Johanna Loyer

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

Chercheuse post-doctorante en cryptologie

Domaine de recherche

Mes centres d'intérêts concernent la **cryptanalyse** des systèmes de sécurité basés sur des problèmes de **réseaux** et de **codes**. Je m'intéresse aussi bien au modèle classique qu'au **quantique**. Je m'intéresse notamment au transfert des techniques entre ces différents domaines.

Parcours professionnel

février 2025 – sept. 2026	**Post-doctorat**, *Inria Saclay*, équipe-projet GRACE. Encadrant : Thomas Debris-Alazard
février. 2024 – janv. 2025	**Post-doctorat**, *CWI*, Amsterdam, Cryptology group. Encadrant : Léo Ducas
sept. 2020 – déc. 2023	**Doctorat**, *Inria*, Paris, équipe COSMIQ. Titre: "*Cryptanalyse quantique des réseaux et des codes*" Direction : André Chailloux et Nicolas Sendrier
sept. 2020 – janv. 2023	**Chargée de travaux dirigés**, *Université de Sorbonne*, Paris. Quantum circuits and logic gates, Master 1 Quantum information, Master 1 Programming in Python, License 1

Formation

mars 2020 – août 2020	**Stage de recherche de fin d'études**, *Inria Paris* Encadrant : André Chailloux.
sept. 2018 – août 2020	**Master en Mathématiques appliquées**, *Université de Limoges.*
sept. 2017 – août 2018	**Première année en école d'ingénieurs en informatique**, *INSA Centre Val de Loire, Bourges.*
sept. 2015 – août 2017	**Classe préparatoire aux grandes écoles PCSI-PSI**, *Lycée Michelet, Vanves.*
2015	**Baccalauréat scientifique**

Publications

Revues à comité de lecture

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

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

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

ASIACRYPT 2021 **Lattice sieving via quantum random walks**, avec 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**, avec 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
avec Léo Ducas
Quantum security analysis of Wave.

Vulgarisation scientifique

2023 Organisation d'un évènement de vulgarisation de ma thèse et sensibilisation aux enjeux de sécurité informatique et de vie privée.

2021 Participation aux rencontres RJMI pour promouvoir les études scientifiques auprès des lycéennes.

2020 Interventions au collège : "Introduction à la cryptologie : RSA"

2018 – 2019 Interventions au lycée : "Les maths, à quoi ça sert pour de vrai ?"

2018 Ateliers de découverte de la robotique et de l'informatique (école primaire), en partenariat avec l'ESPE de Bourges.