Rocco Mora

rocco.mora@cispa.de | 19 décembre 1995 | roccomora.github.io

Intérêts de recherche

Mes intérêts de recherche actuels se situent principalement dans le domaine de la **cryptographie post-quantique**, dont l'objectif est d'étudier les systèmes cryptographiques qui sont considérés comme sûrs même contre les algorithmes quantiques. En particulier, mes recherches portent sur la **cryptanalyse** de schémas issus de la **cryptographie basée sur les codes** et de la **cryptographie multivariée** à travers des techniques empruntées à l'**algèbre computationnelle**, telles que les **bases de Gröbner**. Je m'intéresse également à la **théorie algèbrique du codage**.

Expériences professionnelles

Chercheur postdoctoral — *Sankt Ingbert, Allemagne*

CISPA - Helmholtz Center for Information Security — *depuis novembre 2023*

- Groupe de Cryptologie Algorithmique dirigé par Antoine Joux

Ingénieur de recherche — *Paris, France*

Centre Inria de Paris — *avril 2023 - octobre 2023*

- Équipe-projet COSMIQ dirigé par Jean-Pierre Tillich

Éducation

Doctorat en Informatique — *Paris, France*

Centre Inria de Paris et Sorbonne Université — *octobre 2019 - mars 2023*

- **Intérêts de recherche:** Cryptographie post-quantique, Cryptographie basée sur les codes, Théorie du codage algébrique, Bases de Gröbner, Cryptanalyse algébrique
- **Titre de la thèse :** Techniques algébriques pour le décodage des codes de Reed-Solomon et cryptanalyse des schémas de type McEliece
- **Directeur de thèse :** Jean-Pierre Tillich
- **Date de soutenance :** 7 avril 2023

Master en Mathématiques - Parcours "Theorie des codes et Cryptographie" — *Trente, Italie*

Université de Trente — *octobre 2017 - juillet 2019*

- **Mention :** 110/110 cum laude (très bien)
- **Titre de la thèse :** Algorithmes de décodage efficaces pour les schémas cryptographiques basés sur les codes QC-LDPC et QC-MDPC
- **Directeurs de mémoire :** Prof. Marco Baldi, Prof. Massimiliano Sala
- **Date de soutenance :** 17 juillet 2019

Licence en Mathématiques — *Parme, Italie*

Université de Parme — *octobre 2014 - octobre 2017*

- **Mention :** 110/110 cum laude (très bien)
- **Titre de la thèse :** Cryptographie basée sur les réseaux euclidiens
- **Directeur de mémoire :** Prof. Alessandro Zaccagnini
- **Date de soutenance :** 24 octobre 2017

Diplôme en Piano — *Parme, Italie*

Conservatoire de musique de Parme — *octobre 2008 - septembre 2017*

- **Description :** Diplôme académique équivalent à une Licence

Baccalauréat Scientifique — *Parme, Italie*

Lycée Scientifique G. Marconi, Parme — *septembre 2009 - juillet 2014*

Enseignement

Moniteur pour les TD de "CSE102 Computer Programming" — *Palaiseau, France*

DIX, École Polytechnique — *Trimestre de printemps, 2022*

- Deuxième cours en Python pour les étudiants de première année du B.Sc.

Moniteur pour les TD de "INF442 Algorithms for data analysis in C++" — *Palaiseau, France*

DIX, École Polytechnique — *Trimestres de printemps, 2021, 2022*

- Introduction à C++ et applications aux techniques d'analyse de données pour les étudiants de deuxième année du cycle ingénieur polytechnicien

Moniteur pour les TD de "Computer Programming 2 - Programming in Java" *Trente, Italie*

University of Trento *Trimestre de printemps, 2019*

- Introduction à la programmation orientée objet et à Java pour les étudiants en première année de licence en informatique et ingénierie

Moniteur pour les TD de "Informatics" *Trente, Italie*

University of Trento *Trimestre d'automne, 2018*

- Introduction à l'informatique pour les étudiants de première année de licence en mathématiques

Formateur pour les "Olympiades Mathématiques italienne" *Parme, Italie*

Liceo G. Marconi *2014 - 2016*

- Formateur pour les compétitions locales individuelles et par équipe des Olympiades de mathématiques pour les élèves du lycée

Formateur pour le "Championnat International de Jeux Mathématiques et Logiques" *Parme, Italie*

Liceo G. Marconi *2015*

- Formateur pour les concours locaux du "Championnat International de Jeux Mathématiques et Logiques" destinés aux élèves du collège

Publications

Articles de revues

Understanding the new distinguisher of alternant codes at degree 2
Axel Lemoine, Rocco Mora, Jean-Pierre Tillich
Designs, Codes and Cryptography (2025)

On the matrix code of quadratic relationships for a Goppa code
Rocco Mora
Advances in Mathematics of Communications (2025)

A polynomial time key-recovery attack on high-rate alternant codes
Magali Bardet, Rocco Mora, Jean-Pierre Tillich
IEEE Transactions on Information Theory (2024)

On the dimension and structure of the square of the dual of a Goppa code
Rocco Mora, Jean-Pierre Tillich
Designs, Codes and Cryptography (2023)

Actes de conférence

Quadratic Modelings of Syndrome Decoding
Alessio Caminata, Ryann Cartor, Alessio Meneghetti, Rocco Mora, Alex Pellegrini
PQCrypto 2025

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 Gröbner basis approach
Magali Bardet, Rocco Mora, Jean-Pierre Tillich
IEEE International Symposium on Information Theory (ISIT) 2021

Prépublications

The regular multivariate quadratic problem
Antoine Joux, Rocco Mora

Autres textes

Algebraic techniques for decoding Reed-Solomon codes and cryptanalyzing McEliece-like cryptosystems
Rocco Mora
PhD thesis

Service académique et autres activités

- Co-organisateur du séminaire du groupe "Cryptographie et Codage" de l'UMI (Union mathématique italienne) à partir du printemps 2025.
- Réviseur externe pour les journaux "Designs, Codes and Cryptography", "Transactions on Information Theory" et "Journal of Mathematical Cryptology". Sous-réviseur pour Eurocrypt 2025.

- Membre du jury d'une soutenance de doctorat.

Talks

Products of codes and cryptanalysis in code-based cryptography — *San Cristóbal de La Laguna, Espagne*
Séminaire GASIULL, Universidad de la Laguna — *Avril 2025*

Products of codes and applications to code equivalence — *en ligne*
Séminaire ACCESS — *Mars 2025*

The regular multivariate quadratic problem — *Versailles, France*
Séminaire de l'équipe CRYPTO, UVSQ — *Mars 2025*

The regular multivariate quadratic problem — *Saclay, France*
Séminaire de l'équipe Grace, Inria Saclay — *Mars 2025*

Products of codes and cryptanalysis in code-based cryptography — *Paris, France*
Workshop COSMO 2025, Inria Paris (**invité**) — *Mars 2025*

The regular multivariate quadratic problem — *Paris, France*
Séminaire de l'équipe ALMASTY, Sorbonne Universitè — *Mars 2025*

The regular multivariate quadratic problem — *Montpellier, France*
Séminaire de l'équipe ECO, LIRMM — *Décembre 2024*

The regular multivariate quadratic problem — *Genova, Italy*
Young Cryptographers in Genova (**invité**) — *Novembre 2024*

The regular multivariate quadratic problem — *Rome, Italy*
ReAdPQC24 workshop - conférence CIFRIS24 (**invité**) — *Septembre 2024*

A new approach based on quadratic forms to attack the McEliece cryptosystem — *Nancy, France*
CISPA-LORIA workshop (**invité**) — *Juin 2024*

A new approach based on quadratic forms to attack the McEliece cryptosystem — *Rennes, France*
Séminaire de géométrie et algèbre effectives, IRMAR — *Avril 2024*

A new approach based on quadratic forms to attack the McEliece cryptosystem — *Bordeaux, France*
Séminaire de Théorie Algorithmique des Nombres, IMB Bordeaux — *Mars 2024*

A new approach based on quadratic forms to attack the McEliece cryptosystem — *Amsterdam, Netherlands*
Séminaire de cryptographie du CWI — *Janvier 2024*

A new approach based on quadratic forms to attack the McEliece cryptosystem — *Sankt Ingbert, Germany*
Séminaire de cryptographie du CISPA — *Janvier 2024*

A new approach based on quadratic forms to attack the McEliece cryptosystem — *Guangzhou, China*
Asiacrypt 2023 — *Décembre 2023*

A new approach based on quadratic forms to attack the McEliece cryptosystem — *Riva San Vitale, Switzerland*
Workshop en Théorie des Codes et Cryptographie, Virginia Tech Steger Center (**invité**) — *Juillet 2023*

Polynomial time attack on high-rate random alternant codes — *University of Zurich, Switzerland*
Neuchatel - St.Gallen - Zurich séminaire conjoint en théorie des codes et cryptographie, University of Zurich — *Mai 2023*

Key recovery of McEliece's scheme with random alternant codes of order 3 using Gröbner basis — *Hendaye, France*
Journées C2 (codage et cryptographie) — *Avril 2022*

Attacking high-rate alternant codes by filtration and Gröbner basis — *Paris, France*
Séminaire cryptographie à base de codes, Inria Paris — *Avril 2022*

On the dimension and structure of the square of the dual of a Goppa code — *Paris, France*
Séminaire Mathématiques Discrètes, Codes et Cryptographie, Paris 8 — *Avril 2022*

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

Key recovery of McEliece's scheme with random alternant codes of order 3 using Gröbner basis — *Luminy, France*
Journées Nationales de Calcul Formel (JNCF 2022) — *Mars 2022*

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

Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach — *Paris, France*
Séminaire cryptographie à base de codes, Inria Paris — *Avril 2021*

Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach — *Saclay, France*
Séminaire de l'équipe Grace, Inria Saclay — *Avril 2021*

A randomized step-by-step decoder for LDPC codes — *Paris, France*
Séminaire cryptographie à base de codes, Inria Paris — *Janvier 2021*

Autres accomplissements et Prix

2024 **TII McEliece Challenges,** Prix de 10000$ pour avoir gagné la catégorie *Theoretical Key-Recovery Algorithms* avec l'article cosigné "A new approach based on quadratic Forms to attack the McEliece cryptosystem"
2023 **Bourse postdoctorale ERCIM "Alain Bensoussan",** (refusé)
2014 **Bourse Indam,** Bourse au mérite pour les étudiants commençant une Licence en Mathématiques en Italie (40 bourses au total, classées 15e en Italie
2014 **Médaille de bronze,** Olympiades italiennes de mathématiques
2013 **Médaille de bronze,** Olympiades italiennes de mathématiques

Computer/Programming Skills

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

Langues

Anglais Compétences professionnelles complètes
Italien Langue maternelle
Français Compétences professionnelles complètes