Pierre Pébereau

PhD Candidate at Sorbonne Université/Thales

(+33)06 82 99 98 32
pierrepebereau@hotmail.fr
polsys.lip6.fr/~pebereau

Current and previous positions

2022-2025 PhD Candidate at LIP6, Sorbonne Université and Thales SIX.

2022-2022 Intern at Thales SIX Cryptography Lab.

2021-2021 Intern at INRIA Sophia Antipolis, team COATI

Short summary

My research interests are efficient algorithms for mathematical problems. During my PhD, I studied the cryptanalysis of post-quantum cryptographic algorithms, in particular multivariate signature schemes. I have shown the insecurity of NIST candidates by demonstrating practical attacks that run in seconds on a laptop, and more theoretical results that improve attacks by exponential factors. All the algorithms I design are implemented and tested, with practical and reproducible results. Eager to share my knowledge, I have taught for over 230 hours during my PhD and Masters.

Software

2024 Key recovery algorithm for UOV and VOX based on singular points. (SageMath) `https://github.com/pi-r2/SingPoints`

2023 Polynomial-time key recovery algorithm from one vector for UOV. (SageMath) `https://github.com/pi-r2/OneVector`

2021 Branch-and-bound algorithm for the computation of the pathlength of a graph. (Cython) `https://github.com/pi-r2/pathlength`

2020 Implementation with A. Barreaux of Weisfeiler-Lehman Graph Kernels in the scikit-network Python package. (Cython) `https://github.com/sknetwork-team/scikit-network/tree/master/sknetwork/topology`

Publications

Proceedings of conferences

2025 **Singular points of UOV and VOX.**
Proceedings of Eurocrypt 2025, available here `https://link.springer.com/chapter/10.1007/978-3-031-91095-1_11` or on HAL: `https://cnrs.hal.science/hal-04454521v3`.

2024 **One vector to rule them all: Key recovery from one vector in UOV schemes.**
Proceedings of PQCrypto 2024, avalaible here `https://link.springer.com/chapter/10.1007/978-3-031-62746-0_5` or on HAL: `https://cnrs.hal.science/hal-04215978v1`.

2023 **Shorter and Faster Identity-Based Signatures with Tight Security in the (Q)ROM from Lattices.**
with E. Sageloli, C. Chevalier, P. Méaux. Proceedings of ACNS 2023, avalaible here `https://link.springer.com/chapter/10.1007/978-3-031-33488-7_24` or on HAL `https://hal.science/hal-04107694`.

Preprints

Feb. 2024 **Subfield attack: leveraging composite-degree extensions in the Quotient Ring transform**
Avalaible on the IACR eprint archive: `https://ia.cr/2024/196`

Student supervision

Master thesis

2025 **Study of a multivariate post-quantum signature scheme: OV$\hat{+}$.**
4 months research project for a pair of master students at Sorbonne Université.

Teaching

Introduction to Algebraic Algorithms at Sorbonne Université

2025 **Lecture for master students.**
I gave a 4 hour lecture as an introduction to multivariate cryptology in the course Polynomial System Solving, wrote 10 pages of lecture notes and an exercise sheet.

2024 & 2025 **Exercise sessions for master students**
70 hours of exercise and lab sessions (SageMath and C) for ∼25 students on fast computer algebra (finite fields, formal power series, polynomials, structured/sparse matrices).

Computer science at Sorbonne Université

2024 **Algorithmics and programming for first-year bachelor students**
Exercise and lab sessions in Python for ∼35h.

2023 **Networks (TCP/IP) for third-year bachelor students**
Exercise and lab sessions (using Wireshark, Netkit, VirtualBox) for ∼35h.

2023 **Intro. to cryptology for third-year bachelor students**
Exercise and lab sessions in Python for ∼35h.

Mathematics at Lycée Janson-de-Sailly

2020-2022 **Mathematics for first-year CPGE students**
As a Khôlleur in mathematics, I designed exercise sheets and evaluated students during weekly oral interrogations in preparation of national competitive exams, for ∼60 hours.

Seminars, presentations and talks

Invited talks

August 2024 **International conference "Mathematics for post-quantum cryptanalysis"**
Geometric approach to the cryptanalysis of UOV.

July 2023 **Minisymposium of the international conference SIAM AAG 2023.**
Multivariate signature schemes and cryptanalysis of early proposals.

Talks at national events

April. 2025 **Journées Codage et Cryptographie (national French event) 2025.**
Geometric approach to the cryptanalysis of UOV-based signatures.

March 2025 **Journées nationales du calcul formel (national French event) 2025.**
Geometric approach to the cryptanalysis of UOV-based signatures.

March 2024 **Journées nationales du calcul formel (national French event) 2024.**
Cryptanalysis of multivariate signatures: Singular points of UOV and VOX.

Invitations and seminars

May 2025 Séminaire de Cryptographie, ANSSI, Paris.

April 2025 Effective Algebraic Geometry Seminar, IRMAR, Rennes.

June 2024 Journée des doctorants Thales, Genevilliers.

January 2024 ALMASTY Seminar, LIP6, Paris.

Academic duties

2024 Review for the international journal Design, Codes and Cryptography.

Education

2022–2025 **Ph.D. in computer science**, *Sorbonne Université*, Paris
CIFRE Funding from Thales SIX and ANRT. Supervised by Simon Abelard and Mohab Safey El Din: *Construction and cryptanalysis of post-quantum signature schemes.*

2021–2022 **Master Parisien de Recherche en Informatique**, *Université Paris-Cité*, Paris

2019–2022 **Cycle ingénieur**, *Télécom Paris*, Paris/Palaiseau
Specialised in applied mathematics, computer science and data science.
Received the degrees:
"Diplôme d'ingénieur de Télécom Paris" delivered by Télécom Paris.
"Diplôme de Master mention Informatique" delivered by Institut Polytechnique de Paris.

Associations

2019-2021 **Technical Manager and Liaison with Crous, Aurore**
Aurore is an association providing internet access to student residences. I took part in the maintainance and deployment of our network to a new residence in a contract for CROUS Versailles.

2020-2022 **Administrator, Télécode**
Télécode is the programming club of Télécom Paris. (Re)created this club with fellow students P. Gimalac and J. Béguinot. In 2021, hosted an operations research contest with TotalEnergies Digital Factory.