

Rocco Mora

✉ rocco.mora@cispa.de | 📅 December 19th, 1995 | 🏠 roccomora.github.io

Work Experience

Postdoctoral researcher

CISPA - Helmholtz Center for Information Security
• Algorithmic Cryptology group led by Antoine Joux

Sankt Ingbert, Germany
since November 2023

Research Engineer

Inria Paris Centre
• Project-team COSMIQ led by Jean-Pierre TILLICH

Paris, France
April 2023 - October 2023

Education

Ph.D. in Computer Science

Inria Paris Centre and Sorbonne University

- **Research interests:** Post-quantum cryptography, Code-based Cryptography, Algebraic coding theory, Gröbner bases, Algebraic cryptanalysis
- **Thesis title:** Algebraic techniques for decoding Reed-Solomon codes and cryptanalyzing McEliece-like cryptosystems
- **Thesis advisor:** Jean-Pierre TILLICH
- **Defence date:** April 7th, 2023

Paris, France
October 2019 - March 2023

Master in Mathematics, Curriculum “Coding Theory and Cryptography”

University of Trento

- **Final Mark:** 110/110 cum laude (full marks with honors)
- **Thesis title:** Efficient decoding algorithms for QC-LDPC and QC-MDPC code-based cryptosystems
- **Supervisors:** Prof. Marco BALDI, Prof. Massimiliano SALA
- **Defence date:** July 17th, 2019

Trento, Italy
October 2017 - July 2019

Bachelor in Mathematics

University of Parma

- **Final Mark:** 110/110 cum laude (full marks with honors)
- **Thesis title:** Lattice-based cryptography
- **Supervisor:** Prof. Alessandro ZACCAGNINI
- **Defence date:** October 24th, 2017

Parma, Italy
October 2014 - October 2017

Diploma in Piano

Conservatory of Music of Parma

- **Description:** Academic diploma equivalent to a Bachelor degree

Parma, Italy
October 2008 - September 2017

Maturity diploma

Scientific High School G. Marconi, Parma

Parma, Italy
September 2009 - July 2014

Teaching

TA of “CSE102 Computer Programming”

DIX, École Polytechnique

- Second course in Python for first year students of the B.Sc

Palaiseau, France
Spring 2022

TA of “INF442 Algorithms for data analysis in C++”

DIX, École Polytechnique

- Introduction to C++ and applications to data analysis techniques for second year students of the “Cycle Ingénieur polytechnicien”

Palaiseau, France
Spring 2021, Spring 2022

TA of “Computer Programming 2 - Programming in Java”

University of Trento

- Introduction to object-oriented programming and Java for first year Bachelor’s students in Computer Science and Engineering

Trento, Italy
Spring 2019

TA of “Informatics”

University of Trento

- Introduction to computer science for first year Bachelor’s students in Mathematics

Trento, Italy
Fall, 2018

Trainer for “Italian Mathematical Olympiad”

Liceo G. Marconi

- Trainer for local individual and team competitions of math Olympiad for high school students

Parma, Italy
2014 - 2016

- Trainer for local competitions of “Championnat International de Jeux Mathématiques et Logiques” for middle school students

Publications

JOURNAL ARTICLES

On the matrix code of quadratic relationships for a Goppa code

Rocco Mora

Advances in Mathematics of Communications (2024) pp. 0–0. DOI: 10.3934/amc.2024026

A polynomial time key-recovery attack on high-rate alternant codes

Magali Bardet, Rocco Mora, Jean-Pierre Tillich

IEEE Transactions on Information Theory (Nov. 2023). DOI: 10.1109/TIT.2023.3334592

On the dimension and structure of the square of the dual of a Goppa code

Rocco Mora, Jean-Pierre Tillich

Designs, Codes and Cryptography 91.4 (Apr. 2023) pp. 1351–1372. Springer. DOI: 10.1007/s10623-022-01153-w

CONFERENCE PROCEEDINGS

A new approach based on quadratic forms to attack the McEliece cryptosystem

Alain Couvreur, Rocco Mora, Jean-Pierre Tillich

Asiacrypt 2023. in publication, available at <https://eprint.iacr.org/2023/950>

Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach

Magali Bardet, Rocco Mora, Jean-Pierre Tillich

IEEE International Symposium on Information Theory (ISIT), July 2021. DOI: 10.1109/ISIT45174.2021.9517838

OTHER

Algebraic techniques for decoding Reed-Solomon codes and cryptanalyzing McEliece-like cryptosystems

Rocco Mora

Ph.D. thesis (Sorbonne University). Available at <https://theses.hal.science/THESES-SU/tel-04153803v2>

Talks

17 talks at seminars/workshops/conference

Achievements and Prizes

- 2024 **TII McEliece Challenges**, Prize of 10000\$ for the Theoretical Key-Recovery Algorithms track for the coauthored article “A New Approach Based on Quadratic Forms to Attack the McEliece Cryptosystem”
- 2023 **ERCIM “Alain Bensoussan” Postdoctoral Fellowship**, (refused)
- 2014 **Indam Scholarship**, Merit-based scholarship for students starting a Bachelor in Mathematics in Italy (40 scholarships in total, classified 15th in Italy)
- 2014 **Bronze Medal**, Italian Mathematical Olympiads
- 2013 **Bronze Medal**, Italian Mathematical Olympiads

Computer/Programming Skills

MAGMA, C, C++, PYTHON, JAVA, MATLAB, R, \TeX , Coq

Languages

- English** Full professional proficiency
- Italian** Native language
- French** Full professional proficiency