Rocco Mora

rocco.mora@inria.fr | December 19th, 1995 | roccomora.github.io

Research interests

My current research interests lie primarily in the area of **code-based cryptography**. This includes cryptosystems whose security relies on the hardness of decoding a linear error correcting code and represents one of the most promising alternatives in **post-quantum cryptography**. In particular, I focused on the security of cryptographic schemes built from codes with an underlying algebraic structure, such as **GRS codes** and their subfield subcodes: **alternant** and **Goppa codes**. Their **cryptanalysis** involves the use of techniques borrowed from **algebraic coding theory** as well as from **computational algebra**, for instance **Gröbner bases**.

Education

Inria and Sorbonne University *Paris, France*

Ph.D. in Computer Science *Oct 2019 - Mar 2023*

- **Research interests:** Post-quantum cryptography, Code-based Cryptography, Algebraic coding theory, Gröbner basis, Algebraic cryptanalysis
- **Thesis title:** Algebraic techniques for decoding Reed-Solomon codes and cryptanalyzing McEliece-like cryptosystems
- **Advisor:** Jean-Pierre Tillich

University of Trento *Trento, Italy*

Master in Mathematics *Oct 2017 - Jul 2019*

- **Curriculum:** Coding Theory and Cryptography
- **Final Mark:** 110/110 cum laude (full marks with honors)
- **Thesis title:** Efficient decoding algorithms for QC-LDPC and QC-MDPC code-based cryptography
- **Advisor:** Prof. Marco Baldi

University of Parma *Parma, Italy*

Bachelor in Mathematics *Oct 2014 - Sep 2017*

- **Final Mark:** 110/110 cum laude (full marks with honors)
- **Thesis title:** Lattice-based Cryptography
- **Advisor:** Prof. Alessandro Zaccagnini

Conservatory of Music of Parma *Parma, Italy*

Diploma in Piano *Oct 2008 - Sep 2017*

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

Liceo Scientifico "G. Marconi" *Parma, Italy*

High-School Diploma *Sep 2009 - Jun 2014*

- **Curriculum:** P.N.I.: Scientific studies with focus on mathematics with informatics.

Work Experience

Inria *Paris, France*

Research Engineer *Apr 2023 - Current*

- Research in code-based cryptography.

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" *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

Computer/Programming Skills

MAGMA, C, C++, Python, Java, MATLAB, R, LaTeX, Coq

Achievements

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

Publications

Journal Articles

On the dimension and structure of the square of the dual of a Goppa code
Rocco Mora, Jean-Pierre Tillich
Designs, Codes and Cryptography (2022). 2022

Conference Proceedings

A new approach based on quadratic forms to attack the McEliece cryptosystem
Alain Couvreur, Rocco Mora, Jean-Pierre Tillich
Asiacrypt, 2023

Decoding Reed-Solomon codes by solving a bilinear system with a Gr246;bner basis approach
Magali Bardet, Rocco Mora, Jean-Pierre Tillich
IEEE International Symposium on Information Theory (ISIT), 2021

Preprints

A polynomial time key-recovery attack on high-rate alternant codes
Magali Bardet, Rocco Mora, Jean-Pierre Tillich
available at `https://arxiv.org/abs/2304.14757`, 2023

Other

Algebraic techniques for decoding Reed-Solomon codes and cryptanalyzing McEliece-like cryptosystems
Rocco Mora
Ph.D. thesis (Sorbonne University). Available at `https://roccomora.github.io/publications`, 2023

Talks

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

Workshop in Coding Theory and Cryptography, Virginia Tech Steger Center *Riva San Vitale, Switzerland*

July 2023

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

Code-based cryptography seminar, Inria Paris *Paris, France*

June 2023

Polynomial time attack on high-rate random alternant codes ,

Neuchatel - St.Gallen - Zurich joint seminar in Coding Theory and Cryptography, University of Zurich *University of Zurich, Switzerland*

May 2023

Key recovery of McEliece's scheme with random alternant codes of order 3 using Gröbner basis
French Days of Coding and Cryptography (JC2)
Hendaye, France
Apr 2022

Attacking high-rate alternant codes by filtration and Gröbner basis
Code-based cryptography seminar, Inria Paris
Paris, France
Apr 2022

On the dimension and structure of the square of the dual of a Goppa code
Discrete Mathematics, Codes and Cryptography Seminar, University Paris 8
Paris, France
Apr 2022

On the dimension and structure of the square of the dual of a Goppa code
The Twelfth International Workshop on Coding and Cryptography (WCC 2022)
Rostock, Germany
Mar 2022

Key recovery of McEliece's scheme with random alternant codes of order 3 using Gröbner basis
French Computer Algebra Days (JNCF 2022)
Luminy, France
Mar 2022

Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach
IEEE International Symposium on Information Theory (ISIT 2021)
Melbourne, Australia
Jul 2021

Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach
Code-based cryptography seminar, Inria Paris
Paris, France
Apr 2021

Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach
Grace team seminar, Inria Saclay
Saclay, France
Apr 2021

A randomized step-by-step decoder for LDPC codes
Code-based cryptography seminar, Inria Paris
Paris, France
Jan 2021

Languages

English Full professional proficiency
Italian Native language
French Limited proficiency