

Arthur HERLÉDAN LE MERDY

📍 Brussels, Belgium 📩 arthur.herledanlemerdy@esat.kuleuven.be 🔗 a-hlm.github.io

Current position

Post-doc	on isogeny-based cryptography at COSIC, KU Leuven working in the group of Frederik Vercauteren	2025-today
-----------------	---	------------

Education

PhD	<i>On the foundations of supersingular isogeny-based cryptography,</i> initially at the LIP laboratory at the ENS de Lyon, then at the UMPA laboratory at the ENS de Lyon, under the supervision of Benjamin Wesolowski and Guillaume Hanrot	2022-2025
MSc	in Mathematics and Applications, Mathematics of Information, Cryptography, with a focus on Fundamental Research, at the University of Rennes 1	2020-2022
Erasmus	(Exchange Program) in Mathematics at the University of Göttingen, Germany <i>Interrupted due to COVID</i>	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

The supersingular endomorphism ring problem given one endomorphism published in CiC, Volume 2, Issue 1 with Benjamin Wesolowski Cryptology ePrint Archive ↗	2025
Unconditional foundations for supersingular isogeny-based cryptography published in TCC 2025 with Benjamin Wesolowski Cryptology ePrint Archive ↗	2025
PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies published 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 ↗	2025

Talks

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

Unconditional foundations for supersingular isogeny-based cryptography CASCADE seminar, Paris, France	Jan 2025
Unconditional foundations for supersingular isogeny-based cryptography CANARI seminar, Bordeaux, France	Nov 2024
Unconditional relations between hard problems in isogeny-based cryptography Leuven Isogeny Days 5, KU Leuven, Belgium	Sep 2024
The endomorphism ring problem given one endomorphism Isogeny Club, online	Apr 2024
Post-quantum key exchange using class group actions on oriented supersingular elliptic curves Séminaire d'arithmétique de Lyon, ENS de Lyon, France	Nov 2023
The endomorphism ring problem given an endomorphism Journées Codage et Cryptographie, Najac, France	Oct 2023

Teaching

LIFAPI - Introduction to Imperative Programming Bachelor's in Mathematics and Computer Science, University of Lyon 1 (1st Year)	2024-2025
Cryptography and security Master's in Computer Science, ENS de Lyon (1st Year)	2023-2024
Computer Algebra Master's in Computer Science, ENS de Lyon (1st Year)	2022-2023

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)