# Simon Rastikian

*Cryptography Research Engineer*

simon.rastikian.com
simon-rastikian
SimonRastikian

## Experience

2024–Present **Cryptography Research Engineer**, *Near One*, Zurich

- Implemented, deployed and benchmarked MPC protocols (threshold ECDSA/EdDSA, key derivation).
- Investigated and deployed post-quantum cryptographic primitives.
- Accelerated cryptographic primitives and signatures on the core protocol.
- Improved the MPC smart contract logic and voting mechanisms.
- Submitted a candidate scheme to the NIST call for multi-party threshold schemes.

2021–2024 **PhD in cryptography**, *IBM Research and ETH*, Zurich

- Researched cryptographic combiners, Schnorr, hash-based and threshold signatures.
- Brought post-quantum cryptography expertise to ETSI.
- Presented post-quantum migration strategies to IBM clients.
- Published **seven papers** and filed **one patent**.

Extra: Trained on CryptoHack and HackTheBox; ranked **Top 4%** of 2M+ users on TryHackMe.

2017–2021 **Intern**, *Academia, Startups and Industry*

- **5 months**: Implemented in Rust a one-round-trip KEMTLS at **Crypto Quantique**, London.
- **3 months**: Designed a signature combiner primitive at **IBM Research**, Zurich.
- **5 months**: Optimised a C/ARM Assembly implementation of NTRU Prime at **CryptoNext Security**, Paris.
- **9 months**: Analysed Selene and designed a novel e-voting scheme at **University of Luxembourg**, Belval.
- **2 months**: Implemented a power-analysis attack on Curve25519 (C and ARM Assembly) at **CNRS**, Lorient.

## Education

2018–2021 **Master's in cryptography**, *École Normale Supérieure*, Paris

- Implemented course projects in Python, C, HTML, CSS and JavaScript.
- Elected board representative of Master's students in computer science department.

2015–2018 **Bachelor's in computer science**, *École Normale Supérieure & Sorbonne Université*, Paris

- Built a strong foundation in mathematics and theoretical computer science.
- Implemented course projects in OCaml, C, Java, Python, and X86-64 Assembly.
- Elected board representative of Bachelor students in the Sorbonne Université mathematics department.

## Publications & Patents

Patent **Secure digital signature schemes.**, *B. Poettering and S. Rastikian*, IBM
Patent number: 12603786

Paper **Hyperion: Transparent End-to-End Verifiable Voting with Coercion Mitigation**, *A. Damodaran, S. Rastikian, P. B. Rønne and P. Y. A. Ryan*, ESORICS 2025

Paper **Digital Signatures with Outsourced Hashing**, *B. Poettering and S. Rastikian*, Asiacrypt 2024

Paper **Formalizing Hash-then-Sign Signatures**, *B. Poettering and S. Rastikian*, PKC 2024

Paper **A Study of KEM Generalizations**, *B. Poettering and S. Rastikian*, SSR 2023

Paper **Sequential Digital Signatures for Cryptographic Software-Update Authentication**, *B. Poettering, S. Rastikian*, ESORICS 2022

Paper **KEMTLS with Delayed Forward Identity Protection in (Almost) a Single Round Trip**, *F. Günther, S. Rastikian, P. Towa and T. Wiggers*, ACNS 2022

Paper **Hyperion: An Enhanced Version of the Selene End-to-End Verifiable Voting Scheme**, *P. Y. A. Ryan, P. B. Rønne and S. Rastikian*, E-Vote-ID 2021

## Selected Projects

2021–2024 Streamlet: Textbook Streamlined Blockchains *Python*

Defend the Flag (DtF) – Find and patch vulnerabilities in a virtual machine. *Python & Bash*

ACME protocol implementation (ACME client, web server, DNS server). *Python*

2018–2021 Web Scraper website for tree plantation projects. *Python & CSS & JS*

Peer-to-Peer chat protocol (Time-Length-Value encoding). *C*

2017–2018 Mini-Rust compiler. *OCaml & X86-64 Assembly*

8 bits RISC microprocessor simulator. *OCaml, X86-64 Assembly & Mini-Jazz*

## Selected Talks

2024 **Formalizing Hash-then-Sign Signatures**, *PKC*, Australia

2023 **On the (in)security of ROS**, *IBM Research*, Switzerland

2022 **Cryptographic Software-Update Authentication**, *ESORICS*, Denmark

**KEM Combiners**, *SKECH Workshop*, Italy

2021 **New Signature Primitives**, *ENS*, France

2020 **Individual Verifiable Bulletin Board**, *PhD Colloquium on Voting*, Luxembourg

## Skills

Rust, C, Python, LaTeX *Advanced*

OCaml, Java, HTML, CSS, JavaScript, *Intermediate*

X86-64 Assembly, ARM Assembly, Shell, PostgreSQL

TensorFlow, ProVerif, F* *Beginner*

## Languages

Fluent English, French, Arabic *Read, spoken and written*

B1 German *Read, spoken and written*