ROCCO MORA

PERSONAL INFORMATION

Born in Italy, 19 December 1995

rocco.mora@inria.fr

EDUCATION

Oct 2019 - Present — Sorbonne Université/INRIA Paris, France

PhD in Computer Science

Research interests: Post-quantum cryptography, Code-based Cryptography, Algebraic codes, Gröbner basis, Algebraic cryptanalysis
Project title: Alegbraic structures in code-based cryptography
Supervisor: Jean-Pierre Tillich

Oct 2017 - Jul 2019 — University of Trento, Italy

Masters of Mathematics

Curriculum: Coding Theory and Cryptography
Exams: Advanced Coding Theory and Cryptography, Algebraic Cryptography, Algebraic Geometry, Coding Theory and Applications, Algebraic Number Theory, Computability and Computational Complexity, Computational Algebra, Digital Signal Processing, Discrete Fourier Analysis, English Language (C1 level), Formal Techniques for Cryptographic Protocol Analysis, Galois Theory, Java Programming, Statistics of Stochastic Processes, Stochastic Processes.
Final Mark: 110/110 cum laude (full marks with honors)
Thesis title: Efficient decoding algorithms for QC-LDPC and QC-MDPC code-based cryptography
Supervisor: Prof. Massimiliano Sala
Co-advisor: Prof. Marco Baldi

Oct 2014 - Oct 2017 — University of Parma, Italy

Bachelor of Mathematics

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

Oct 2008 - Sep 2017 — Conservatory of Music of Parma, Italy

First level academic Diploma in piano

Description: The title is equivalent to a Bachelor degree.

Sep 2016 - Oct 2016 — University of Perugia, Italy

Summer school

Description: A math summer school reserved to INdAM scholarship winners.

Sep 2009 - Jun 2014 — Liceo Scientifico "G. Marconi" of Parma, Italy

High school Diploma

Description: Scientific studies.

TEACHING/WORK EXPERIENCE

Feb 2022 - May 2022 — Teaching Assistant for "CSE102 Computer Programming"

DIX, École Polytechnique

Teaching Assistant for a course in Python for undergraduate students.

Mar 2021 - May 2021 / Mar 2022 - May 2022
Teaching Assistant for "INF442 Algorithms for data analysis in C++"

DIX, École Polytechnique

Teaching Assistant for a course in C++ for data analysis for computer engineering undergraduate students.

Feb 2019 - May 2019
Teaching Assistant for "Linguaggi di Programmazione"

University of Trento

Teaching Assistant for a course in Java Programming for computer science and engineering undergraduate students.

Sep 2018 - Dec 2018
Teaching Assistant for "Informatica"

University of Trento

Teaching Assistant for an introductory course in computer science for math undergraduate students.

Oct 2014 - Feb 2016
Trainer for "Italian Mathematical Olympiad"

Liceo Scientifico "G. Marconi", Parma

Trainer for Italian Mathematical Olympiad for high school students.

Apr 2015 - May 2015
Trainer for "Giochi della Bocconi"

Liceo Scientifico "G. Marconi", Parma

Trainer for the Italian selection of "Championnat International de Jeux Mathématiques et Logiques" for middle school students.

PUBLICATIONS

DCC

"On the dimension and structure of the square of the dual of a Goppa code", joint work with Jean-Pierre Tillich, 2022

ISIT 2021

"Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach", joint work with Magali Bardet, Jean-Pierre Tillich, 2021

TALKS

French Days of Coding and Cryptography 2022
Inria Paris

Apr 2022 · "Key recovery of McEliece's scheme with random alternant codes of order 3 using Gröbner basis"

Apr 2022 · "Attacking high-rate alternant codes by filtration and Gröbner basis"

University Paris 8

Apr 2022 · "On the dimension and structure of the square of the dual of a Goppa code"

Workshop on Coding and Cryptography 2022

Mar 2022 · "On the dimension and structure of the square of the dual of a Goppa code"

French Computer Algebra Days 2022

Mar 2022 · "Key recovery of McEliece's scheme with random alternant codes of order 3 using Gröbner basis"

ISIT 2021

Jul 2021 · "Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach"

INRIA Paris — Apr 2021 · "Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach"

INRIA Saclay — Apr 2021 · "Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach"

INRIA Paris — Jan 2020 · "A randomized step-by-step decoder for LDPC codes"

University of Trento — May 2018 · "Shor's algorithm"

COMPUTER SKILLS

C, C++, PYTHON, JAVA, MATLAB, R, MAGMA, LaTeX, Coq

OTHER INFORMATION

Awards

May 2013/2014 · Twice Bronze Medal winner at Italian Mathematical Olympiad.

Sep 2014 · INdAM merit-based scholarship winner for math university entering students.

November 17, 2022