Johanna Loyer

Inria Saclay
johanna.loyer@gmail.com
+33 6 95 16 50 22

Postdoctoral researcher in Cryptology

Research interests

My research focuses on the cryptanalysis of security systems based on **lattice** and **code** problems, in both classical and **quantum** settings. I am particularly interested in transferring techniques between these domains.

Parcours professionnel

febr. 2025 – sept. 2026	**Post-doctoral researcher**, *Inria Saclay*, GRACE team. Supervisor : Thomas Debris-Alazard
febr. 2024 – jan. 2025	**Post-doctoral researcher**, *CWI*, Amsterdam, Cryptology group. Supervisor : Léo Ducas
sept. 2020 – dec. 2023	**Ph.D.**, *Inria*, Paris, COSMIQ team. Thesis: "*Quantum Cryptanalysis of Lattices and Codes*" Advisors: André Chailloux and Nicolas Sendrier
sept. 2020 – jan. 2023	**Teaching assistant**, *Sorbonne University*, Paris. Quantum circuits and logic gates, Master 1 Quantum information, Master 1 Programming in Python, Bachelor 1

Education

2018 – 2020	**Master in Applied Mathematics**, *University of Limoges, France.*
mars – august 2020	**Master's thesis internship**, *Inria Paris* Supervisor: André Chailloux
2017 – 2018	**Engineering school 1st year**, *INSA Centre Val de Loire, Bourges.*
2015 – 2017	**Preparatory classes for engineering schools**, *Lycée Michelet, Vanves.*
2015	**Scientific Baccalauréat** (high school diploma)

Publications

Peer-Reviewed Conferences and Journals

CRYPTO 2025 **Wagner's Algorithm Provably Runs in Subexponential Time for SIS^∞**, with Léo Ducas and Lynn Engelberts.
https://eprint.iacr.org/2021/570.pdf

DCC 2024, CFAIL 2024 **Quantum sieving for code-based cryptanalysis and its limitations for ISD**, with Lynn Engelberts and Simona Etinski.
https://eprint.iacr.org/2024/1358.pdf

PQCrypto 2023 **Classical and quantum 3 and 4-sieves to solve SVP with low memory**, with André Chailloux.
https://eprint.iacr.org/2023/200.pdf

ASIACRYPT 2021 **Lattice sieving via quantum random walks**, with André Chailloux.
https://eprint.iacr.org/2021/570.pdf

Participation à l'effort de standardisation

NIST Post-Quantum Cryptography 2023 Round 1 **Wave digital signature scheme**, with Gustavo Banegas, Kévin Carrier, André Chailloux, Alain Couvreur, Thomas Debris-Alazard, Philippe Gaborit, Pierre Karpman, Ruben Niederhagen, Nicolas Sendrier, Benjamin Smith, Jean-Pierre Tillich.
https://wave-sign.org/wave_documentation.pdf

Preprints

Lattice Reduction via Dense Sublattices: A Cryptanalytic No-Go
with Léo Ducas
Quantum security analysis of Wave.

Outreach and Science Communication

2023 Organized an outreach event to present my Ph.D. work and raise awareness about cybersecurity and privacy issues

2021 Participated in the RJMI meetings to promote STEM careers among high school girls

2020 Talks in middle schools: "*Introduction to cryptology: RSA*"

2018 – 2019 Talks in high schools: "*What are mathematices are useful for in daily life?*" in the context of a new high school reform that excluded mathematics from mandatory curriculum

2018 Workshops in elemantary schools to introduce robotics and programming, in partnership with the Graduate School of Teaching and Education (ESPE) of Bourges