Dr. Julien Devevey

Expert en Cryptographie

6 Janvier 1997

31, Quai de Grenelle, 75015 Paris

01 71 75 25 93

https://perso.ens-lyon.fr/julien.devevey

julien.devevey@ens-lyon.fr

À propos de moi

Expert en Cryptographie au sein de l'ANSSI.
Je suis membre de HAETAE, une signature post-quantique actuellement candidate au 4ème round du NIST et au Kpqc.
Mes intérêts de recherche sont centrés autour de la cryptographie sur les réseaux Euclidiens et les signatures numériques.

Langues

Français (Natif)

Anglais (C1 certifié CAE)

Allemand (B2)

Scolarité

2016-2020 — Diplôme de l'ENS de Lyon – Normalien élève — ENS de Lyon, Lyon
Majeure Informatique et mineure Mathématiques.

2019-2020 — Master d'Informatique — ENS de Lyon, Lyon
Master d'Informatique Fondamentale.

2019 — Agrégation de mathématiques — France
Reçu 66ème, option D (informatique).

2018-2019 — Master de Mathématiques — ENS de Lyon, Lyon
Master FEADéP (Formation à l'Enseignement, Agrégation, Développement Professionnel) en Mathématiques.

Expériences Scientifiques

2020-2023 — Doctorat — ENS de Lyon, Lyon
Signatures Fondées sur les Réseaux Euclidiens dans le paradigme de Fiat-Shamir. Sous la direction de Damien Stehlé.
Soutenance prévue le 18 septembre 2023.

Depuis 2023 — Membre de HAETAE — ENS de Lyon, Ruhr University Bochum et Cryptolab
Soumission d'une signature numérique pour la Korean post-quantum competition `https://www.kpqc.or.kr/competition.html`.
Soumission aussi au 4ème round de la post-quantum competition du NIST `https://csrc.nist.gov/projects/pqc-dig-sig/`.
Page web du projet : `https://kpqc.cryptolab.co.kr/haetae`

Depuis 2020 — Sous-relecteur — IACR
Pour Eurocrypt'22, Asiacrypt'22, PKC'23, Crypto'23, Asiacrypt'23.

2020 — Stage de recherche — ENS de Lyon, Lyon
Avec Benoît Libert. Sujet : Construction de cryptosystèmes à seuil fondés sur les réseaux.

2018 — Stage de recherche — Faculty of IT, Monash University, Melbourne
Avec Ron Steinfeld. Sujet : On the Integer Variant of MP-LWE, IMP-LWE.

Publications

2023 — A Detailed Analysis of Fiat-Shamir with Aborts — Crypto'23
Avec Pouria Fallahpour, Alain Passelègue et Damien Stehlé.
`https://eprint.iacr.org/2023/245.pdf`

2022 — On Rejection Sampling in Lyubashevsky's Signature Scheme — Asiacrypt'22
Avec Omar Fawzi, Alain Passelègue et Damien Stehlé.
`https://eprint.iacr.org/2022/1249.pdf`

2022 — Rational Modular Encoding in the DCR Setting : Non-Interactive Range Proofs and Paillier-Based Naor-Yung in the Standard Model — PKC'22
Avec Benoît Libert et Thomas Peters.
`https://doi.org/10.1007/978-3-030-97121-2_22`

2021 — Non-Interactive CCA2-Secure Threshold Cryptosystems : Achieving Adaptive Security in the Standard Model Without Pairings — PKC'21
Avec Benoît Libert, Khoa Nguyen, Thomas Peters et Moti Yung.
`https://eprint.iacr.org/2021/630.pdf`

2021 — On the Integer Polynomial Learning with Errors Problem — PKC'21
Avec Amin Sakzad, Damien Stehlé, Ron Steinfeld.
`https://eprint.iacr.org/2021/277.pdf`

Responsabilités

Depuis 2023 — Point de contact pour HAETAE — ENS de Lyon, Ruhr University Bochum et Cryptolab
Point de contact principal auprès du NIST.

2022-2023 — Conseil de Laboratoire — LIP, Lyon
Représentant élu des doctorants au conseil de laboratoire du LIP, le laboratoire d'informatique de l'ENS de Lyon.

2023 — Conférence Eurocrypt 2023 — Lyon
Membre de l'équipe qui a veillé au bon déroulement de la plus grande conférence de l'IACR à ce jour (plus de 700 participants).