Last updated in May 2025

Arthur HERLÉDAN LE MERDY

PhD Student in isogeny-based cryptography

Lyon, France   arthur.herledan_le_merdy@ens-lyon.fr   a-hlm.github.io

Education

PhD	in Mathematics and Computer Science in the UMPA laboratory at the ENS de Lyon, under the supervision of Benjamin Wesolowski and Guillaume Hanrot	2022-Today
MSc	in Mathematics and Applications, Mathematics of Information, Cryptography, with a focus on Fundamental Research, at the University of Rennes 1	2020-2022
Exchange	program in Mathematics at the University of Göttingen, Germany (Interrupted due to COVID)	2019-2020
BSc	in Mathematics and Applications at the University of Rennes 1	2016-2019
BAC S	French High School Diploma in Science	2016
BAC STD2A	French High School Diploma in Design and Applied Arts	2015

Publications

PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies 2025
accepted in Crypto 2025

with Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren and Benjamin Wesolowski
Cryptology ePrint Archive

The supersingular endomorphism ring problem given one endomorphism 2025
published in Communications in Cryptology, Volume 2, Issue 1

with Benjamin Wesolowski Cryptology ePrint Archive

Preprint

Unconditional foundations for supersingular isogeny-based cryptography 2025

with Benjamin Wesolowski Cryptology ePrint Archive

Talks

Unconditional foundations for supersingular isogeny-based cryptography Apr 2025
Journées Codage et Cryptographie, Pornichet, France

Unconditional foundations for supersingular isogeny-based cryptography Jan 2025
CASCADE seminar, Paris, France

Unconditional foundations for supersingular isogeny-based cryptography Nov 2024
CANARI seminar, Bordeaux, France

Unconditional relations between hard problems in isogeny-based cryptography Sep 2024
Leuven Isogeny Days 5, KU Leuven, Belgium

The endomorphism ring problem given one endomorphism Apr 2024
Isogeny Club, online

Post-quantum key exchange using class group actions on oriented supersingular elliptic curves Nov 2023
Séminaire d'arithmétique de Lyon, ENS de Lyon, France

The endomorphism ring problem given an endomorphism Oct 2023
Journées Codage et Cryptographie, Najac, France

Teaching

LIFAPI - Introduction to Imperative Programming 2024-2025
Bachelor's in Mathematics and Computer Science, University of Lyon 1 (1st Year)

Cryptography and security 2023-2024
Master's in Computer Science, ENS de Lyon (1st Year)

Computer Algebra 2022-2023
Master's in Computer Science, ENS de Lyon (1st Year)

Technical Skills

Programming Languages: C, Python, Java, Racket

Computer algebra system: SageMath, Maple, Magma, PARI/GP

Languages

French (Native)

English (Fluent)

German (Intermediate)

Russian, **Esperanto** (Beginner)