Paul Vié — Engineering Student at Télécom Paris

paul.vie@telecom-paris.fr • paul-vie • plvie

Aspiring Researcher in Post-Quantum Cryptanalysis & Lattice Reduction.

Research Experience

CWI (Centrum Wiskunde & Informatica) **Amsterdam**
Research Intern (Cryptology Group) *June–August 2025*
Supervised by **Ludo Pulles & Léo Ducas** on Cryptanalysis of Lattice-based cryptography (Sparse LWE).
Contributions:

- Practical analysis of primal hybrid attacks leading to the publication *Cool + Cruel = Dual* at **Eurocrypt 2026**.
- Implementation of `cuBLASter`, a GPU-accelerated lattice reduction tool (LLL, BKZ) improving upon state-of-the-art open-source implementations.
- Development of a GPU Batched Babai Nearest Plane algorithm, which, in combination with cuBLASter, outperforms state-of-the-art attacks on Sparse LWE benchmark instances.

Publications & Preprints

To appear: A. Karenin, E. Kirshanova, J. Nowakowski, E. W. Postlethwaite, L. N. Pulles, F. Virdia, **P. Vié**.
Cool + Cruel = Dual, and New Benchmarks for Sparse LWE.
Accepted at **Eurocrypt 2026** (45th Annual International Conference on the Theory and Applications of Cryptographic Techniques). [IACR ePrint 2025/1002].

2025: L. N. Pulles, **P. Vié**. *Accelerating the Primal Hybrid Attack against Sparse LWE using GPUs*. [IACR ePrint 2025/1990] - Talk given at CWI Cryptology Group. [View Slides].

Education

Télécom Paris **Palaiseau**
Engineering Student *2024–Present*
Track: ACCQ (Applied Algebra: Cryptography, Coding Theory, Quantum Information).
Research Project: *Lattice-Based Receiver Selective Opening (RSO) Security* – Supervised by **Matthieu Rambaud**.

- **Key Coursework:** Computer Algebra, Intro to Algebraic Curves, Mathematical Cryptography, Algorithms for Arithmetic, Coding Theory, Quantum Computing (Full catalogue here).
- **CS Electives:** Advanced Algorithms, Programming Pearls (Data Structures), Concurrent Programming, Rust.
- **First year:** Compiler Construction, Logic and Foundations of CS (Computability, Coq/Rocq) (Full catalogue here).

Université Paris Cité **Paris**
Double Bachelor's Degree in Mathematics and Computer Science *2021–2024*
Selected Projects: Bachelor's Thesis on the Mertens function [Link], Functional Programming (OCaml), Custom Cryptography Implementation, Operating Systems (Shell).

Technical Skills

Languages: C, C++, CUDA, Python, SageMath, OCaml, x86-64 Assembly, Rust, Bash

Cryptology: **CryptoHack**: Global Rank **#105** – France **#10** (Top 0.01%, Link).
Algorithmic Number Theory & Cryptanalysis (***SageMath***): Elliptic Curves ($\mathbb{C}/\Lambda \cong E$ via $\wp$, Weil Pairing, Isogenies, Genus Theory), Primality Testing (*Prime and Prejudice* attack), Differential/Linear Cryptanalysis.

System Security: **Root-Me**: Global Rank **#343** (Top 0.1%, Link).
Automated Analysis & Low-level Exploitation: Constraint solving (**Z3** SMT), Symbolic Execution (**angr**), Reverse Engineering (ELF, x86-64), and Side-Channel Attacks (Timing/Power).

Awards

2024: **France Cybersecurity Challenge (FCSC) / ANSSI**: Qualified for the French Team selection (ECSC).