Valentina **Astore**

PHD STUDENT AT INRIA SACLAY & ÉCOLE POLYTECHNIQUE

Office 2046, Bâtiment Alan Turing - Campus de l'École polytechnique
1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France

✉ valentina.astore@inria.fr, valentina.astore@ip-paris.fr · ⌂ valentina-astore.github.io · 🖿 linkedin.com/in/valentina-astore

Education

PhD in Computer Science *Palaiseau, France*

INRIA PARIS-SACLAY & ÉCOLE POLYTECHNIQUE *Oct. 2024 - Present*

- Research Areas: Algebraic Coding Theory, Finite Fields, Finite Geometry, and applications to Cryptography.
- Supervisors: Alain Couvreur and Martino Borello.

MSc in Mathematics, curriculum Cryptography *Trento, Italy*

UNIVERSITY OF TRENTO *Sept. 2021 - March 2024*

- Highly selective Master program (10 students per year, with admission test).
- Attended courses: Algebra and its applications to Cryptography and Coding Theory, Computer science, Information theory.
- Graduation grade: 110 with honour/110.

Master's Project *Saint-Denis, France*

UNIVERSITY OF PARIS 8 - LAGA *Oct. 2023 - Dec. 2023*

- Topics: Coding Theory, Rank-Metric Codes, Distinguishers, Castelnuovo-Mumford Regularity.
- Supervisors: Martino Borello (University of Paris 8) and Marco Calderini (University of Trento).

BSc in Mathematics *Trento, Italy*

UNIVERSITY OF TRENTO *Sept. 2018 - Sept. 2021*

- Attended courses: Algebra, Analysis, Classical Physics, Computer Science, Geometry, Probability and Statistics.
- Bachelor's project: "Paillier Cryptosystem", Supervisor: Nadir Murru (University of Trento).
- Graduation grade: 108/110.

Teaching

TUTORING

Fall 2024 Foundations of Computer Science: Logic, Models, Computability and Computational Complexity.

Research

TALKS

Contributed talk at OpeRa 2024 - Open Problems on Rank-Metric Codes. 14-16 February 2024, Caserta (Italy).
Title of the talk: *Castelnuovo-Mumford Regularity in the Rank Metric*.

COURSES

PQCifris 2022 School on Post-Quantum Cryptography. October 2022, Trento (Italy).
Organizers: University of Trento and De Componendis Cifris (Italian national association).
Topics: post-quantum cryptography, multivariate-based, code-based, isogeny-based, and lattice-based methods.

De Cifris Trends in Modern Cryptography. March 2022 - May 2022, Trento (Italy).
Organizer: De Componendis Cifris (Italian national association).
Topics: post-quantum cryptography, cloud encryption and secure multiparty computation.