CV (Year 2024-2025)

Pierre PÉBEREAU **PhD Student at Sorbonne Université / Thales SIX**
Born 12/11/1999

pierre.pebereau[at]lip6.fr https://github.com/pi-r2
https://polsys.lip6.fr/~pebereau/

Education

December 2022-December 2025 : Sorbonne Université, LIP6, CNRS / Thales
PhD Student under the supervision of Simon Abelard and Mohab Safey el Din.
Cryptanalysis of multivariate post-quantum signature schemes with Gröbner basis algorithms, with practical (few seconds on a laptop) and theoretical results (exponential degradation of the security of NIST candidates).

2021-2022 : Université Paris-Diderot
Master Parisien de Recherche en Informatique (**M2 MPRI**), specialized in Combinatorics, Computer Algebra, Cryptography and Algorithmics.

2019-2022 : Télécom Paris, cursus Paris,
Options :

- MITRO : Mathematics, Theoretical Computer Science, Operational Research
- ACCQ : Algebra, Cryptography, Encryption, Quantum Information
- SD : Data Science

2020 : Stanford Coursera MOOC on Machine Learning by Andrew Ng (certificate link)

2017-2019 : Lycée **Janson-de-Sailly**
Classe préparatoire MPSI-MP*, specialized in Computer Science
Enrolled at Télécom Paris on the national exam “Concours Commun Mines-Ponts”

Professional Experience

Semester 2 24/25 : Supervision of master thesis: **Study of a signature scheme**: OV^+(M1)
Semester 2 24/25 : TA at Sorbonne University: **Foundations of Algorithmic Algebra** (M1)
Semester 1 24/25 : Lecture in Master CCA: **Intro. to multivariate cryptology** (M2)
Semester 1 24/25 : TA at Sorbonne University: **Intro. to Programming** (L1)
Semester 2 23/24 : TA at Sorbonne University: **Foundations of Algorithmic Algebra** (M1)
Semester 1 23/24 : TA at Sorbonne University: **Networks** (L3)
Semester 2 22/23 : TA at Sorbonne University: **Intro. to Cryptology** (L3)

04/2022-08/2022 : M2 Intern at **Thales SIX** cryptology lab (LCH) supervised by Eric Sageloli (Thales) and Pierrick Meaux (University of Luxembourg). **Identity-based signature schemes with tight security from lattices.** (Lead to this paper published at ACNS 2023)

06/2021-08/2021 : M1 Intern at **INRIA** project-team COATI supervised by David Coudert and Nicolas Nisse. **Exact computation of pathlength by branch and bound** (link in French)

2020-2022 : Khôlleur in mathematics at Lycée Janson-de-Sailly for MPSI students. This consist in giving oral interrogations for “classe préparatoire” students each week.

Associations

2019-2021 : Technical Manager for association **Aurore.**
Aurore is an association providing internet access, run benevolently by students of Université Paris-Saclay and surrounding engineering schools. I took part in deploying our network to a new residence in a contract for CROUS Versailles, and maintained the network.

2020-2022 : Administrator of **Télécode**, competitive programming club of Télécom Paris. We breathed life to a long deceased club which aims to prepare fellow students for a set of different programming contests such as ICPC. In 2021, we organized an operations research contest in partnership with Total.

2020 : Administrator of **Rezel** : Rezel is a student association of Télécom Paris which provides a range of online services, such as website hosting and Jitsi, for students.

2019-2020 : Forum Telecom Paris : Development of the website and related tools.

Projects

2019-2021 : Took part in several programming contests with fellow Telecom Paris students: Hashcode, Hackathon Renault hosted by KIRO, BattleDev, and many in-house contests.

2018-2019 : My TIPE in classe préparatoire was focused on ElGamal Encryption and the Discrete Logarithm Problem, over Finite Field and Elliptic Curves, with a comparison to the RSA scheme.

2020 : My end of year project in my first year at Télécom Paris was implementing **Weisfeiler-Lehman Graph Kernels** in the Python package scikit-network under the supervision of Thomas Bonald. It was written in Cython targeting efficiency.The source code has been merged to scikit-network and can be found here. Our implementation was competitive with state-of-the-art implementations of this kernel.

Languages

- English (C1), (IELTS band 8)
- Spanish(B1)

- Python /Cython/Sage	- Java	- C/C++	- Bash
- OCaml	- SQL	- Octave	- TypeScript

Research

Publications:

- Pierre Pébereau. *Singular points of UOV and VOX*. Eurocrypt 2025, May 2025.
- Pierre Pébereau. *One vector to rule them all: Key recovery from one vector in UOV schemes*. International Conference on Post-Quantum Cryptography, 2024.
- Eric Sageloli, Pierre Pébereau, Pierrick Méaux, Céline Chevalier. *Shorter and Faster Identity-Based Signatures with Tight Security in the (Q)ROM from Lattices.* International Conference on Applied Cryptography and Network Security, 2023.

Invited talks:

- *Geometric approach to the cryptanalysis of UOV,* Mathematics for post-quantum cryptanalysis, Budapest, 2024 [slides]

Preprints:

- Pierre Pébereau. *Subfield attack: leveraging composite-degree extensions in the Quotient Ring transform*. IACR eprint archive, February 2024

Seminars and short talks:

- Cryptanalysis of multivariate signatures from a geometric point of view. Séminaire cryptographie de l'**ANSSI**, 28 Mai 2025, Paris.
- Cryptanalysis of multivariate signatures from a geometric point of view. Séminaire GAE de l'**IRMAR**, 25 Avril 2025, Rennes (1h) [slides]
- Geometric approach to the cryptanalysis of UOV-based signatures (crypto flavor). **JC2** 2025 (20 mins) [slides]
- Geometric approach to the cryptanalysis of UOV-based signatures (computer algebra flavor). **JNCF** 2025 (20 mins) [slides]
- Schémas de signature post-quantiques: Construction et cryptanalyse. Journée des doctorants 2024, **Thales** [slides]
- Cryptanalysis of multivariate signatures: Singular points of UOV and VOX. **JNCF** 2024 [slides]
- Key recovery from one vector in UOV schemes. **ALMASTY** Seminar, January 19, 2024 [slides]
- Multivariate signature schemes and cryptanalysis of early proposals. **SIAM AG** 2023, symposium "Applications of Algebraic Geometry to Post-Quantum Cryptology"[slides]