Simon Masson

PhD and engineer in cryptography

France
✉ *simon.masson@proton.me*
32 years

Professional experience

Feb. 2025 – Today **Cryptography engineer**, *ZKNOX, remote*
Research and development of post-quantum cryptography in the context of blockchain.

Feb. 2024 – Jul. 2024 **Intern in underwater signal processing**, *Puerto Madryn (AR) and Gandía (ES)*
Signal analysis for characterizing the underwater seabed.

Apr. 2021 – Feb. 2023 **Cryptography engineer**, *Heliax, remote*
Implementation of zero-knowledge proofs in Python and Rust for Anoma.
Optimization of finite field arithmetic, elliptic curve group law, and proof circuits.

Jan. 2018 – Jan. 2021 **PhD student and engineer**, *Thales, Gennevilliers (FR)*
Generation of pairing-friendly elliptic curves resisting Number Field Sieve variants.
Construction of a verifiable delay function from isogeny-based and pairing-based cryptography.
Cryptanalysis of post-quantum constructions based on supersingular isogenies.

2019 **Computer Science teacher**, *Paris Diderot Univeristy*
Introduction to Java (48 hours) and Python (24 hours).

2017 **Intern in elliptic curve cryptography**, *Thales, Gennevilliers (FR)*
Development of a tool for searching dimension 4 GLV elliptic curves.
Implementation of the fast scalar multiplication for a curve defined modulo $2^{255} - 19$.

Education

2018–2021 **PhD in cryptography**, Lorraine University, Nancy (FR)
Algorithmic of curves in the context of bilinear and post-quantum cryptography.
Advisors: Emmanuel Thomé and Aurore Guillevic.

2022–2024 **WAVES Master**, ***W**aves, **A**coustics, **V**ibrations, **E**ngineering and **S**ound*
Coimbra (Portugal), Valencia (Spain) and Marseille (FR). Ranked 1st/12 (16.8/20).

2017 **Applied Algebra Master**, *Paris Saclay University*, Ranked 1st/12 (16.7/20).

2016 **Agrégation de Mathématiques**, *Rennes 1 University*, Ranked 92nd/306.
Competitive mathematics exam.

2014 **Bachelor of Mathematics**, *Rennes 1 University*

Programming languages

LaTeX	● ● ● Scientific paper, slides, posters
Python, Magma	● ● ● Proofs of concept for cryptography research
Matlab	● ● ○ Signal processing, simulation of non-linear equations
Rust, C	● ● ○ Optimized modular arithmetic and elliptic curve scalar multiplication
Git, Bash	● ● ○ Daily use for various projects
Java	● ○ ○ Basic knowledge, teaching experience

Languages

French (fluent), english (spoken, written), spanish (spoken, written).

Hobbies

Volley-ball, music, magic tricks.

Publications

2025 **Fast elliptic curve scalar multiplications in SN(T)ARK circuits**, *(Latincrypt 2025)*, with Liam Eagen, Youssef El Housni and Thomas Piellard

New techniques for optimized scalar multiplication circuits in zero-knowledge proofs.

2024 **Embedded curves and embedded families for SNARK-friendly curves**, *(in progress)*, with Aurore Guillevic

Extension and generalization of a method for searching curves using imaginary quadratic field results. Applications for recursive zero-knowledge proof constructions.

2024 **Bandersnatch: a fast elliptic curve built over the BLS12-381 scalar field**, *(Designs, Codes and Cryptography)*, with Antonio Sanso and Z. Zhang

Construction of an efficient and secure elliptic curve embedded above BLS12-381, using the Complex Multiplication method. Efficient implementation of the GLV acceleration using the degree 2 endomorphism.

2021 **Algorithmic of curves in the context of bilinear and post-quantum cryptography**, *PhD thesis*

2020 **Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation**, *(Designs, Codes and Cryptography)*, with Aurore Guillevic and Emmanuel Thomé.

Generation of efficient pairing-friendly elliptic curve resistant to NFS variants, for an embedding degree between 5 and 8.

2019 **Verifiable Delay Functions from Supersingular Isogenies and Pairings**, *(Asiacrypt 2019)*, with L. De Feo and Antonio Sanso.

Construction of verifiable delay functions based on pairings and computation of isogenies defined over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$.

2018 **Efficient four-dimensional GLV curve with high security**, with Olivier Bernard and Renaud Dubois.

Construction of an elliptic curve allowing dimension 4 GLV decomposition for a high security. The curve has been patented.