roberto De Prisco and Moti Yung, editors, *SCN 06*, volume 4116 of *LNCS*, pages 348–359. Springer, Berlin, Heidelberg, September 2006. DOI: 10.1007/11832072_24. Cited on page 86.

[LN25] Jianwei Li and Phong Q. Nguyen. A complete analysis of the BKZ lattice reduction algorithm. *Journal of Cryptology*, 38(1):12, January 2025. DOI: 10.1007/s00145-024-09527-0. Cited on pages 39 and 76.

[LJPW24] Hengyi Luo, Kaijie Jiang, Yanbin Pan, and Anyu Wang. Cryptanalysis of rank-2 module-LIP with symplectic au-

tomorphisms. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part IV*, volume 15487 of *LNCS*, pages 359–385. Springer, Singapore, December 2024. DOI: 10.1007/978-981-96-0894-2_12. Cited on pages 195, 206, 207, 208, 210, and 212.

[LDK+22] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2022. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. Cited on page 146.

[LM09] Vadim Lyubashevsky and Daniele Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 577–594. Springer, Berlin, Heidelberg, August 2009. DOI: 10.1007/978-3-642-03356-8_34. Cited on pages 44 and 252.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Berlin, Heidelberg, May / June 2010. DOI: 10.1007/978-3-642-13190-5_1. Cited on page 49.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6), November 2013. Preliminary version in EUROCRYPT '10. DOI: 10.1145/2535925. Cited on page 19.

[MAT22] MATZOV. Report on the security of LWE: Improved dual lattice attack, April 2022. DOI: 10.5281/zenodo.6493704. Cited on pages 20, 85, 87, 88, 91, 92, 95, 96, 101, 102, 105, 108, 109, 110, 112, 115, 116, 117, 120, and 121.

[McH15] Nat McHugh. The magic words are squeamish ossifrage - factoring RSA-129 using CADO-NFS. Blogspot, March 2015. URL: https://natmchugh.blogspot.com/2015/03/

the-magic-words-are-squeamish-ossifrage.html. Cited on page 6.

[MT23] Charles Meyer-Hilfiger and Jean-Pierre Tillich. Rigorous foundations for dual attacks in coding theory. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023, Part IV*, volume 14372 of *LNCS*, pages 3–32. Springer, Cham, November / December 2023. DOI: 10.1007/978-3-031-48624-1_1. Cited on pages 89 and 141.

[Mic14] Daniele Micciancio. Lattice algorithms and applications, lecture 3: The dual lattice, 2014. URL: https://cseweb.ucsd.edu/classes/sp14/cse206A-a/lec3.pdf. Cited on page 55.

[MG02] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems: a cryptographic perspective*, volume 671 of *The Springer International Series in Engineering and Computer Science*. Springer, New York, first edition, March 31, 2002. Cited on page 33.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007. DOI: 10.1137/S0097539705447360. Cited on pages 57, 58, and 156.

[MV10] Daniele Micciancio and Panagiotis Voulgaris. Faster exponential time algorithms for the shortest vector problem. In Moses Charika, editor, *21st SODA*, pages 1468–1480. ACM-SIAM, January 2010. DOI: 10.1137/1.9781611973075.119. Cited on pages 42, 80, 86, 105, and 132.

[MW17] Daniele Micciancio and Michael Walter. Gaussian sampling over the integers: Efficient, generic, constant-time. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 455–485. Springer, Cham, August 2017. DOI: 10.1007/978-3-319-63715-0_16. Cited on page 27.

[Min1896] Hermann Minkowski. *Geometry of Numbers [Geometrie der Zahlen]*. B.G. Teubner, Leipzig, Germany, 1896. Cited on page 30.

[Mon85] Peter L. Montgomery. Modular multiplication without trial division. *Mathematics of computation*, 44(170):519–521, 1985. DOI: 10.2307/2007970. Cited on page 177.

[MSV09] Ivan Morel, Damien Stehlé, and Gilles Villard. H-LLL: using Householder inside LLL. In *2009 International Symposium on Symbolic and Algebraic Computation*, ISSAC '09, pages 271–278, Seoul, Republic of Korea, July 28–31, 2009. ACM Press, New York. DOI: 10.1145/1576702.1576740. Cited on page 75.

[MdJvH+20] Moritz Müller, Jins de Jong, Maran van Heesch, Benno Overeinder, and Roland van Rijswijk-Deij. Retrofitting post-quantum cryptography in internet protocols: a case study of dnssec. *SIGCOMM Comput. Commun. Rev.*, 50(4):49–57, October 2020. DOI: 10.1145/3431832.3431838. Cited on page 146.

[MPPW24] Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet. Cryptanalysis of rank-2 module-LIP in totally real number fields. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part VII*, volume 14657 of *LNCS*, pages 226–255. Springer, Cham, May 2024. DOI: 10.1007/978-3-031-58754-2_9. Cited on page 206.

[Nat16] National Institute of Standards and Technology. Announcing request for nominations for public-key post-quantum cryptographic algorithms, December 20, 2016. Accessed: 2026-02-20. URL: https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms. Cited on page 8.

[Nat22] National Institute of Standards and Technology. Call for additional digital signature schemes for the post-quantum cryptography standardization process, October 2022. Accessed: 2026-02-20. URL: https://csrc.nist.gov/Projects/

pqc-dig-sig/standardization/call-for-proposals. Cited on page 11.

[Nat24a] National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standards Publication (FIPS) 203, August 13, 2024. DOI: 10.6028/NIST.FIPS.203. Cited on page 10.

[Nat24b] National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. Federal Information Processing Standards Publication (FIPS) 204, August 13, 2024. DOI: 10.6028/NIST.FIPS.204. Cited on page 10.

[Nat24c] National Institute of Standards and Technology. Stateless Hash-Based Digital Signature Standard. Federal Information Processing Standards Publication (FIPS) 205, August 13, 2024. DOI: 10.6028/NIST.FIPS.205. Cited on page 10.

[NS16] Arnold Neumaier and Damien Stehlé. Faster LLL-type reduction of lattice bases. In *2016 International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 373–380, Waterloo, ON, Canada, July 20–22, 2016. ACM Press, New York. DOI: 10.1145/2930889.2930917. Cited on page 75.

[NP33] Jerzy Neyman and Egon Sharpe Pearson. On the problem of the most efficient tests of statistical hypotheses. *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*, 231(694-706):289–337, 1933. DOI: 10.1098/rsta.1933.0009. Cited on page 95.

[NR09] Phong Q. Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology*, 22(2):139–160, April 2009. DOI: 10.1007/s00145-008-9031-0. Cited on pages 14, 146, 147, 156, 191, 203, and 206.

[NS06] Phong Q. Nguyen and Damien Stehlé. LLL on the average. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Algorithmic Number Theory*, ANTS '06, pages 238–256, Berlin, Germany, July 23–28, 2006. Springer, Berlin, Heidelberg. DOI: 10.1007/11792086_18. Cited on page 78.

[NS09] Phong Q. Nguyen and Damien Stehlé. An LLL algorithm with quadratic complexity. *SIAM Journal on Computing*, 39(3):874–903, 2009. Preliminary version in EUROCRYPT '05. DOI: 10.1137/070705702. Cited on page 75.

[NV10] Phong Q. Nguyen and Brigitte Vallée, editors. *The LLL Algorithm - Survey and Applications*. ISC. Springer, 2010. DOI: 10.1007/978-3-642-02295-1. Cited on pages 14, 71, 236, and 249.

[NV08] Phong Q. Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, 2008. DOI: 10.1515/JMC.2008.009. Cited on pages 80, 81, 86, 105, and 202.

[OtR85] Andrew M. Odlyzko and Herman J.J. te Riele. Disproof of the Mertens conjecture. *J. Reine Angew. Math.*, 1985(357):138–160, 1985. DOI: 10.1515/crll.1985.357.138. Cited on page 71.

[Ove06] Raphael Overbeck. Statistical decoding revisited. In Lynn Margaret Batten and Reihaneh Safavi-Naini, editors, *ACISP 06*, volume 4058 of *LNCS*, pages 283–294. Springer, Berlin, Heidelberg, July 2006. DOI: 10.1007/11780656_24. Cited on pages 89 and 90.

[Pei10] Chris Peikert. An efficient and parallel Gaussian sampler for lattices. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 80–97. Springer, Berlin, Heidelberg, August 2010. DOI: 10.1007/978-3-642-14623-7_5. Cited on page 146.

[PS97] W. Plesken and B. Souvignier. Computing isometries of lattices. *J. Symbolic Computation*, 24(3–4):327–334, 1997. DOI: 10.1006/jsco.1996.0130. Cited on page 17.

[Poh87] Michael Pohst. A modification of the LLL reduction algorithm. *Journal of Symbolic Computation*, 4(1):123–127, 1987. DOI: 10.1016/S0747-7171(87)80061-5. Cited on pages 74 and 76.

[Pol75] John M. Pollard. A monte carlo method for factorization. *BIT Numerical Mathematics*, 15:331–334, September 1975. DOI: 10.1007/BF01933667. Cited on page 5.

[Pom85] Carl Pomerance. The quadratic sieve factoring algorithm. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *EUROCRYPT'84*, volume 209 of *LNCS*, pages 169–182. Springer, Berlin, Heidelberg, April 1985. DOI: 10.1007/3-540-39757-4_17. Cited on page 6.

[Por23] Thomas Pornin. Improved key pair generation for falcon, BAT and hawk. Cryptology ePrint Archive, Report 2023/290, 2023. URL: https://eprint.iacr.org/2023/290. Cited on page 175.

[Por25] Thomas Pornin. Improved (again) key pair generation for falcon, BAT and hawk. Cryptology ePrint Archive, Report 2025/1239, 2025. URL: https://eprint.iacr.org/2025/1239. Cited on page 175.

[PP19] Thomas Pornin and Thomas Prest. More efficient algorithms for the NTRU key generation using the field norm. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 504–533. Springer, Cham, April 2019. DOI: 10.1007/978-3-030-17259-6_17. Cited on pages 147, 151, 152, 153, and 172.

[PS05] Thomas Pornin and Julien P. Stern. Digital signatures do not guarantee exclusive ownership. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, *ACNS 2005*, volume 3531 of *LNCS*, pages 138–150. Springer, Berlin, Heidelberg, June 2005. DOI: 10.1007/11496137_10. Cited on page 175.

[PV21] Eamonn W. Postlethwaite and Fernando Virdia. On the success probability of solving unique SVP via BKZ. In Juan Garay, editor, *PKC 2021, Part I*, volume 12710 of *LNCS*, pages 68–98. Springer, Cham, May 2021. DOI: 10.1007/978-3-030-75245-3_4. Cited on pages 80, 158, and 213.

[PS24] Amaury Pouly and Yixin Shen. Provable dual attacks on learning with errors. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part VII*, volume 14657 of *LNCS*, pages 256–285. Springer, Cham, May 2024. DOI: 10.1007/978-3-031-58754-2_10. Cited on pages 92 and 122.

[Pre15] Thomas Prest. *Gaussian sampling in lattice-based cryptography*. PhD thesis, Ecole normale supérieure-ENS PARIS, 2015. URL: https://tprest.github.io/pdf/pub/thesis-thomas-prest.pdf. Cited on page 174.

[Pre17] Thomas Prest. Sharper bounds in lattice-based cryptography using the Rényi divergence. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 347–374. Springer, Cham, December 2017. DOI: 10.1007/978-3-319-70694-8_13. Cited on page 26.

[PFH+22] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2022. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. Cited on pages 57, 145, 146, 149, 157, 165, 167, 168, 169, 170, 171, 173, 179, and 190.

[PT24] Ludo N. Pulles and Mehdi Tibouchi. Cryptanalysis of EagleSign. In Clemente Galdi and Duong Hieu Phan, editors, *SCN 24, Part II*, volume 14974 of *LNCS*, pages 165–186. Springer, Cham, September 2024. DOI: 10.1007/978-3-031-71073-5_8. Cited on page xvi.

[PV25] Ludo N. Pulles and Paul Vié. Accelerating the primal hybrid attack against sparse LWE using GPUs. Cryptology ePrint Archive, Paper 2025/1990, 2025. URL: https://eprint.iacr.org/2025/1990. Cited on page xvi.

[Rad68] Charles M. Rader. Discrete Fourier transforms when the number of data samples is prime. *Proceedings of the IEEE*, 56(6):1107–1108, 1968. DOI: 10.1109/PROC.1968.6477. Cited on page 56.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005. DOI: 10.1145/1060590.1060603. Cited on page 86.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):1–40, September 2009. Preliminary version in STOC '05. DOI: 10.1145/1568318.1568324. Cited on pages 19, 44, 86, and 252.

[Reg25] Oded Regev. An efficient quantum factoring algorithm. *J. ACM*, 72(1):1–13, January 2025. DOI: 10.1145/3708471. Cited on page 6.

[Rén61] Alfréd Rényi. On measures of entropy and information. In Jerzy Neyman, editor, *4th Berkeley Symposium on Mathematical Statistics and Probability*, volume 1, pages 547–561. University of California Press, 1961. URL: http://digicoll.lib.berkeley.edu/record/112906. Cited on page 26.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the Association for Computing Machinery*, 21(2):120–126, February 1978. DOI: 10.1145/359340.359342. Cited on pages 4, 10, and 252.

[Rog56] Claude A. Rogers. The number of lattice points in a set. *Proceedings of the London Mathematical Society*, s3-6(2):305–320, 1956. DOI: 10.1112/plms/s3-6.2.305. Cited on page 39.

[RH23] Keegan Ryan and Nadia Heninger. Fast practical lattice reduction through iterated compression. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part III*, volume 14083 of *LNCS*, pages 3–36. Springer, Cham, August 2023. DOI: 10.1007/978-3-031-38548-3_1. Cited on pages 63, 65, and 75.

[Sch87] Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53(2):201–224, 1987. DOI: 10.1016/0304-3975(87)90064-8. Cited on pages 14, 75, and 251.

[Sch03] Claus-Peter Schnorr. Lattice reduction by random sampling and birthday methods. In Helmut Alt and Michel Habib, editors, *20th Annual Symposium on Theoretical Aspects of Computer Science*, volume 2607 of *STACS '03*, pages 145–156. Springer, Berlin, Heidelberg, February 27 – March 1, 2003. DOI: 10.1007/3-540-36494-3_14. Cited on pages 78 and 251.

[Sch06] Claus-Peter Schnorr. Fast LLL-type lattice reduction. *Information and Computation*, 204(1):1–25, 2006. DOI: 10.1016/j.ic.2005.04.004. Cited on page 75.

[SE94] Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66:181–199, 1994. Preliminary version in FCT '91. DOI: 10.1007/BF01581144. Cited on pages 59 and 75.

[Sch91] Arnold Schönhage. Fast reduction and composition of binary quadratic forms. In *1991 International Symposium on Symbolic and Algebraic Computation*, ISSAC '91, pages 128–133, Bonn, West Germany, July 15–17, 1991. ACM Press, New York. DOI: 10.1145/120694.120711. Cited on page 70.

[SS71] Arnold Schönhage and Volker Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7(3):281–292, September 1971. DOI: 10.1007/BF02242355. Cited on page 70.

[SAB+22] Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2022. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. Cited on page 109.

[Sey93] Martin Seysen. Simultaneous reduction of a lattice basis and its reciprocal basis. *Combinatorica*, 13(3):363–376, 1993. DOI: 10.1007/BF01202355. Cited on pages 64, 65, and 67.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, November 1994. DOI: 10.1109/SFCS.1994.365700. Cited on page 6.

[Sie45] Carl Ludwig Siegel. A mean value theorem in geometry of numbers. *Annals of Mathematics*, 46(2):340–347, 1945. DOI: 10.2307/1969027. Cited on pages 36 and 39.

[Sie89] Carl Ludwig Siegel. *Lectures on the Geometry of Numbers*. Springer, Berlin, Heidelberg, 1989. DOI: 10.1007/978-3-662-08287-4. Cited on page 28.

[Sil21] Joseph Silverman. Origin of name "NTRU"?, June 9, 2021. URL: https://en.wikipedia.org/wiki/Talk:NTRU#Origin_of_name_%22NTRU%22? Cited on page 252.

[SLM+25] M.C. Smith, A.D. Leu, K. Miyanishi, M.F. Gely, and D.M. Lucas. Single-qubit gates with errors at the 10-7 level. *Physical Review Letters*, 134(23):230601, 2025. DOI: 10.1103/42w2-6ccy. Cited on page 6.

[Söd11] Anders Södergren. On the Poisson distribution of lengths of lattice vectors in a random lattice. *Mathematische Zeitschrift*, 269(3):945–954, 2011. DOI: 10.1007/s00209-010-0772-8. Cited on page 39.

[Ste10] Damien Stehlé. Floating-point LLL: Theoretical and practical aspects. In Nguyen and Vallée [NV10], pages 179–213. DOI: 10.1007/978-3-642-02295-1. Cited on page 75.

[SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 617–635. Springer, Berlin, Heidelberg, December 2009. DOI: 10.1007/978-3-642-10366-7_36. Cited on page 19.

[SW71] Elias M. Stein and Guido Weiss. *Introduction to Fourier Analysis on Euclidean Spaces*. Number 32 in Princeton Mathematical Series. Princeton University Press, 1971. URL: https://www.jstor.org/stable/j.ctt1bpm9w6. Cited on pages 28, 54, and 126.

[Sto96] Arne Storjohann. Near optimal algorithms for computing Smith normal forms of integer matrices. In *1996 International Symposium on Symbolic and Algebraic Computation*, ISSAC '96, pages 267–274, Zürich, Switzerland, July 24–26, 1996. ACM Press, New York. DOI: 10.1145/236869.237084. Cited on page 98.

[SL96] Arne Storjohann and George Labahn. Asymptotically fast computation of Hermite normal forms of integer matrices. In *1996 International Symposium on Symbolic and Algebraic Computation*, ISSAC '96, pages 259–266, Zürich, Switzerland, July 24–26, 1996. ACM Press, New York. DOI: 10.1145/236869.237083. Cited on page 35.

[Szy03] Michael Szydlo. Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 433–448. Springer, Berlin, Heidelberg, May 2003. DOI: 10.1007/3-540-39200-9_27. Cited on pages 147 and 206.

[Via17] Maryna S. Viazovska. The sphere packing problem in dimension 8. *Annals of Mathematics*, 185(3):991–1015, 2017. DOI: 10.4007/annals.2017.185.3.7. Cited on page 31.

[Vor1908a] Georges Voronoï [Георгій Феодосійович Вороний]. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Premier Mémoire. Sur quelques propriétés des formes quadratiques positives parfaites. *J. Reine Angew. Math.*, 1908(133):97–102, 1908. DOI: 10.1515/crll.1908.133.97. Cited on page 31.

[Vor1908b] Georges Voronoï [Георгій Феодосійович Вороний]. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième Mémoire. Recherches sur les paralléllоèdres primitifs. *J. Reine Angew. Math.*, 1908(134):198–287, 1908. DOI: 10.1515/crll.1908.134.198. Cited on page 31.

[Wat1922] George Neville Watson. *A treatise on the theory of Bessel functions*. Cambridge University Press, 1922. URL: https://archive.org/details/treatiseontheory00watsuoft. Cited on page 123.

[Wes25] Bas Westerbaan. State of the post-quantum Internet in 2025. Cloudflare Blog, October 2025. Accessed: 2026-01-22. URL: https://blog.cloudflare.com/pq-2025/. Cited on page 8.

[WV24] Bas Westerbaan and Luke Valenta. A look at the latest post-quantum signature standardization candidates. Cloudflare Blog, November 7, 2024. Accessed: 2026-02-20. URL: https://blog.cloudflare.com/another-look-at-pq-signatures/. Cited on page 8.

[Yap92] Chee-Keng Yap. Fast unimodular reduction: Planar integer lattices (extended abstract). In *33rd FOCS*, pages 437–446. IEEE Computer Society Press, October 1992. DOI: 10.1109/SFCS.1992.267808. Cited on page 70.

List of Acronyms

AVX2 advanced vector extensions 2; 148, 169–171, 173, 176, 178, 180, 181

BDD bounded distance decoding; 14–16, 41–44, 86–92, 94–97, 101–108, 110–112, 114, 115, 117, 120–122, 125, 129, 133–138, 141, *see* CVP

BKZ block Korkine–Zolotarev basis reduction [Sch87], see Section 2.5.5; ix, 14, 15, 75, 76, 78–80, 92, 96, 100, 101, 116, 117, 158–163, 166, 207, 208, 212–215

CDF cumulative distribution function; 25, 114, 128, 130–133, 136, 137

CPU central processing unit; 6, 10, 111, 148, 171

CRQC cryptographically relevant quantum computer; 6–8, 10

CVP closest vector problem; 15, 16, 40, 41, 59, *see also* SVP

DFT discrete Fourier transform, see Section 2.3.2; 56, 97

DGS discrete Gaussian sampling, see Section 2.4; 146, 171, 178

EUF-CMA existential unforgeability under chosen message attack, see Section 2.7; 9, 10, 82

ffNP fast Fourier variant of NP [DP16]; 152, 174, 186, *see* NP

FFT fast Fourier transform; ix, 19, 56, 85–87, 89, 99, 116, 117, 122, 141, 148, 170–172, 176–178, 180–182, *see* DFT

G6K general sieve kernel [ADH+19], /ʒe.si.ka/; 81, 110, 111, 134

GH Gaussian heuristic, see Section 2.2.2; 88

GSA geometric series assumption [Sch03]; 79, 214

HKZ Hermite–Korkine–Zolotarev basis reduction [Sch87]; 80, *see* BKZ

HNF Hermite normal form, see Definition 2.31; 35, 36, 185

i.i.d. independent and identically distributed; 26, 81, 89, 127–129,

191, 202

KEM key encapsulation mechanism; 8, 12, 14

LIP Lattice Isomorphism Problem [DvW22]; 17–19, 21, 34, 35, 48, 52, 145–147, 158, 184, 188, 205, 206, 258, 260

LLL Lenstra–Lenstra–Lovász basis reduction [LLL82], see Section 2.5.4; ix, 14, 15, 71–76, 78, 79, 159, 188

LWE learning with errors [Reg09]; 19, 44, 86, 87, 95, 97, 99, 109, 159, *see* BDD

MATZOV Israel's Center of Encryption and Information Security, MATZOV; 85, 87, 91, 95, 101, 109

NFS number field sieve [LL93]; 6

NIST National Institute of Standards and Technology; xvi, 8, 10, 11, 20, 21, 85, 145, 146, 175, 207, 263

NP Babai's nearest-plane algorithm; 60, 91, 251, *see also* RO

NTRU number theorists 'r' us, according to [Sil21]; 14, 17, 19, 146, 149, 164, 206

NTT number theoretic transform; 148, 170–172, 176–178, 181–183, *see* DFT

omSVP one more (approximate) SVP; 21, 147, 156, 183, 192–194, 196, 197, 202, 203, 205–209, 258, 260, *see* SVP

PDF probability density function; 25, 129, 130

PSF Preimage Sampleable Function [GPV08], see Section 5.6.2; 183, 190, 192

RAM random access memory; 169–171, 175

RHF root Hermite factor, see Definition 2.108; 77, 78

RO rounding-off algorithm; 60, *see also* NP

ROM random oracle model; xiv, 192, 193, 201

RSA Rivest–Shamir–Adleman [RSA78]; 4–8, 10

SF survival function; 25, 113, 139, 140, *see* CDF

smLIP search module LIP; 21, 52, 183–185, 188, 189, 205–209, 211, 215, 216, 258, 260, *see* LIP

SNF Smith normal form, see Definition 2.35; 36, 98

SUF-CMA strong existential unforgeability under chosen message attack; xiv, 82, 190, 192, 193, 200, 201, 206, 209, *see* EUF-CMA

SVP shortest vector problem, see Section 2.2.3; 14, 17, 40–42, 44, 75, 81, 147, 214, 215

UniqueSVP unique shortest vector problem [LM09]; 44, 213, *see* SVP

WHT Walsh–Hadamard transform; 56, 111, *see* DFT

List of Symbols

$\lvert\cdot\rvert$	absolute value, *or* cardinality of a set
$\lVert\cdot\rVert$	Euclidean norm, or ℓ^2 norm
$\lVert\cdot\rVert_{\mathrm{F}}$	Frobenius norm of a matrix, i.e., ℓ^2-norm of all its entries
$[n]$	the set $\{1, 2, \ldots, n\}$ given $n \in \mathbb{N}$
$[\![\cdot]\!]$	Iverson bracket, i.e., 1 if its content is true, and 0 otherwise
$\lceil\cdot\rfloor$	rounding to nearest integer, $\mathbb{R} \to \mathbb{Z}$, such that $x - \lceil x \rfloor \in (-1/2, 1/2]$ holds for all $x \in \mathbb{R}$
$\mathbf{1}_{(\cdot)}$	indicator function on a set
$\widehat{(\cdot)}$	Fourier transform of a function, *or* the dual of a group (Definition 2.70)
$(\cdot)^\vee$	dual of a lattice (Definition 2.71), *or* dual of a basis
${}^\vee(\cdot)$	reversed dual basis related to some primal basis
$(\cdot)^\intercal$	transpose of a matrix
$(\cdot)^\star$	complex conjugation in $\mathbb{K}$, *or* Hermitian adjoint of a matrix
$(\cdot)^*$	Gram–Schmidt orthogonalisation of a basis
$\cdot \,\|\, \cdot$	concatenation of two strings
$\langle\cdot, \cdot\rangle$	dot product of two vectors

Greek

Γ	gamma function, $\Gamma(z) = \int_0^\infty t^{z-1} \exp(-t) \mathrm{d}t$
$\eta_\varepsilon(\Lambda)$	smoothing parameter
$\xi(\alpha; x)$	Scaled multiple of Bessel function , *see* J_α
σ	canonical embeddings of $\mathbb{K}$ into $\mathbb{C}$, *or* parameter of (discrete) Gaussian distribution
μ_{ij}	Gram–Schmidt coefficient , *see* $(\cdot)^*$
$\mu_{\mathbb{K}}$	roots of unity of a number field $\mathbb{K}$, *see* $\mathbb{K}$

ρ_σ	Gaussian mass with parameter σ
$\rho_{\mathbf{Q},\sigma}$	Gaussian mass with respect to quadratic form $\mathbf{Q}$, *see* ρ_σ

Alphabetic

$\mathbb{C}, \mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}$	sets of complex, natural, rational and real numbers, and integers, respectively. Natural numbers start from 0
$\lg, \ln, \log$	logarithm base $2, e$ and 10, respectively
$\arg\max_{x \in S} f(x)$	argument $x \in S$ maximising f, i.e., $f(x) = \max f(S)$
$\mathcal{B}^n$	n-dimensional ball
DFT_G	discrete Fourier transform using group G , *see* DFT
$\mathrm{diag}(\mathbf{d})$	diagonal matrix given by $\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$
$\mathcal{D}_{\Lambda+\mathbf{c},\sigma}$	discrete Gaussian on $\Lambda + \mathbf{c}$ with parameter σ
$\mathcal{D}_{\mathbf{Q},\sigma}$	discrete Gaussian with respect to a quadratic form $\mathbf{Q}$, *see* $\mathcal{D}_{\Lambda+\mathbf{c},\sigma}$
$\widetilde{\mathcal{D}}_{\mathbf{Q},\sigma}[\mathbf{h}]$	discrete Gaussian on the coset $R^2 + \mathbf{h}$ with respect to a quadratic form $\mathbf{Q}$, *see* $\mathcal{D}_{\mathbf{Q},\sigma}$
erf	error function
erfc	complementary error function, i.e., $\mathrm{erfc}(x) = 1 - \mathrm{erf}(x)$
ev_x	evaluation at x, i.e., $\mathrm{ev}_x(f) = f(x)$
$\mathbb{E}$	expectation value
$\mathbb{F}_q$	finite field of q elements
$\mathrm{GH}(n)$	Gaussian heuristic, i.e., $r \in \mathbb{R}_{>0}$ satisfying $\mathrm{Vol}_n(r\mathcal{B}^n) = 1$
$\mathrm{GL}_n(R)$	general linear group, $\{\mathbf{M} \in R^{n\times n} : \det \mathbf{M} \in R^*\}$
$\mathcal{G}$	Group of trivial automorphisms of $\mathbf{I}_2(R)$
$\mathcal{G}_\mathbf{Q}$	Group of trivial automorphisms of $\mathbf{Q}$
$\mathbf{I}_n$	identity matrix of order n
J_α	Bessel function (of the first kind) of order α
$j_{\alpha,n}$	nth root of the Bessel function of order α , *see* J_α
$\mathbb{K}$	algebraic number field, but in this thesis mostly the cyclotomic field $\mathbb{K} = \mathbb{Q}(\zeta_{2n})$
$\mathcal{L}(\mathbf{B})$	lattice generated by a basis $\mathbf{B}$
$\mathcal{L}_q(\mathbf{A})$	q-ary lattice generated by matrix $\mathbf{A}$
$\mathcal{L}_q^\perp(\mathbf{A})$	q-ary lattice generated by all vectors orthogonal to $\mathbf{A}$
N	algebraic (absolute) field norm

$\mathcal{N}(c, \sigma^2)$	Gaussian with centre c and standard deviation σ
$\mathcal{N}_n(\mathbf{c}, \sigma^2)$	n-dimensional normal distribution with centre $\mathbf{c}$ and standard deviation σ
$\mathrm{O}_n(R)$	orthogonal group, $\{\mathbf{M} \in R^{n\times n} : \mathbf{M}^\mathsf{T}\mathbf{M} = 1\}$
$\mathrm{O}(\Lambda)$	automorphism group of a lattice
$\mathrm{O}(\mathbf{Q})$	automorphism group of a quadratic form $\mathbf{Q}$
ord	order of a group element
$\mathcal{O}_\mathbb{K}$	ring of integers of $\mathbb{K}$, *see* $\mathbb{K}$
$\mathcal{P}(\mathbf{B})$	fundamental domain generated by basis $\mathbf{B}$
$\mathrm{Pot}(\mathbf{B})$	lattice potential of a basis, see [LLL82, Eq. (1.25)]
$\Pr[\,\cdot\,]$	probability of a certain event happening
R	ring of integers of $\mathbb{K}$, *see* $\mathcal{O}_\mathbb{K}$ & $\mathbb{K}$
rk	rank of lattice
$\mathrm{R}_a(D_1 \parallel D_2)$	Rényi divergence at order a of distribution D_1 from D_2
$\textsc{Rot}(\mathbf{x})$	coefficient embedding of all rotations, $R \to \mathbb{Z}^{n\times n}$, *see* $\textsc{Vec}(\mathbf{x})$
$\mathrm{SL}_n(R)$	special linear group, $\{\mathbf{M} \in R^{n\times n} : \det \mathbf{M} = 1\}$
$\mathrm{sl}(\mathbf{B})$	slope of a lattice basis
$\mathrm{span}(\,\cdot\,)$	$\mathbb{R}$-linear span
$\mathcal{S}^1$	unit circle (subset of $\mathbb{C}$)
$\mathcal{S}^{n-1}$	sphere of dimension $n-1$, which is a subset of $\mathbb{R}^n$
Supp	support (of a distribution)
Tr	algebraic (absolute) field trace
$\mathrm{U}(\,\cdot\,)$	uniform distribution on a given set
$\mathbb{V}$	variance, i.e., $\mathbb{V}[X] = \mathbb{E}[X^2] - (\mathbb{E}[X])^2$
$\textsc{Vec}(\mathbf{x})$	coefficient embedding $R \to \mathbb{Z}^n$
Vol_k	volume of k-dimensional object
$\mathcal{V}(\Lambda)$	Voronoi cell of lattice Λ