

Antoine Moran

PhD Candidate — Hardware Security & Post-Quantum Cryptography

📍 Grenoble, France ✉ contact@mail.amoran.fr

🌐 linkedin.com/in/antoine-moran

PROFESSIONAL EXPERIENCE

Doctoral Researcher — Hardware Security

Nov. 2023 – present

CEA-Leti

Grenoble, FR

- Side-channel attacks on ML-KEM, HQC and SHA-2 — published at *Designs, Codes and Cryptography* (2025) and *CHES* (2026).
- Side-channel leakage characterization of post-quantum cryptographic schemes (KEMs).
- Design and implementation of embedded countermeasures.
- Contributor to Secbench, CEA-Leti's open-source framework for hardware security characterization (side-channel analysis & fault injection). Implementation of a Belief Propagation framework in Rust.

Instructor — C Programming

2025 – 2026

Grenoble INP-Ensimag

Grenoble, FR

Led the tutorials and course projects in C for two engineering cohorts, 30 h per year.

Research Internship — Automated machine-log factoring

May – Sep. 2022

Laboratoire d'Informatique de Grenoble (LIG)

Grenoble, FR

Applied NLP techniques and spectral clustering to machine-log factoring.

Specialization Project — AES key enumeration on GPU

Feb. – May 2022

CEA-Leti / Ensimag

Grenoble, FR

Developed a Rust library for GPU-accelerated AES key enumeration on CUDA hardware.

IT Support

Mar. 2020 – Feb. 2022

Grenoble INP-Ensimag

Grenoble, FR

EDUCATION

PhD, Hardware Security

Nov. 2023 – present

CEA-Leti

Grenoble, FR

M.Sc. in Cybersecurity (Advanced Cryptography)

2022 – 2023

Université Grenoble Alpes / Grenoble INP-Ensimag

Grenoble, FR

Engineering Degree, Computer Science & Applied Mathematics

2020 – 2023

Grenoble INP-Ensimag, UGA

Grenoble, FR

Preparatory Classes MPSI / MP*

2018 – 2020

Lycée Michel de Montaigne

Bordeaux, FR

TECHNICAL SKILLS

Languages

Rust (performance-critical code), C (embedded), Python

Domains

Side-channel analysis, post-quantum cryptography (KEM), applied cryptography, embedded systems

Tools

NumPy, CUDA, Git, Nix/NixOS, SciPy, scikit-learn, Docker