Joël **Felderhoff**

Postdoctoral Researcher in Cryptology

Lyon, France

☎ (+33) 681 23 15 63 | ✉ joel.felderhoff@ens-lyon.fr | 🏠 perso.jfelderhoff.fr | jetSett

Published scientific work

Hardness of Structured Lattice Problems for Post-Quantum Cryptography, Felderhoff *PhD thesis*

Ideal-SVP is Hard for Small-Norm Uniform Prime Ideals, Felderhoff, Stehlé, Pellet-Mary, Wesolowski *TCC 2023*

On Module-unique-SVP and NTRU, Felderhoff, Stehlé, Pellet-Mary *Asiacrypt 2022*

Talks and unpublished work

Ideal-SVP is Hard for Small-Norm Uniform Prime Ideals, Journés C2 10/23, CANARI seminar, Cryptography seminar of Université de Rennes, Number Theory seminar of the UMPA *Talk*

Module-unique-SVP and NTRU, Journées C2 04/22, CANARI seminar, GRACE Team working-group 05/2022 *Talk*

Politics, Cryptography and New Regulation, Journées C2 04/22 *Round table*

Impossibility results for Module LLL based on Euclidean Division, 2020 *Internship report*

Hard Homogenous Spaces and Commutative Supersingular Isogeny based Diffie–Hellman, 2019 *Internship report*

Homological product code and weight of random tensors, 2018 *Internship report*

Walking along the infrastructures of real quadratic and pure cubic Fields, 2017 *Internship report*

Technical Skills

Languages mastered, C, C++, Python/Sage, Rust

Languages known, OCaml, Java, PHP, HTML, CSS, Magma, Latex, Coq

Operating System and others, Linux, Windows, Docker, Git, MySQL, SQLite, ElasticSearch

Languages

English, C1 Cambridge English Advanced (CEA) - Spoken, Written

French, Native - Spoken, Written

Spanish, Niçois (Regional language), Notions

Education

École Normale Supérieure de Lyon *Lyon, France*

PhD degree in Computer Science *2021-2024*

- Hardness of Structured Lattice Problems for Post-Quantum Cryptography

Leiden University *Leiden, The Netherlands*

Lectures taken during internship *2021*

- Topics in Algebraic Number Theory, Quantum Computing

École Normale Supérieure de Lyon *Lyon, France*

Fundamental Computer Science Master of Science Year 2 *2018 - 2019*

- Computational Geometry, Hard lattice problems, Lower bound methods, Cryptanalysis, Topological combinatorics.
- Local Fields and Galois Cohomology classes followed in Mathematics department.

ENS de Lyon *Lyon, France*

Fundamental Computer Science Master of Science Year 1 *2017 - 2018*

- Major part of CS department's lectures.
- Advanced Algebra, Introduction to Number Theory and Algebraic Geometry classes followed in Mathematics department.

ENS de Lyon
Lyon, France

FUNDAMENTAL COMPUTER SCIENCE LICENSE ”MENTION TRÈS BIEN” (HIGHEST HONORS) *2016 - 2017*

- Major part of CS department's lectures, Introduction to Quantum Computing. Algebra I & II and Probability and Integration I & II courses validated in Mathematics department.

Lycée Thierry Maulnier and Lycée Massena
Nice, France

SCIENTIFIC BACALAURÉAT AND PREPARATORY CLASSES TO ”GRANDES ÉCOLES” MATHEMATICS PHYSICS * *2011 - 2016*

Professional and Miscellaneous Experience

INRIA Lyon, LIP - AriC team
Lyon , France

PHD: RELATIVE DIFFICULTIES OF STRUCTURED LATTICES IN THE CONTEXT OF POST-QUANTUM CRYPTOGRAPHY *Sept 2021 - Nov 2024*

Under the supervision of Damien Stehlé, Guillaume Hanrot and Bruno Salvy

ENS de Lyon, Université Claude Bernard Lyon 1
Lyon, France

TEACHING ASSISTANT *2021-2024*

Quantum CS (M1), Competitive Programming (L3), Networks (L3), Cryptography (M1), Software Engineering (M1), OS (L2)

CWI - Crypto Group
Amsterdam, The Netherlands

RESEARCH INTERNSHIP: A CHSP ORACLE FOR THE ARAKELOV CLASS GROUP *Feb - Jul 2021*

Under the supervision of Léo Ducas

LIP - AriC team
Lyon , France

RESEARCH INTERNSHIP: IMPOSSIBILITY RESULTS FOR MODULE LLL BASED ON EUCLIDEAN DIVISION *Sept 2020 - Feb 2021*

Under the supervision of Damien Stehlé

Esker France / Freelance
Lyon , France

BACKEND DEVELOPPER *Oct 2019 - August 2020*

Backend Programming in C++ and Python for web applications. Scripting in Python and Javascript.

LIX - GRACE team
Palaiseau , France

RESEARCH INTERNSHIP: HARD HOMOGENOUS SPACES AND ISOGENY BASED DIFFIE–HELLMAN *Feb - July 2019*

Under the supervision of Benjamin Smith

Lycée du Parc
Lyon, France

MATHEMATICS ORAL QUESTIONING IN PREPARATORY CLASSES TO ”GRANDES ÉCOLES” *Sept 2017 - Jan 2019*

For the MPSI students of Mr. Demange (832) and Mr. Kapoudjian (833)

University of Copenhagen - QMATH team
Copenhagen , Denmark

RESEARCH INTERNSHIP: HOMOLOGICAL PRODUCT CODE AND WEIGHT OF RANDOM TENSORS *Mai - July 2018*

Under the supervision of Péter Vrana

INRIA Nancy Grand Est- CARAMBA Team
Nancy , France

RESEARCH INTERNSHIP: WALKING ALONG THE INFRASTRUCTURES OF REAL QUADRATIC AND PURE CUBIC FIELDS *June - July 2017*

Under the supervision of Pierre-Jean Spaenlehauer

Extracurricular Activities

French Red Cross
France

CHIEF OF FIRST RESPONDERS TEAM (CHEF D'INTERVENTION). CERTIFIED FIRST RESPONDER. SOCIAL VOLUNTEER *2022-Today*

Training in social work and medical emergency response, management of a team of first responders.

Maths En Jeans
Lyon, France

SCIENTIFIC TUTOR *2022-2025*

Creation and realization of a 1-year research project in Mathematics with middle-scholers.

Girls Can Code

ORGANIZER AND TUTOR *2017 - 2022*

Summer camp for girls bellow 18, to promote the programming to girls. (`https://gcc.prologin.org`).

Recruitement of tutors, organization of the event beforehand, on-site management and tutoring.

Competitive Programming

SWERC 2017-2018, TEAM ENPLS (ENS DE LYON)

Camp Monitor

France

BAFA (French brevet of aptitude for Camp monitoring) obtained in Aug 2016 — *June 2016 - Today*

Prologin

Member — *2017- 2022*

Organization of Prologin contest (competitive programming), problem-writting. `https://prologin.org`

ConférENS (ENS de Lyon)

President — *2017- 2018*

Organization of conferences for scientific vulgarization and various knowledge sharing.