LUDO PULLES

Utrecht, NLD | ludiq.eu | ludopulles | ludopulles | 0000-0002-8014-9221

WORK EXPERIENCE

Ph.D. in Cryptology
2021 – 2025

Centrum Wiskunde & Informatica — Amsterdam

- Subject: cryptanalysis in lattice-based cryptography.
- Supervisor: Léo Ducas
- Research visit: collaboration with Damien Stehlé at CryptoLab in Lyon (France) in September 2024.
  Topic: *security of sparse-secret LWE*.

EDUCATION

M.Sc. in Mathematics
2019 – 2021

Leiden University

- Specialization: Algebra, Geometry and Number theory.
- Thesis: *Finite Separable Rings* (grade 9.0)
  Supervisor: Prof. Dr. H.W. Lenstra Jr.
- *Cum Laude*

B.Sc. in Mathematics
2015 – 2018

Utrecht University

- Double bachelor with Computer Science and Physics.
- Thesis: *A theoretic background on Pollard's Rho algorithm* (grade 8.5)
- Honours student
- *Cum Laude*

B.Sc. in Computer Science
2015 – 2018

Utrecht University

- Double bachelor with Mathematics.
- Final project: developing software in a large team using SCRUM for ½ year.
- *Cum Laude*

B.Sc. in Physics
2015 – 2018

Utrecht University

- Double bachelor with Mathematics.
- *Cum Laude*

TEACHING EXPERIENCE

During Ph.D. (voluntarily):

- Modern Cryptology (MSc Math course, fall 2022)
- Competitive Programming (MSc CS course, spring 2022)

At Leiden University:

- Algebra/Getaltheorie (course for highschool teachers, spring 2021)
- Combinatorial Game Theory (BSc/MSc Math course, fall 2020)
- Competitive Programming (MSc CS course, spring 2020)
- Wiskundige Structuren (1st year Math course, fall 2019)

MOST PROUD OF

Winner of BAPC & NWERC 2019
These programming contests are the Benelux & Northwestern Europe qualifiers respectively for the ICPC World Finals, in which teams of three participate.

IOI Bronze medalist
140th place in International Olympiad in Informatics 2015, and winner of the national competition (NIO).

Android App 'RoosterSGN'
I developed an app to show the timetable of my high school.

STRENGTHS

Hard-working | Eye for detail

Algorithms | C/C++ | Python | PHP | Java | HTML, CSS & JavaScript | LaTeX | Linux | Git

LANGUAGES

Dutch	**Native**
English	**C1 Advanced**
French	**Basic level**

HOBBIES & INTERESTS

Project Euler
More than 500 math problems solved.

Kattis
Top 100 users ranklist (dated 1-1-2025).

Piano
I play classical piano pieces by mostly Chopin, Liszt & Rachmaninoff.

Cycling
Completed the 150 km Amstel Gold Race for amateurs in 2024.

VOLUNTEER WORK

Member Activity Committee
2021 – 2023
We organized social events for colleagues with an annual budget of 2k. Co-chair in 2023.
CWI, Amsterdam

Jury member BAPC
2018, 2020 – 2023
We prepared programming exercises, consisting of writing problem description, test data, and correct & wrong solutions.

Dutch Olympiad Informatics (NIO)
2016 – Now
I tested and gave feedback on the exercise sets, and prepared the exercises for the final round in 2020–2023.

Back-end developer for CodeCup
2016 – Now
The website hosts a board game competition between computer programs. Responsibility: website & back-end.

Website developer for A–Eskwadraat
2016 – 2018
Improved & fixed issues for the website of my study-association.
Utrecht

PUBLICATIONS

Conference Proceedings

- **L. N. Pulles** and M. Tibouchi, "Cryptanalysis of EagleSign," in *SCN 2024: 14th International Conference on Security in Communication Networks, Part II*, Sep. 2024, pp. 165–186.
- L. Ducas and **L. N. Pulles**, "Does the dual-sieve attack on learning with errors even work?" In *Advances in Cryptology – CRYPTO 2023, Part III*, Aug. 2023, pp. 37–69.
- L. Ducas, E. W. Postlethwaite, **L. N. Pulles**, and W. P. J. van Woerden, "Hawk: Module LIP makes lattice signatures fast, compact and simple," in *Advances in Cryptology – ASIACRYPT 2022, Part IV*, Dec. 2022, pp. 65–94.

In Submission

[omitted]

Preprints & Miscellaneous

- L. Ducas and **L. N. Pulles**, *Accurate score prediction for dual-sieve attacks*, URL: https://eprint.iacr.org/2023/1850.
- J. W. Bos et al., *HAWK*, Submission to NIST's on-ramp call for additional signature schemes. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures, 2024.

PRESENTATIONS

SCN 2024
12 September 2024
Title: Cryptanalysis of EagleSign
Amalfi (IT)

London-ish Lattice Meeting
15 March 2024
Title: Accurate Score Prediction for Dual-Sieve Attacks
London (UK)

ATTACC Workshop
5 February 2024
Title: Accurate Score Prediction for Dual-Sieve Attacks
München (DE)

CRYPTO 2023
22 August 2023
Title: Does the Dual-Sieve Attack on LWE even Work?
Santa Barbara, CA (USA)

Alumni day Leidsche Flesch
2 June 2023
Title: Recent developments in PQC: lattices as a promising solution
Leiden (NL)

ASIACRYPT 2022
8 December 2022
Title: HAWK: Module-LIP makes lattice signatures fast, compact and simple
Taipei (TW)

PQCifris Workshop
7 October 2022
Title: HAWK: Module-LIP makes lattice signatures fast, compact and simple
Trento (IT)