Lattice cryptography: from cryptanalysis to New Foundations

Woerden, W.P.J. van

Bibliography

[ABD16] Martin Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched NTRU assumptions. In: Springer, 2016, pages 153–178.

[AD21] Martin Albrecht and Léo Ducas. Lattice Attacks on NTRU and LWE: A History of Refinements. In: *Computational Cryptography: Algorithmic Aspects of Cryptology*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2021, pages 15–40.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange–A New Hope. In: 2016, pages 327–343.

[AEN19] Yoshinori Aono, Thomas Espitau, and Phong Q. Nguyen. Random Lattices: Theory And Practice. Available at https://espitau.github.io/bin/random_lattice.pdf. 2019.

[AFG13] Martin R. Albrecht, Robert Fitzpatrick, and Florian Göpfert. On the efficacy of solving LWE by reduction to unique-SVP. In: Springer, 2013, pages 293–310.

[AGPS20] Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, and John M. Schanck. Estimating quantum speedups for lattice sieves. In: Springer, 2020, pages 583–613.

[AGVW17] Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving uSVP and applications to LWE. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2017, pages 297–322.

[Ajt99] Miklós Ajtai. Generating Hard Instances of the Short Basis Problem. In: *ICALP*. 1999, pages 1–9.

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In: *STOC*. 2001, pages 601–610.

[AL22] Martin R. Albrecht and Jianwei Li. Predicting BKZ Z-Shapes on q-ary Lattices. Cryptology ePrint Archive, Report 2022/843. 2022.

[Alb+15] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugere, Robert Fitzpatrick, and Ludovic Perret. On the complexity of the BKW algorithm on LWE. In: *Designs, Codes and Cryptography* 74.2 (2015), pages 325–354.

[Alb+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: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2019, pages 717–746.

[ALL19] Nicolas Aragon, Julien Lavauzelle, and Matthieu Lequesne. Decoding Challenge. Available at `http://decodingchallenge.org`. 2019.

[AN17] Yoshinori Aono and Phong Q. Nguyen. Random sampling revisited: lattice enumeration with discrete pruning. In: *Eurocrypt*. 2017, pages 65–102.

[ANS18] Yoshinori Aono, Phong Q. Nguyen, and Yixin Shen. Quantum lattice enumeration and tweaking discrete pruning. In: *Asiacrypt*. 2018, pages 405–434.

[AP11] Joël Alwen and Chris Peikert. Generating Shorter Bases for Hard Random Lattices. In: *Theory of Computing Systems* 48.3 (Apr. 2011). Preliminary version in STACS 2009, pages 535–553.

[AR05] Dorit Aharonov and Oded Regev. Lattice problems in NP ∩ coNP. In: *J. ACM* 52.5 (2005). Preliminary version in FOCS 2004, pages 749–765.

[AUV19] Divesh Aggarwal, Bogdan Ursu, and Serge Vaudenay. Faster sieving algorithm for approximate SVP with constant approximation factors. Cryptology ePrint Archive, Report 2019/1028. 2019.

[AWHT16] Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi. Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator. In: Springer, 2016, pages 789–819.

[Bab16] László Babai. Graph isomorphism in quasipolynomial time. In: *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. 2016, pages 684–697.

[Bab19] László Babai. Canonical form for graphs in quasipolynomial time: preliminary report. In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. 2019, pages 1237–1246.

[Bab86] László Babai. On Lovász' lattice reduction and the nearest lattice point problem. In: *Combinatorica* 6.1 (1986). Preliminary version in STACS 1985, pages 1–13.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. In: *Mathematische Annalen* 296.4 (1993), pages 625–636.

[Bar+11] Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, François-Xavier Standaert, and Yu Yu. Leftover hash lemma, revisited. In: *Annual Cryptology Conference*. Springer. 2011, pages 1–20.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In: *Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms*. SIAM. 2016, pages 10–24.

[Ber+20] Daniel J. Bernstein, Billy Bob Brumley, Ming-Shing Chen, Chitchanok Chuengsatiansup, Tanja Lange, Adrian Marotzke, Bo-Yuan Peng, Nicola Tuveri, Christine van Vredendaal, and Bo-Yin Yang. *NTRU Prime*. Technical report. Available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions. National Institute of Standards and Technology, 2020.

[BGJ15] Anja Becker, Nicolas Gama, and Antoine Joux. Speeding-up lattice sieving without increasing the memory, using sub-quadratic nearest neighbor search. 2015.

[Bia+17] Jean-François Biasse, Thomas Espitau, Pierre-Alain Fouque, Alexandre Gélin, and Paul Kirchner. Computing generator in cyclotomic integer rings. In: *Eurocrypt*. Springer. 2017, pages 60–88.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in 2 n/20: How 1+ 1= 0 improves information set decoding. In: Springer, 2012, pages 520–536.

[BKL80] László Babai, Paul Klingsberg, and Eugene M. Luks. Canonical labeling for vertex colored graphs. In: *To appear* (1980).

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. In: *Journal of the ACM (JACM)* 50.4 (2003), pages 506–519. ISSN: 0004-5411.

[BL16] Anja Becker and Thijs Laarhoven. Efficient (ideal) lattice sieving using cross-polytope LSH. In: *International Conference on Cryptology in Africa*. Springer. 2016, pages 3–23.

[BL83] László Babai and Eugene M. Luks. Canonical labeling of graphs. In: *Proceedings of the fifteenth annual ACM symposium on Theory of computing*. 1983, pages 171–183.

[Bla+20] Pierre Blanchard, Nicholas J. Higham, Florent Lopez, Theo Mary, and Srikara Pranesh. Mixed Precision Block Fused Multiply-Add: Error Analysis and Application to GPU Tensor Cores. In: *SIAM Journal on Scientific Computing* 42.3 (2020), pages C124–C141.

[BLLN13] Joppe W. Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In: Springer, 2013, pages 45–64.

[BLS16] Shi Bai, Thijs Laarhoven, and Damien Stehlé. Tuple lattice sieving. In: *LMS Journal of Computation and Mathematics* 19.A (2016), pages 146–162.

[BM18] Leif Both and Alexander May. Decoding linear codes with high error rate and its impact for LPN security. In: Springer, 2018, pages 25–46.

[BM21] Tamar Lichter Blanks and Stephen D. Miller. Generating cryptographically-strong random lattice bases and recognizing rotations of $\mathbb{Z}^n$. In: *CoRR* (2021).

[BMPS20] Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, and Paolo Santini. LESS is more: Code-based signatures without syndromes. In: *International Conference on Cryptology in Africa*. Springer. 2020, pages 45–65.

[BN09] Johannes Blömer and Stefanie Naewe. Sampling methods for shortest vectors, closest vectors and successive minima. In: *Theoretical Computer Science* 410.18 (2009), pages 1648–1665. ISSN: 0304-3975.

[BNP17] Joppe W. Bos, Michael Naehrig, and Joop Van De Pol. Sieving for shortest vectors in ideal lattices: a practical perspective. In: *International Journal of Applied Cryptography* 3.4 (2017), pages 313–329.

[Bog01] Michael I. Boguslavsky. Radon transforms and packings. In: *Discrete applied mathematics* 111.1-2 (2001), pages 3–22.

[BP22] Huck Bennett and Chris Peikert. Hardness of the (Approximate) Shortest Vector Problem: A Simple Proof via Reed-Solomon Codes. arXiv preprint arXiv:2202.07736. 2022.

[Bra+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In: *STOC*. 2013, pages 575–584.

[BSW18] Shi Bai, Damien Stehlé, and Weiqiang Wen. Measuring, simulating and exploiting the head concavity phenomenon in BKZ. In: Springer, 2018, pages 369–404.

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In: *Eurocrypt*. Springer. 2016, pages 559–585.

[CG05] Michael Coglianese and Bok-Min Goi. MaTRU: A new NTRU-based cryptosystem. In: *International Conference on Cryptology in India*. Springer. 2005, pages 232–243.

[Cha02] Moses S. Charikar. Similarity estimation techniques from rounding algorithms. In: *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*. 2002, pages 380–388.

[Che+20] Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hulsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, Zhenfei Zhang, Tsunekazu Saito, Takashi Yamakawa, and Keita Xagawa. *NTRU*. Technical report. Available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions. National Institute of Standards and Technology, 2020.

[CJL16] Jung Hee Cheon, Jinhyuck Jeong, and Changmin Lee. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero. In: *LMS Journal of Computation and Mathematics* 19.A (2016), pages 255–266.

[CN11] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. In: *Asiacrypt*. 2011, pages 1–20.

[COT16] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. Polynomial time attack on wild McEliece over quadratic extensions. In: *IEEE Transactions on Information Theory* 63.1 (2016), pages 404–427. ISSN: 0018-9448.

[CR88] Benny Chor and Ronald L. Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. In: *IEEE Transactions on Information Theory* 34.5 (1988), pages 901–909.

[CS13] John Horton Conway and Neil James Alexander Sloane. Sphere packings, lattices and groups. Volume 290. Springer Science & Business Media, 2013.

[CS97] Don Coppersmith and Adi Shamir. Lattice Attacks on NTRU. In: *Eurocrypt*. 1997, pages 52–61.

[Dam02] Ivan Damgård. On Σ-protocols. In: *Lecture Notes, University of Aarhus, Department for Computer Science* (2002).

[DB15] Daniel Dadush and Nicolas Bonifas. Short paths on the Voronoi graph and closest vector problem with preprocessing. In: *Proceedings of the twenty-sixth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics. 2015, pages 295–314.

[DDGR20] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. LWE with side information: attacks and concrete security estimation. In: *Annual International Cryptology Conference*. Springer. 2020, pages 329–358.

[DDW22] Thomas Debris-Alazard, Leo Ducas, and Wessel van Woerden. An Algorithmic Reduction Theory for Binary Codes: LLL and more. In: *IEEE Transactions on Information Theory* (2022), pages 1–1.

[DE+04] Persi Diaconis, Paul Erdös, et al. On the distribution of the greatest common divisor. In: *A festschrift for Herman Rubin*. Institute of Mathematical Statistics, 2004, pages 56–61.

[DG22] Léo Ducas and Shane Gibbons. Hull Attacks on the Lattice Isomorphism Problem. To appear. 2022.

[DHVW20] Mathieu Dutour Sikirić, Anna Haensch, John Voight, and Wessel van Woerden. A canonical form for positive definite matrices. In: *ANTS XIV* 4.1 (2020), pages 179–195.

[Dij59] Edsger W. Dijkstra. A note on two problems in connexion with graphs. In: *Numerische Mathematik* 1.1 (1959), pages 269–271.

[DLW19] Emmanouil Doulgerakis, Thijs Laarhoven, and Benne de Weger. Finding closest lattice vectors using approximate Voronoi cells. In: *PQCrypto*. 2019.

[DLW20a] Emmanouil Doulgerakis, Thijs Laarhoven, and Benne de Weger. Sieve, Enumerate, Slice, and Lift. In: Springer, 2020, pages 301–320.

[DLW20b] Léo Ducas, Thijs Laarhoven, and Wessel van Woerden. The randomized slicer for CVPP: sharper, faster, smaller, batchier. In: *IACR International Conference on Public-Key Cryptography*. Springer. 2020, pages 3–36.

[DM13] Daniel Dadush and Daniele Micciancio. Algorithms for the densest sub-lattice problem. In: *Proceedings of the twenty-fourth annual ACM-SIAM symposium on Discrete algorithms*. SIAM. 2013, pages 1103–1122.

[DMW22] Mathieu Dutour Sikirić, Alexander Magazinov, and Wessel van Woerden. The complete classification of six-dimensional C-types. In: *To appear.* (2022).

[DP19] Léo Ducas and Cécile Pierrot. Polynomial time bounded distance decoding near minkowski's bound in discrete logarithm lattices. In: *Designs, Codes and Cryptography* 87.8 (2019), pages 1737–1748.

[DPPW22] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden. Hawk: Module LIP makes Lattice Signatures Fast, Compact and Simple. In: *Asiacrypt, 28th Annual International Conference* (2022).

[DST19] Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. Wave: A new family of trapdoor one-way preimage sampleable functions based on codes. In: Springer, 2019, pages 21–51.

[DSW21] Léo Ducas, Marc Stevens, and Wessel van Woerden. Advanced Lattice Sieving on GPUs, with Tensor Cores. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2021, pages 249–279.

[Duc18] Léo Ducas. Shortest vector from lattice sieving: a few dimensions for free. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2018, pages 125–145.

[Duc22] Léo Ducas. Estimating the Hidden Overheads in the BDGL Lattice Sieving Algorithm. In: *International Conference on Post-Quantum Cryptography*. Springer. 2022, pages 480–497.

[Dum91] Ilya Dumer. On minimum distance decoding of linear codes. In: 1991, pages 50–52.

[Dut22] Mathieu Dutour Sikirić. Polytopes, lattices and quadratic forms programs. Available at https://github.com/MathieuDutSik/polyhedral_common. 2022.

[DW18] Léo Ducas and Wessel van Woerden. The closest vector problem in tensored root lattices of type A and in their duals. In: *Designs, Codes and Cryptography* 86.1 (2018), pages 137–150.

[DW21] Léo Ducas and Wessel van Woerden. NTRU Fatigue: How Stretched is Overstretched? In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2021, pages 3–32.

[DW22] Léo Ducas and Wessel van Woerden. On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2022, pages 643–673.

[EHKS14] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In: *STOC*. ACM. 2014, pages 293–302.

[EV22] Friedrich Eisenbrand and Moritz Venzin. Approximate CVPp in time 20.802 n. In: *Journal of Computer and System Sciences* 124 (2022), pages 129–139. ISSN: 0022-0000.

[Fit+14] Robert Fitzpatrick, Christian Bischof, Johannes Buchmann, Özgür Dagdelen, Florian Göpfert, Artur Mariano, and Bo-Yin Yang. Tuning GaussSieve for speed. In: *International Conference on Cryptology and Information Security in Latin America*. Springer. 2014, pages 288–305.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In: Springer, 1999, pages 537–554.

[FP85] Ulrich Fincke and Michael Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. In: *Mathematics of computation* 44.170 (1985), pages 463–471.

[FSS83] Martin Fürer, Walter Schnyder, and Ernst Specker. Normal forms for trivalent graphs and graphs of bounded valence. In: *Proceedings of the fifteenth annual ACM symposium on Theory of computing*. 1983, pages 161–170.

[FSW14] Felix Fontein, Michael Schneider, and Urs Wagner. PotLLL: a polynomial time version of LLL with deep insertions. In: *Designs, codes and cryptography* 73.2 (2014), pages 355–368. ISSN: 1573-7586.

[Gab85] Ernest Mukhamedovich Gabidulin. Theory of codes with maximum rank distance. In: *Problemy peredachi informatsii* 21.1 (1985), pages 3–16. ISSN: 0555-2923.

[Gab95] Ernst M. Gabidulin. Public-key cryptosystems based on linear codes. Citeseer, 1995.

[Gen+19] Nicholas Genise, Craig Gentry, Shai Halevi, Baiyu Li, and Daniele Micciancio. Homomorphic encryption for finite automata. In: Springer, 2019, pages 473–502.

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate Multilinear Maps from Ideal Lattices. In: *Eurocrypt*. 2013, pages 1–17.

[GHKN06] Nicolas Gama, Nick Howgrave-Graham, Henrik Koy, and Phong Q. Nguyen. Rankin's constant and blockwise lattice reduction. In: *Annual International Cryptology Conference*. Springer. 2006, pages 112–130.

[GMSS99] Oded Goldreich, Daniele Micciancio, Shmuel Safra, and Jean-Pierre Seifert. Approximating Shortest Lattice Vectors is not Harder than Approximating Closest Lattice Vectors. In: *Inf. Process. Lett.* 71.2 (1999), pages 55–61.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. In: *Journal of the ACM (JACM)* 38.3 (1991), pages 690–728.

[GN08a] Nicolas Gama and Phong Q. Nguyen. Finding short lattice vectors within mordell's inequality. In: *Proceedings of the fortieth annual ACM symposium on Theory of computing*. ACM. 2008, pages 207–216.

[GN08b] Nicolas Gama and Phong Q. Nguyen. Predicting Lattice Reduction. In: *Eurocrypt*. 2008, pages 31–51.

[GNR10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. Lattice Enumeration Using Extreme Pruning. In: *Eurocrypt*. 2010, pages 257–278.

[GP12] Elena Grigorescu and Chris Peikert. List Decoding Barnes-Wall Lattices. In: *IEEE Conference on Computational Complexity*. 2012, pages 316–325.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In: *STOC*. 2008, pages 197–206.

[Gri60] James H. Griesmer. A bound for error-correcting codes. In: *IBM Journal of Research and Development* 4.5 (1960), pages 532–542. ISSN: 0018-8646.

[GS02] Craig Gentry and Michael Szydlo. Cryptanalysis of the Revised NTRU Signature Scheme. In: *Eurocrypt*. 2002, pages 299–320.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. In: *SIAM Journal on Computing* 28.4 (1999), pages 1364–1396.

[HK17] Gottfried Herold and Elena Kirshanova. Improved algorithms for the approximate k-list problem in Euclidean norm. In: *IACR International Workshop on Public Key Cryptography*. Springer. 2017, pages 16–40.

[HKL18] Gottfried Herold, Elena Kirshanova, and Thijs Laarhoven. Speed-ups and time–memory trade-offs for tuple lattice sieving. In: *IACR International Workshop on Public Key Cryptography*. Springer. 2018, pages 407–436.

[HM19] Nicholas J. Higham and Theo Mary. A new approach to probabilistic rounding error analysis. In: *SIAM Journal on Scientific Computing* 41.5 (2019), A2815–A2835.

[HP10] W. Cary Huffman and Vera Pless. Fundamentals of error-correcting codes. Cambridge university press, 2010.

[HPS11a] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Algorithms for the shortest and closest lattice vector problems. In: *International Conference on Coding and Cryptology*. Springer, 2011, pages 159–190.

[HPS11b] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In: Springer, 2011, pages 447–464.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In: *ANTS*. 1998, pages 267–288.

[HR14] Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In: *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*. SIAM. 2014, pages 391–404.

[IKMT14] Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, and Tsuyoshi Takagi. Parallel Gauss sieve algorithm: Solving the SVP challenge over a 128-dimensional ideal lattice. In: *International Workshop on Public Key Cryptography*. Springer, 2014, pages 411–428.

[IM98] Piotr Indyk and Rajeev Motwani. Approximate nearest neighbors: towards removing the curse of dimensionality. In: 1998, pages 604–613.

[JK07] Tommi Junttila and Petteri Kaski. Engineering an efficient canonical labeling tool for large and sparse graphs. In: *2007 Proceedings of the Ninth Workshop on Algorithm Engineering and Experiments (ALENEX)*. SIAM, 2007, pages 135–149.

[Kan83] Ravi Kannan. Improved Algorithms for Integer Programming and Related Lattice Problems. In: *STOC*. 1983, pages 193–206.

[KB79] Ravindran Kannan and Achim Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. In: *siam Journal on Computing* 8.4 (1979), pages 499–507.

[Ker+22] Andrew Kerr, Haicheng Wu, Manish Gupta, Dustyn Blasig, Pradeep Ramini, Duane Merrill, Aniket Shivam, Piotr Majcher, Paul Springer, Markus Hohnerbach, Jin Wang, and Matt Nicely. *CUTLASS*. Version 2.9. Available at https://github.com/NVIDIA/cutlass. Apr. 2022.

[KF17] Paul Kirchner and Pierre-Alain Fouque. Revisiting lattice attacks on overstretched NTRU parameters. In: Springer, 2017, pages 3–26.

[KL20] Jonathan Katz and Yehuda Lindell. Introduction to modern cryptography. CRC press, 2020.

[Kle00] Philip N. Klein. Finding the closest lattice vector when it's unusually close. In: *SODA*. 2000, pages 937–941.

[Laa15] Thijs Laarhoven. Sieving for shortest vectors in lattices using angular locality-sensitive hashing. In: *Annual Cryptology Conference*. Springer. 2015, pages 3–22.

[Laa16] Thijs Laarhoven. Sieving for closest lattice vectors (with preprocessing). In: *SAC*. 2016, pages 523–542.

[Laa19] Thijs Laarhoven. Approximate Voronoi cells for lattices, revisited. In: *MathCrypt*. 2019.

[Lap21] Oleksandra Lapiha. Comparing Lattice Families for Bounded Distance Decoding near Minkowski's Bound. Cryptology ePrint Archive, Report 2021/1052. 2021.

[LB88] Pil Joong Lee and Ernest F. Brickell. An observation on the security of McEliece's public-key cryptosystem. In: Springer, 1988, pages 275–280.

[Len91] Hendrik W Lenstra. On the Chor-Rivest knapsack cryptosystem. In: *Journal of Cryptology* 3.3 (1991), pages 149–155.

[LLL82] Arjen K. Lenstra, Hendrik W. Lenstra Jr., and László Lovász. Factoring polynomials with rational coefficients. In: *Mathematische Annalen* 261.4 (Dec. 1982), pages 515–534.

[LLXY20] Zhe Li, San Ling, Chaoping Xing, and Sze Ling Yeo. On the bounded distance decoding problem for lattices constructed and their cryptographic applications. In: *IEEE Transactions on Information Theory* 66.4 (2020), pages 2588–2598.

[LM09] Vadim Lyubashevsky and Daniele Micciancio. On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem. In: *Crypto*. 2009, pages 577–594.

[LM18] Thijs Laarhoven and Artur Mariano. Progressive lattice sieving. In: *International Conference on Post-Quantum Cryptography*. Springer. 2018, pages 292–311.

[LN14] Jianwei Li and Phong Q. Nguyen. Approximating the densest sublattice from Rankin's inequality. In: *LMS Journal of Computation and Mathematics* 17.A (2014), pages 92–111.

[LN20] Jianwei Li and Phong Q. Nguyen. A complete analysis of the BKZ lattice reduction algorithm. Cryptology ePrint Archive, Report 2020/1237. 2020.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On Ideal Lattices and Learning with Errors Over Rings. In: *Journal of the ACM* 60.6 (Nov. 2013). Preliminary version in Eurocrypt 2010, 43:1–43:35.

[LS14] Hendrik W. Lenstra and Alice Silverberg. Revisiting the gentry-szydlo algorithm. In: *Annual Cryptology Conference*. Springer. 2014, pages 280–296.

[LW20] Changmin Lee and Alexandre Wallet. Lattice analysis on MiNTRU problem. Cryptology ePrint Archive, Report 2020/230. 2020.

[MBL15] Artur Mariano, Christian Bischof, and Thijs Laarhoven. Parallel (probable) lock-free hash sieve: A practical sieving algorithm for the SVP. In: *2015 44th International Conference on Parallel Processing*. IEEE, 2015, pages 590–599.

[McE78] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. In: *Coding Thv* 4244 (1978), pages 114–116.

[McK07] Brendan D. McKay. Nauty user's guide (version 2.4). In: *Computer Science Dept., Australian National University* (2007), pages 225–239.

[McK81] Brendan D. McKay. Practical graph isomorphism. In: (1981).

[MDB14] Artur Mariano, Özgür Dagdelen, and Christian Bischof. A comprehensive empirical comparison of parallel ListSieve and GaussSieve. In: *European Conference on Parallel Processing*. Springer, 2014, pages 48–59.

[MG02] Daniele Micciancio and Shafi Goldwasser. Complexity of Lattice Problems: a cryptographic perspective. Volume 671. The Kluwer International Series in Engineering and Computer Science. Boston, Massachusetts: Kluwer Academic Publishers, 2002.

[Mic08] Daniele Micciancio. Efficient reductions among lattice problems. In: *SODA*. 2008, pages 84–93.

[Min97] Hermann Minkowski. Allgemeine Lehrsatze uber die konvexen Polyeder. In: *Nachr. Ges. Wiss. Gottingen, Math.-Phys. KL* (1897), pages 198–219.

[MLB17] Artur Mariano, Thijs Laarhoven, and Christian Bischof. A parallel variant of LDSieve for the SVP on lattices. In: *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. IEEE. 2017, pages 23–30.

[MMT11] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$. In: Springer, 2011, pages 107–124.

[MN08] Daniele Micciancio and Antonio Nicolosi. Efficient bounded distance decoders for Barnes-Wall lattices. In: *2008 IEEE International Symposium on Information Theory*. IEEE. 2008, pages 2484–2488.

[MO15] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In: Springer, 2015, pages 203–228.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In: *Eurocrypt*. 2012, pages 700–718.

[MP14] Brendan D. McKay and Adolfo Piperno. Practical graph isomorphism, II. In: *Journal of symbolic computation* 60 (2014), pages 94–112.

[MP21] Ethan Mook and Chris Peikert. Lattice (List) Decoding Near Minkowski's Inequality. In: *IEEE Transactions on Information Theory* (2021). ISSN: 0018-9448.

[MR07] Daniele Micciancio and Oded Regev. Worst-Case to Average-Case Reductions Based on Gaussian Measures. In: *SIAM J. Comput.* 37.1 (Apr. 2007), pages 267–302. ISSN: 0097-5397.

[MR09] Daniele Micciancio and Oded Regev. Lattice-based Cryptography. In: *Post Quantum Cryptography*. Springer, Feb. 2009, pages 147–191.

[MS01] Alexander May and Joseph H. Silverman. Dimension reduction methods for convolution modular lattices. In: *International Cryptography and Lattices Conference*. Springer. 2001, pages 110–125.

[MS11] Benjamin Milde and Michael Schneider. A parallel implementation of GaussSieve for the shortest vector problem in lattices. In: *International Conference on Parallel Computing Technologies*. Springer, 2011, pages 452–458.

[MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. The theory of error correcting codes. Volume 16. Elsevier, 1977.

[MTB14] Artur Mariano, Shahar Timnat, and Christian Bischof. Lock-free GaussSieve for linear speedups in parallel high performance SVP calculation. In: *2014 IEEE 26th International Symposium on Computer Architecture and High Performance Computing*. IEEE, 2014, pages 278–285.

[Mul54] David E. Muller. Application of Boolean algebra to switching circuit design and to error detection. In: *Transactions of the IRE professional group on electronic computers* 3 (1954), pages 6–12. ISSN: 2168-1740.

[MV10] Daniele Micciancio and Panagiotis Voulgaris. Faster Exponential Time Algorithms for the Shortest Vector Problem. In: *SODA*. 2010, pages 1468–1480.

[MV13] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. In: *SIAM Journal on Computing* 42.3 (2013), pages 1364–1391.

[MW01] Daniele Micciancio and Bogdan Warinschi. A linear space algorithm for computing the Hermite normal form. In: *ISSAC*. 2001, pages 231–236.

[MW16] Daniele Micciancio and Michael Walter. Practical, predictable lattice basis reduction. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2016, pages 820–849.

[NBGS08] John Nickolls, Ian Buck, Michael Garland, and Kevin Skadron. Scalable parallel programming with CUDA. In: *Queue* 6.2 (2008), pages 40–53.

[NS11] Gabriele Nebe and Neil Sloane. Table of the Highest Kissing Numbers Presently Known. Available at http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/kiss.html. 2011.

[NV08] Phong Q. Nguyen and Thomas Vidick. Sieve Algorithms for the Shortest Vector Problem Are Practical. In: *Journal of Mathematical Cryptology* (2008).

[NVF20] NVIDIA, Péter Vingelmann, and Frank H.P. Fitzek. CUDA, release: 10.2.89. Available at https://developer.nvidia.com/cuda-toolkit. 2020.

[NVI] NVIDIA. cuBLAS: Basic Linear Algebra on NVIDIA GPUs. Available at https://developer.nvidia.com/cublas.

[Odl90] Andrew M. Odlyzko. The rise and fall of knapsack cryptosystems. In: *Cryptology and Computational Number Theory*. Edited by C. Pomerance. Volume 42. Proceedings of Symposia in Applied Mathematics. 1990, pages 75–88.

[OS09] Raphael Overbeck and Nicolas Sendrier. Code-based cryptography. In: Springer, 2009, pages 95–145.

[OTU00] Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama. Quantum public-key cryptosystems. In: *Annual international cryptology conference*. Springer. 2000, pages 147–165.

[Pei10] Chris Peikert. An Efficient and Parallel Gaussian Sampler for Lattices. In: *Crypto*. 2010, pages 80–97.

[Poh87] Michael Pohst. A modification of the LLL reduction algorithm. In: *Journal of Symbolic Computation* 4.1 (1987), pages 123–127. ISSN: 0747-7171.

[PP02] Athanasios Papoulis and S Unnikrishna Pillai. Probability, random variables, and stochastic processes. Tata McGraw-Hill Education, 2002.

[PP85] Wilhelm Plesken and Michael Pohst. Constructing integral lattices with prescribed minimum. I. In: *mathematics of computation* 45.171 (1985), pages 209–221.

[PR06] Chris Peikert and Alon Rosen. Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices. In: *TCC*. 2006, pages 145–166.

[Pra62] Eugene Prange. The use of information sets in decoding cyclic codes. In: *IRE Transactions on Information Theory* 8.5 (1962), pages 5–9. ISSN: 0096-1000.

[Pre+20] 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. Available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions. National Institute of Standards and Technology, 2020.

[PS09] Xavier Pujol and Damien Stehlé. Solving the Shortest Lattice Vector Problem in Time 22.465 n. 2009.

[PS97] Wilhelm Plesken and Bernd Souvignier. Computing isometries of lattices. In: *Journal of Symbolic Computation* 24.3-4 (1997), pages 327–334.

[PT08] Gábor Pataki and Mustafa Tural. On sublattice determinants in reduced bases. arXiv preprint arXiv:0804.4014. 2008.

[PV21] Eamonn W. Postlethwaite and Fernando Virdia. On the success probability of solving unique SVP via BKZ. In: Springer, 2021, pages 68–98.

[PW11] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In: *SIAM Journal on Computing* 40.6 (2011), pages 1803–1844.

[Rab79] Michael O. Rabin. *Digitalized signatures and public-key functions as intractable as factorization.* Technical report. 1979.

[Ree53] Irving S. Reed. *A class of multiple-error-correcting codes and the decoding scheme.* Technical report. 1953.

[Reg04] Oded Regev. Quantum Computation and Lattice Problems. In: *SIAM J. Comput.* 33.3 (2004). Preliminary version in FOCS 2002, pages 738–760.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In: *J. ACM* 56.6 (2009). Preliminary version in STOC 2005, pages 1–40.

[RV22] Thomas Rothvoss and Moritz Venzin. Approximate in Time-Now in Any Norm! In: Springer, 2022, pages 440–453.

[Sch03] Claus-Peter Schnorr. Lattice Reduction by Random Sampling and Birthday Methods. In: *STACS*. 2003, pages 145–156.

[Sch87] Claus-Peter Schnorr. A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms. In: *Theor. Comput. Sci.* 53 (1987), pages 201–224.

[Sch94] Claus-Peter Schnorr. Block reduced lattice bases and successive minima. In: *Combinatorics, Probability and Computing* 3.4 (1994), pages 507–522. ISSN: 1469-2163.

[SCM01] Patrick Solé, Chris Charnes, and Bruno Martin. A lattice-based McEliece scheme for encryption and signature. In: *Electronic Notes in Discrete Mathematics* 6 (2001), pages 402–411.

[SE94] Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. In: *Mathmatical Programming* 66 (1994), pages 181–199.

[Sen00] Nicolas Sendrier. Finding the permutation between equivalent linear codes: The support splitting algorithm. In: *IEEE Transactions on Information Theory* 46.4 (2000), pages 1193–1203.

[SFS09] Naftali Sommer, Meir Feder, and Ofir Shalvi. Finding the closest lattice point by iterative slicing. In: *SIAM Journal on Discrete Mathematics* 23.2 (2009), pages 715–731.

[SG10] Michael Schneider and Nicolas Gama. Darmstadt SVP Challenges. Accessed: 16-02-2022. 2010.

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In: *FOCS*. 1994, pages 124–134.

[Sie45] Carl Ludwig Siegel. A mean value theorem in geometry of numbers. In: *Annals of Mathematics* (1945), pages 340–347. ISSN: 0003-486X.

[SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient Public Key Encryption Based on Ideal Lattices. In: *Asiacrypt*. 2009, pages 617–635.

[SSV07] Mathieu Sikirić, Achill Schürmann, and Frank Vallentin. Classification of eight-dimensional perfect forms. In: *Electronic Research Announcements of the American Mathematical Society* 13.3 (2007), pages 21–32.

[Ste88] Jacques Stern. A method for finding codewords of small weight. In: Springer, 1988, pages 106–113.

[Szy03] Michael Szydlo. Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2003, pages 433–448.

[tea21a] The FPLLL development team. FPLLL, a lattice reduction library, Version: 5.4.1. Available at https://github.com/fplll/fplll. 2021.

[tea21b] The FPLLL development team. fpylll, a Python wraper for the fplll lattice reduction library, Version: 0.5.6. Available at https://github.com/fplll/fpylll. 2021.

[TV95] Michael A. Tsfasman and Serge G. Vladut. Geometric approach to higher weights. In: *IEEE Transactions on Information Theory* 41.6 (1995), pages 1564–1588.

[Var97] Alexander Vardy. The intractability of computing the minimum distance of a code. In: *IEEE Transactions on Information Theory* 43.6 (1997), pages 1757–1766. ISSN: 0018-9448.

[Vlă19] Serge Vlăduţ. Lattices with exponentially large kissing numbers. In: *Moscow Journal of Combinatorics and Number Theory* 8.2 (2019), pages 163–177.

[Vor08] Georges Voronoi. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs. In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1908.134 (1908), pages 198–287.

[Vor09] Georges Voronoi. Nouvelles applications des paramètres continus à théorie des formes quadratiques. Deuxième Mémoire. Recherches sur les paralléloèdres primitifs. In: *Journal für die reine und angewandte Mathematik* 1909.136 (1909), pages 67–182.

[Wal21] Michael Walter. The Convergence of Slide-type Reductions. In: Springer, 2021, pages 45–67.

[Wei91] Victor K. Wei. Generalized Hamming weights for linear codes. In: *IEEE Transactions on information theory* 37.5 (1991), pages 1412–1418.

[Woe18] Wessel P.J. van Woerden. Perfect quadratic forms: an upper bound and challenges in enumeration. Master's thesis. Leiden University, 2018.

[Woe20] Wessel van Woerden. An upper bound on the number of perfect quadratic forms. In: *Advances in Mathematics* 365 (2020), page 107031.

[YD17] Yang Yu and Léo Ducas. Second order statistical behavior of LLL and BKZ. In: Springer, 2017, pages 3–22.

[YKYC17] Shang-Yi Yang, Po-Chun Kuo, Bo-Yin Yang, and Chen-Mou Cheng. Gauss sieve algorithm on GPUs. In: *Cryptographers' Track at the RSA Conference*. Springer. 2017, pages 39–57.