Wessel van Woerden

Bordeaux – France
+316 10 46 64 81 • wesselvanwoerden@gmail.com
Born in Koudekerk aan den Rijn, Netherlands, on Mar. 8, 1995. Dutch nationality.

Education

Institut de Mathématiques de Bordeaux **Bordeaux**
Postdoc *2022-now*

Centrum Wiskunde & Informatica (CWI) **Amsterdam**
PhD *2018–2022*
PhD Thesis: Lattice Cryptography, from Cryptanalysis to New Foundations, Supervised by Léo Ducas.

Centrum Wiskunde & Informatica (CWI) **Amsterdam**
Internship *2017–2018*
Master Thesis: Perfect Quadratic Forms. Supervised by Léo Ducas.

Leiden University **Leiden**
Master Mathematics, with highest honor *2016–2018*
Algebra, Geometry and Number Theory

Leiden University **Leiden**
Double bachelor Mathematics and Computer Science, with highest honor *2013–2016*
Thesis: The closest vector problem in cyclotomic lattices. Supervised by Léo Ducas.

Leiden University **Leiden**
Pre-University College *2011–2013*
Final project: The study of water-splitting catalysis as a route to renewable fuel. Supervised by Robin Purchase.

Groene Hart Lyceum **Alphen aan den Rijn**
VWO Gymnasium *2007–2013*

Scientific Publications

PhD Thesis: Lattice Cryptography, from Cryptanalysis to New Foundations.
Wessel van Woerden
Leiden University, 2023.

Hawk: Module LIP makes lattice signatures fast, compact and simple.
Leo Ducas, Eamonn W Postlethwaite, Ludo N Pulles, Wessel van Woerden
Asiacrypt 2023.

On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography.
Leo Ducas, Wessel van Woerden
Eurocrypt 2022.

An Algorithmic Reduction Theory for Binary Codes: LLL and more.
Thomas Debris-Alazard, Leo Ducas, Wessel van Woerden
IEEE Transactions on Information Theory, 2022.

NTRU Fatigue: How Stretched is Overstretched?
Leo Ducas, Wessel van Woerden
Asiacrypt 2021.

Advanced Lattice Sieving on GPUs, with Tensor Cores.
Leo Ducas, Marc Stevens, Wessel van Woerden
Eurocrypt 2021.

A Canonical Form for Positive Definite Matrices.
Mathieu Dutour Sikirić, Anna Haensch, John Voight and Wessel van Woerden
ANTS 2020, Open Book Series 4.1, 2020.

The Randomized Slicer for CVPP: Sharper, Faster, Smaller, Batchier.
Leo Ducas, Thijs Laarhoven and Wessel van Woerden
PKC 2020. Lecture Notes in Computer Science, vol 12111.

An upper bound on the number of perfect quadratic forms.
Wessel van Woerden
Advances in Mathematics, Volume 365, 2020.

The closest vector problem in tensored root lattices of type A and in their duals
Léo Ducas, Wessel van Woerden
Design, Codes and Cryptography, Volume 86, Issue 1, 2018.

Talks given

On LIP, Cryptography and the Signature Scheme HAWK.
RISC Seminar on Lattice-based Cryptography, CWI, Amsterdam. *2023*

An Algorithmic Reduction Theory for Binary Codes: LLL and More.
LFANT Seminar, Institut de Mathḿatiques de Bordeaux. *2023*

On LIP, Cryptography and the Signature Scheme HAWK.
Séminaire de Cryptographie, Inria, Rennes. *2023*

On LIP, Quadratic Forms, Remarkable Lattices, and Cryptography.
COSIC, Leuven. *2022*

On LIP, Quadratic Forms, Remarkable Lattices, and Cryptography.
Eurocrypt 2022, Trondheim. *2022*

On LIP, Quadratic Forms, Remarkable Lattices, and Cryptography.
IMB, Bordeaux. *2022*

An Algorithmic Reduction Theory for Binary Codes: LLL and More.
Post-Quantum Cryptanalysis workshop, Birmingham. *2022*

On LIP, Quadratic Forms, Remarkable Lattices, and Cryptography.
Post-Quantum Cryptanalysis workshop, Birmingham. *2022*

NTRU Fatigue: How Stretched is Overstretched?
Asiacrypt 2021, online. *2021*

On LIP, Quadratic Forms, Remarkable Lattices, and Cryptography.
DIAMANT Symposium, Utrecht. *2021*

Advanced Lattice Sieving on GPUs, with Tensor Cores.
Eurocrypt 2021, Zagreb. *2021*

An Algorithmic Reduction Theory for Binary Codes: LLL and More.
SIAM Conference on Applied Algebraic Geometry, AG 2021, online. *2021*

A Canonical Form for Positive Definite Matrices.
ANTS 2020, online. *2020*

The randomized slicer for CVPP: sharper, faster, smaller, batchier.
PKC 2020, online. *2020*

Lattice packings: an upper bound on the number of perfect lattices.
Simons Institute, Berkeley. *2020*

A tight analysis of the Iterative Slicer to solve the Closest Vector Problem.
Invited by Prof. Dr. Damien Stehlé at ENS Lyon. *2019*

Challenges in Enumerating Perfect Quadratic Forms.
Invited by Prof. Dr. Achill Schürmann at Universität Rostock. *2018*

Experience

Vocational

Institut de Mathématiques de Bordeaux **Bordeaux**
Postdoc *2022–now*

CWI **Amsterdam**
PhD Student *2018–2022*

Job Motion **Leiden**
Student Assistant Leiden University *2017–2018*
Course: Besliskunde A, Besliskunde B, Quantum Algorithms, Quantum Information Theory

Skills

Main Research Interests: Lattices, Linear Codes, Cryptography, Cryptanalysis, and (High Performance) Scientific Computing.

Programming: C/C++, CUDA, SageMath, Python, JavaScript, PHP, SQL, LaTeX, git

Languages: Dutch (native), English (fluent)

Interests

Sport: Tennis and Cycling

Competitive Programming: Participated in several coding competitions (teams of 3)
Detailed achievements:
- Catalyst Coding Competition Global - Hyperloop Metro - 2017
  - First place of over 600 teams globally.
- BAPC Preliminaries Leiden University
  - 2015: 3rd. 2016: 1st. 2017: 1st.
- BAPC (Benelux Algorithm Programming Contest)
  - 2015: 7th. 2016: 7th. 2017: 7th.
- NWERC (Northwestern Europe Regional Contest)
  - 2015: 65th. 2016: 24th. 2017: 19th.
- Ultrahack 2017 Sprint I
  - First prize for best student team.

Competitive Mathematics:
- Contests on several universities
- International Mathematics Competition for University Students 2017
  - Silver medal.