Rocco Mora

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

Work Experience

Postdoctoral researcher
Sankt Ingbert, Germany

CISPA - Helmholtz Center for Information Security
since November 2023

- Algorithmic Cryptology group led by Antoine Joux

Research Engineer
Paris, France

Inria Paris Centre
April 2023 - October 2023

- Project-team COSMIQ led by Jean-Pierre Tillich

Education

Ph.D. in Computer Science
Paris, France

Inria Paris Centre and Sorbonne University
October 2019 - March 2023

- **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

Master in Mathematics, Curriculum “Coding Theory and Cryptography”
Trento, Italy

University of Trento
October 2017 - July 2019

- **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

Bachelor in Mathematics
Parma, Italy

University of Parma
October 2014 - October 2017

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

Diploma in Piano
Parma, Italy

Conservatory of Music of Parma
October 2008 - September 2017

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

Maturity diploma
Parma, Italy

Scientific High School G. Marconi, Parma
September 2009 - July 2014

Teaching

TA of “CSE102 Computer Programming”
Palaiseau, France

DIX, École Polytechnique
Spring 2022

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

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

DIX, École Polytechnique
Spring 2021, Spring 2022

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

TA of “Computer Programming 2 - Programming in Java”
Trento, Italy

University of Trento
Spring 2019

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

TA of “Informatics”
Trento, Italy

University of Trento
Fall, 2018

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

Trainer for “Italian Mathematical Olympiad”
Parma, Italy

Liceo G. Marconi
2014 - 2016

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

Trainer for “Giochi della Bocconi” *Parma, Italy*

Liceo G. Marconi *2015*

- 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). 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

Other

- Given $>$10 talks at seminars and 5 talks at workshops/conferences, of which one invited;
- External reviewer of 3 articles for the journal Designs, Codes and Cryptography and 2 for the journal Transactions on Information Theory.

Achievements and Prizes

2024	**TII McEliece ChallengesII 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, LaTeX, Coq

Languages

English	Full professional proficiency
Italian	Native language
French	Full professional proficiency