



Universiteit
Leiden
The Netherlands

Lattice cryptography: isomorphisms & dual attacks

Pulles, L.N.

Citation

Pulles, L. N. (2026, September 23). *Lattice cryptography: isomorphisms & dual attacks*. Retrieved from <https://hdl.handle.net/1887/4309918>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/4309918>

Note: To cite this publication please use the final published version (if applicable).

Lattice Cryptography: Isomorphisms & Dual Attacks

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr. S. de Rijcke,
volgens besluit van het college voor promoties
te verdedigen op woensdag 23 september 2026
klokke 16:00 uur

door

Ludo Niels Pulles
geboren te Wageningen
in 1997

Promotores:

Prof.dr. L. Ducas (CWI & Universiteit Leiden)

Prof.dr. R.J.F. Cramer (CWI & Universiteit Leiden)

Promotiecomissie:

Prof.dr.ir. G.L.A. Derks

Prof.dr. S. Fehr (CWI & Universiteit Leiden)

Prof.dr. C. Ling (Imperial College London)

Prof.dr. P.Q. Nguyen (Inria Paris & École normale supérieure – PSL)

Dr. T. Debris-Alazard (Inria Saclay & École polytechnique)

The author of this thesis carried out his research at Centrum Wiskunde & Informatica (CWI) in the Cryptology group. The PhD position was funded by ERC Starting Grant project ARTICULATE (no. 947821).



Centrum Wiskunde & Informatica



**Universiteit
Leiden**

Lattice Cryptography: Isomorphisms & Dual Attacks

Ludo Niels Pulles

© 2026 L.N. Pulles

ISBN 978-90-6196-440-7

Book cover by Puck Swildens

Printed & bound by Ridderprint

Contents

List of Algorithms	viii
List of Tables	xi
List of Figures	xiii
List of Publications	xv
I Introduction & Preliminaries	1
1 Introduction	3
1.1 Motivation	11
1.2 Overview	20
2 Preliminaries	23
2.1 Elementary theory	23
2.1.1 Terminology	23
2.1.2 Geometric objects	24
2.1.3 Probability theory	25
2.1.4 Fourier transform	28
2.2 Lattice	28
2.2.1 Lattice basis	32
2.2.2 Random lattice	36
2.2.3 Hard problems	40
2.2.4 Projection	45
2.2.5 Lattice isomorphism	47
2.2.6 Module lattice and Hermitian form	49

2.3	Duality	52
2.3.1	Dual basis	55
2.3.2	Discrete Fourier transform	56
2.4	Discrete Gaussian sampling	56
2.4.1	Smoothing parameter	58
2.5	Lattice basis reduction	58
2.5.1	Babai’s reduction algorithms	59
2.5.2	Size reduction	62
2.5.3	Lagrange reduction	68
2.5.4	Lenstra–Lenstra–Lovász	70
2.5.5	Block Korkine–Zolotarev	75
2.6	Lattice sieving	80
2.7	Signature scheme	82

II Dual-Sieve Attack 83

3 Dual-Sieve Attack Heuristics 85

3.1	Introduction	86
3.1.1	Contributions	87
3.1.2	Coding theory analogue	89
3.2	Dual attack	90
3.2.1	Solving decision-BDD	90
3.2.2	Reducing search-BDD to decision-BDD	91
3.3	Prior dual attack models	92
3.3.1	Laarhoven–Walter	92
3.3.2	Guo–Johansson and MATZOV	95
3.4	Generalisation of the Dual-Sieve-FFT attack	96
3.4.1	Abstracting Guo–Johansson	97
3.4.2	Implementation	98
3.4.3	Advantages	99
3.5	Contradictions to the independent score heuristic	101
3.5.1	Distinguishing the indistinguishable	102
3.5.2	Candidates closer than the solution (asymptotic)	105
3.5.3	Candidates closer than the solution (concrete)	107
3.6	Experiments	110
3.6.1	Implementation details	111
3.6.2	Uniform targets	112
3.6.3	BDD targets	112

3.7	Conclusion	116
3.7.1	Possible pitfalls	116
3.7.2	Possible improvements	117
4	Accurate Score Prediction for Dual-Sieve Attacks	119
4.1	Introduction	120
4.1.1	Contributions	120
4.1.2	Related work	122
4.2	Bessel function	122
4.2.1	Relation to the Fourier transform	124
4.3	Score distribution models	125
4.3.1	Individual score function	125
4.3.2	Total score function	127
4.3.3	Radial error distributions	129
4.3.4	Error uniform modulo lattice	131
4.4	Experiments	133
4.4.1	Implementation details	134
4.4.2	BDD targets	135
4.4.3	Uniform targets	135
4.5	Conclusion	138
4.5.1	Future work	141
III	Lattice Isomorphism Problem	143
5	Hawk Signature Scheme	145
5.1	Introduction	146
5.1.1	Contributions	146
5.2	Scheme	150
5.2.1	Uncompressed Hawk	150
5.2.2	(Compressed) Hawk	154
5.3	Cryptanalysis	156
5.3.1	Signature sampling	157
5.3.2	Key recovery	158
5.3.3	Signature forgery	163
5.4	Parameters and performance	164
5.4.1	Parameter selection	165
5.4.2	Encoding	167
5.4.3	Performance	169

5.5	Implementation details	169
5.5.1	Key generation	172
5.5.2	Signature generation	176
5.5.3	Signature verification	179
5.6	Formal reductions	183
5.6.1	Module LIP self reduction	183
5.6.2	Inapplicability of PSF framework	190
5.6.3	One more shortest vector problem	192
6	Solving Module-LIP using Automorphisms	205
6.1	Introduction	206
6.1.1	Contributions	207
6.2	Main result	208
6.3	Heuristic hardness of SVP	212
6.4	Group-theoretic heuristics	214
6.5	Conclusion	215
	Bibliography	217
	List of Acronyms	251
	List of Symbols	253
	Samenvatting	257
	Summary	259
	Acknowledgments	261
	Curriculum Vitæ	263

List of Algorithms

2.1	SAMPLERANDOM: sampler for Goldstein–Mayer lattices . . .	37
2.2	RO($\mathbf{B}, \mathbf{t}$): Rounding-Off algorithm	60
2.3	NP($\mathbf{B}, \mathbf{t}$): Babai’s Nearest-Plane algorithm	61
2.4	SIZEREDUCE($\mathbf{B}$): size reduction of a basis	62
2.5	SEYSENREDUCE($\mathbf{R}$): Seysen-reduction of a basis	66
2.6	LAGRANGEREDUCE($\mathbf{b}_1, \mathbf{b}_2$): Lagrange basis reduction . . .	69
2.7	LLL($\mathbf{B}, \delta$): LLL basis reduction	73
2.8	BKZ($\mathbf{B}, \beta$): BKZ basis reduction	76
3.1	DUALFFT($\mathbf{B}, \mathbf{B}', \mathcal{W}, \mathbf{t}$): Dual-Sieve-FFT attack	99
5.1	KEYGEN(1^n): HAWK key generation	152
5.2	SIGN $\mathbf{B}$ ($\mathbf{m}$): HAWK signature generation	152
5.3	VERIFY $\mathbf{Q}$ ($\mathbf{m}, \text{sig}$): HAWK signature verification	153
5.4	SAMPLER $\mathbb{Z}(c)$: sampler for $2\mathbb{Z} + c$ with std. dev. $2\sigma_{\text{sign}}$. .	179
5.5	HERMITESOLVE($\mathbb{K}, f, g$): basis completion (if possible) . .	185
5.6	REDUCE($\mathbf{Q}, \mathbf{y}_1, \mathbf{y}_2$): size reduction of $\mathbf{y}_2$ w.r.t. $\mathbf{Q}$ and $\mathbf{y}_1$.	186
5.7	AC $_{\mathbb{K}, \sigma}(\mathbf{Q})$: sampler for AC $_{\mathbb{K}, \sigma}([\mathbf{Q}]_{\text{sl}})$	187

List of Tables

2.1	Known Hermite constants	31
3.1	Experimental BDD score distribution versus prediction . .	115
5.1	Performance of FALCON and HAWK	148
5.2	Key and signature sizes of FALCON and HAWK	149
5.3	Parameter sets for HAWK and their estimated security . .	166
5.4	Performance of dynamic signing for FALCON and HAWK .	170

List of Figures

1.1	Public-key encryption	4
1.2	Landscape of quantum computing capabilities in 2025	7
1.3	Digital signature scheme	9
1.4	Two examples of a lattice	12
1.5	Tiling using a good and a bad basis	13
1.6	High-level idea of a lattice-based signature scheme	13
1.7	Solving BDD by finding the nearest coset to the target	15
1.8	Dual vector visualisation	16
1.9	Lattice Isomorphism Problem	17
2.1	Voronoi diagram of the hexagonal lattice	30
2.2	Search bounded distance decoding with $\alpha = 0.49$	41
2.3	Fundamental domain of $\mathbf{B}$	59
2.4	Babai's domain of $\mathbf{B}$	61
2.5	Possible final state of Algorithm 2.6	69
2.6	Situation in which Lovász' condition holds	72
2.7	Example of a basis profile before and after BKZ reduction	79
3.1	Simulation of the dual basis profile	100
3.2	Equation $e^2 \ln(x) = x^2 r^2$ for various r	103
3.3	Concrete contradictory regime	108
3.4	Survival function of score for uniform targets	113
3.5	CDF of score for Gaussian BDD targets	114
4.1	CDF of score for BDD targets at distance $0.7 \text{ GH}(n)$	136
4.2	CDF of score for BDD targets at distance $0.5 \text{ GH}(n)$	137
4.3	Survival function of score for uniform targets with saturation radius $r_{\text{sat}} = \sqrt{4/3}$	139

4.4	Survival function of score for uniform targets with a different saturation radius	140
5.1	Illustration of signing	151
5.2	Summary of necessary relationships between various $\sigma_{\bullet}$	157
5.3	Block size required to recover a shortest vector via lattice reduction as a function of dimension d	160
5.4	Block size required to recover a shortest vector via lattice reduction as a function of the standard deviation $\widetilde{\sigma_{\text{pk}}}$	161
5.5	Shortest basis vector length before the recovery of a length one vector, given in terms of σ_{sec}	162
5.6	ROM-SUF-CMA game	193
5.7	SAMPLE game	197
6.1	Reductions related to SUF-CMA security of HAWK	209

List of Publications

This is a comprehensive list of all the publications and preprints that the author has contributed to during their PhD programme. Each publication here lists authors alphabetically ordered. Each author has contributed equally to each publication.

Four chapters from this thesis are based on the following published papers, ordered chronologically.

- [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.
- [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.
- [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.
- [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.

This thesis is also based on the following specification document submitted to NIST for the standardisation of additional signature schemes.

- [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>.

In addition, the author has published the following papers that are not part of this thesis.

- [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.

- [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.

- [KKN⁺26] Alexander Karenin, Elena Kirshanova, Julian Nowakowski, Eamonn W. Postlethwaite, Ludo N. Pulles, Fernando Viridia, 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.

Finally, the author authored the following preprint that is not part of this thesis.

- [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>.