Lattice cryptography: isomorphisms & dual attacks

Pulles, L.N.

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

ISBN 978-90-6196-440-7
Book cover by Puck Swildens
Printed & bound by Ridderprint

Contents

List of Algorithms

List of Tables

List of Figures

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 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.

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.