

# 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    2025-today  
working in the group of [Frederik Vercauteren](#)

## Education

**PhD**    *On the foundations of supersingular isogeny-based cryptography,*    2022-2025  
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](#)

**MSc**    in Mathematics and Applications, Mathematics of Information, Cryptography,    2020-2022  
with a focus on Fundamental Research, at the University of Rennes 1

**Erasmus**    (Exchange Program) in Mathematics at the University of Göttingen, Germany    2019-2020  
*Interrupted due to COVID*

**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**    2025  
published in [CiC, Volume 2, Issue 1](#)  
*with Benjamin Wesolowski*  
[Cryptology ePrint Archive](#) 🔗

**Unconditional foundations for supersingular isogeny-based cryptography**    2025  
published in [TCC 2025](#)  
*with Benjamin Wesolowski*  
[Cryptology ePrint Archive](#) 🔗

**PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies**    2025  
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](#) 🔗

## Talks

**Unconditional foundations for supersingular isogeny-based cryptography**    Dec 2025  
TCC 2025, Aarhus, Denmark

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

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

## Teaching

---

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