

Mathias Marty

Address: Rue de l'Orée 5, 2054 Chézard, Switzerland

Date of birth: 10.15.1999

Phone: +41 78 784 84 78

Email: mathiasmarty99@gmail.com

Nationality: Swiss

Linkedin: www.linkedin.com/in/mathias-marty-ch



EDUCATION

2022 : 2024

Master of Science - Cyber Security • EPFL/ETHZ • Lausanne/Zürich (*GPA = 5.34/6*)

2021 : 2022

HES gateway • EPFL • Lausanne (*GPA = 5.12/6*)

2018 : 2021

Bachelor of Science - Computer Science • HES/SO Haute Ecole Arc • Neuchâtel (*GPA = 5.24/6*)

2015 : 2018

Professional Baccalaureate • CPLN • Neuchâtel

2015 : 2018

Federal Diploma of Vocational Education and Training in Computer Science • CPLN • Neuchâtel

PUBLICATIONS

- **Gamma Special Soundness for Linear Time IOPs**
Jonathan Bootle, Alessandro Chiesa & Mathias Marty
(under review) TCC 2025 – Theory of Cryptography Conference
- **Implicit Curves: From Discrete Extraction to Applied Formalism**
Mathias Marty, Antoine Lestrade, Artan Sadiku, Christophe Muller, Joep Neijt, Yann Voumard & Stéphane Gobron
ICGG 2022 - Proceedings of the 20th International Conference on Geometry and Graphics
- **Real-Time Renderings of Multidimensional Massive DataCubes on Jupyter Notebook**
Antoine Lestrade, Mathias Marty, Artan Sadiku, Christophe Muller, Joep Neijt, Yann Voumard & Stéphane Gobron
ICGG 2022 - Proceedings of the 20th International Conference on Geometry and Graphics
- **Earth Observation: Datacubes Multi-Visualization Toolbox**
Christophe Muller, Antoine Lestrade, Mathias Marty, Artan Sadik, Yann Voumard & Stéphane Gobron
The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences

RESEARCH PROJECTS

2025 – present:

Independent Research • with Prof. Eylon Yogev and Gal Arnon

Implementing a PoC in Rust and lower bounds for hash-based signatures

2024 – present:

Independent Research • with Prof. Alessandro Chiesa and Dr. Jonathan Bootle

Gamma Special Soundness for Linear Time IOPs

2024:

Master Project • EPFL

On State-Restoration Knowledge Soundness from Special Soundness • supervisor: Prof. Alessandro Chiesa • grade = 5.75 /6

2023:

Semester Project • EPFL

Code-based Cryptography in the Lee metric • supervisor: Prof. Serge Vaudenay • grade = 5.75/6

2022:

Formal Verification Course Project • EPFL

Prove some RSA security properties with the proof assistant EasyCrypt (not graded)

2021:

Bachelor Project • HES/SO Haute Ecole Arc

DataCube: Implicit Curves • supervisor: Prof. Stéphane Gobron • grade = 6/6

SKILLS

In addition to my theoretical skills, I acquired many practical skills by studying at a University of Applied Sciences and working with Prof. Eylon Yogev and at CSEM, including:

- **Programming:** Rust, Assembly, C, VHDL, C++, Scala & Stainless, Java, C#, JavaScript, WebGL/GLSL, SQL, Python/Sage, Kotlin
- **Software and tools:** Git, Linux, EasyCrypt, GDB, Latex, QEMU, RTOS, embedded device, Docker, American Fuzzy Lop
- **Soft skills:** Writing technical reports and papers, making presentations, teaching, ability to adapt to different learning levels and needs, communication

WORK EXPERIENCE

2025 – present:

Programmer • 50% work for Prof. Eylon Yogev •

Implementing cryptographic primitives and proofs of concepts

2023:

Summer internship • Swiss Center for Electronics and Microtechnology (CSEM) • Neuchâtel •

supervisor: Dr. Damian Vizár

Embedded fuzzing testbench of a RTOS with HALucinator (evaluation: Excellent)

2018 – present:

Private tutoring •

Tutored students across a wide academic range, from elementary to University level (I now have a [Superprof account](#))

RELATED COURSES

Courses taken and grades: Cryptography and Security (5), Advanced Cryptography (5.25), Number Theory in Cryptography (5.5), Foundations of Probabilistic Proofs (5), Computational Complexity (5.25), Computer Architecture (5), OS (5.5), Computer Networks (5.75), Algorithms (5), Advanced Algorithms (5.25), Formal Verification (5), Gödel and Recursivity (5.75), Advanced Encryption Schemes, Zero-Knowledge Proofs...

LANGUAGES

- French – Mother tongue
- English – Fluent (FCE in 2018 & TOEFL 102/120 in 2024)
- German – School knowledge

HOBBIES

- Piano playing
- Computer science
- Math