CV (Year 2024-2025)

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

pierre.pebereau[at]lip6.fr

Education

December 2022- : Sorbonne Université, LIP6 / Thales
PhD Student under the supervision of Mohab Safey el Din and Simon Abelard.
Construction and Cryptanalysis of Post-Quantum Signature Schemes.

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 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 on specific subjects for “classe préparatoire” students each week.

Associations

2019-2021 : Technical Manager for association **Aurore.**
Aurore is an association providing internet access, ran 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.

From 2020 : Administrator of **Télécode**, competitive programming club of Télécom Paris. We breathed life to a long deceased club which aims to prepare ourselves and 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

Projects

2019-2021 : I 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
- OCaml
- Java
- SQL
- C/C++
- Octave
- Bash

Research

Publications:

- 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, 2024

Preprints:

- Pierre Pébereau. *Singular points of UOV and VOX*. IACR eprint archive, February 2024
- Pierre Pébereau. *Subfield attack: leveraging composite-degree extensions in the Quotient Ring transform*. IACR eprint archive, February 2024