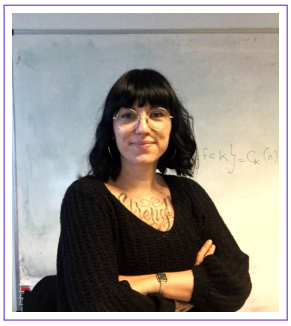

Ilaria Zappatore

Post-Doc at INRIA Saclay-Île-de-France

Personal Information

Birthplace: Taranto (Italy)
Birthdate: May 18, 1990
Citizenship: Italian

Current Position

November 2020 – September 2022 **Postdoc fellow**, *team GRACE, LIX (Laboratoire d'Informatique de l'École Polytechnique), INRIA Saclay-Île-de-France*, France.

Education

2021 **Qualified in section 25-26-27 (CNU).**

2017-2020 **Ph.D. program in Computer Science**, *LIRMM, University of Montpellier*, France, Supervisors: Laurent Imbert, Eleonora Guerrini, Romain Lebreton.

Thesis: "Simultaneous Rational Function Reconstruction and Applications to Algebraic Coding Theory."

Jury:

- Daniel Augot (*Rapporteur*), *Directeur de Recherche* INRIA-Saclay Palaiseau (France),
- Clément PERNET (*Rapporteur*), *Maître de Conférences* Université Grenoble Alpes, LJK, Grenoble (France),
- Magali BARDET (*Examiner*), *Maître de Conférences* Université de Rouen, LITIS, Rouen (France),
- Elisa GORLA (*Examiner*), *Professeur* Université de Neuchâtel (Switzerland),
- Gilles VILLARD (*President of the jury*), *Directeur de Recherche* CNRS, LIP, Lyon,
- Laurent IMBERT (*Supervisor*), *Directeur de Recherche* CNRS, LIRMM, Montpellier (France),
- Eleonora GUERRINI (*Supervisor*), *Maître de Conférences* Université de Montpellier, LIRMM, Montpellier (France),
- Romain LEBRETON (*Supervisor*), *Maître de Conférences* Université de Montpellier, LIRMM, Montpellier (France).

2014-2017 **Master Degree in Mathematics (Coding Theory and Cryptography)**, *University of Trento*, Italy, Thesis: "Primitivity of generalized translation based block ciphers".
Final mark: 110/110 cum laude

2009-2014 **Bachelor Degree in Mathematics**, *University of Bari*, Italy, Thesis: "Primality tests and factorization algorithms: a cryptographic approach".
Final mark: 106/110

2004-2009 **High School Diploma (Science Studies)**, *Liceo Scientifico Battaglini*, Taranto, Italy.
Final mark: 100/100

Internship supervision

2022 **Supervisor of an L3 Bachelor Thesis**, *"Efficient decoding of Reed-Solomon codes"*.

Teaching

2021–2022 **Teaching assistant (*Vacations*), responsible of laboratory sessions for the Bachelor program of the École Polytechnique, Palaiseau**, *France*.
- Introduction to Computer Programming (Python)(TD, L1),
- Advanced Programming (Python) (TD, L1)

2019–2020 **Teaching assistant (*Mission Complémentaire d'Enseignement*) at the University of Montpellier**, *France*.
- Introduction à l'algorithmique et à la programmation (TD-TP, L1),
- Modélisation et programmation objet 1 (Java) (TD-TP, L2)

2018–2019 **Teaching assistant (*Mission Complémentaire d'Enseignement*) at the University of Montpellier**, *France*.
- Introduction à l'algorithmique et à la programmation (TD-TP, L1),
- Programmation Linéaire (TP, L3)

2017–2018 **Teaching assistant (*Mission Complémentaire d'Enseignement*) at the University of Montpellier**, *France*.
- Programmation Linéaire (TP, L3),
- Programmation Applicative (Scheme) (TP L2),
- Programmation Impérative (C++) (TP, L1)

Professional Experiences

February–July 2016 **Internship at AliasLab S.p.A.**, *Via Cremona 27/6*, Mantova, Italy, *Design and implementation of an electronic signature software using the Bitcoin Blockchain and the Ethereum one.*
Business sector: computer science

Publications

Proceedings

2021 **Polynomial Linear System Solving with Random Errors: New Bounds and Early Termination Technique**, *Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore*, Proceedings of ISSAC'21.

2020 **On the Uniqueness of the Simultaneous Rational Function Reconstruction**, *Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore*, Proceedings of ISSAC'20.

2019 **Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon codes**, *Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore*, Proceedings of ISIT'19.

Additional infos **In my research fields the authors are listed in alphabetical order. The *International Symposium on Symbolic and Algebraic Computation (ISSAC)* is the premier conference for research in symbolic computation and computer algebra. The *IEEE International Symposium on Information Theory (ISIT)* is the flagship conference dedicated to the advancement of information theory and related areas.**

Journals

2019 **Wave-shaped round functions and primitive groups**, *Riccardo Aragona, Marco Calderini, Roberto Civino, Massimiliano Sala, Ilaria Zappatore*, Advances in Mathematics of Communications 13,1.

Preprints

2022 **Simultaneous Rational Function Reconstruction with Errors: handling poles and multiplicities.**, *Eleonora Guerrini, Kamel Lairedj, Romain Lebreton, Ilaria Zappatore*, (submitted).

2020 **Enhancing simultaneous rational function recovery: adaptive error correction capability and new bounds for applications**, *Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore.*

In progress

2022 **An algebraic Overbeck attack to the GPT cryptosystem based on Twisted Gabidulin codes**, *Alain Couvreur, Ilaria Zappatore.*

2021 **Computing the Discrete Logarithm over Finite Fields using Reed-Solomon codes**, *Daniel Augot, François Morain, Ilaria Zappatore.*

Talks at International Conferences

2021 **Polynomial Linear System Solving with Random Errors: new bounds and Early Termination Technique**, *ISSAC'21*, Saint Petersburg, Russia.

2020 **On the Uniqueness of the Simultaneous Rational Function Reconstruction**, *ISSAC'20*, Kalamata, Greece.

2019 **Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon codes**, *ISIT'19*, Paris, France.

Other Research Talks

2022 **Simultaneous Rational Function Reconstruction with errors:handling poles and multiplicities**.

- February 2022, Journées Nationales de Calcul Formel (JNCF), CIRM, Luminy, France.
- February 2022, Invited Talk, Séminaire de l'équipe Algèbre, Géomètrie, Combinatoire et applications à la Cryptographie et au Codage, Laboratoire LAGA, Paris 8, France.
- January 2022, Invited Talk, Séminaire CASC, Laboratoire Jean Kuntzmann, Grenoble, France.

2021 **Una tecnica per costruire algoritmi resistenti agli errori per la risoluzione di sistemi lineari polinomiali.**, *Seminario di Crittografia e Codici, gruppo UMI*, Online, (November).

2021 **Polynomial Linear System Solving with Random Errors: new bounds and Early Termination Technique**, *Journées Nationales de Calcul Formel (JNCF)*, CIRM, Luminy, France (Mars).

2021 **Simultaneous Rational Function Reconstruction and application to Coding Theory**.

- Mars 2021, Invited Talk, Séminaire Limousin de Calcul Formel, XLIM, Limoges, France
- February 2021, Invited Talk, PolSys SpecFun Seminar, LIP6, Sorbonne Université, Paris, France.

2020 **Décodage des codes Reed-Solomon classiques et entrelacés du point de vue du Calcul Formel : le problème de la Reconstruction Rationnelle**, *Groupe de Travail de (post) doctorants de l'equipe GRACE, Inria-Saclay*, (December).

2020 **Algorithm-Based Fault Tolerant Technique for Polynomial Linear System Solving by Evaluation-Interpolation**.

- September 2021, Cryptography and Coding Theory, `First Annual Conference`,
- December 2020, Invited Talk, Groupe de Travail de l'équipe GRACE, INRIA-Saclay,
- November 2020, Journées Codage et Cryptographie `Journées C2'20`

2020 **On the Uniqueness of the Simultaneous Rational Function Reconstruction**.

- June 2020, Invited Talk, Laboratoire Jean Kuntzmann, Grenoble, France
- Mars 2020, Journées Nationales de Calcul Formel (JNCF), CIRM, Luminy, France

2018–2019 **Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon codes**.

- Mars 2019, Invited Talk, Laboratoire IMATH-CPT-COSMER, University of Toulon, France,
- February 2019, Journées Nationales de Calcul Formel (JNCF), CIRM, Luminy, France,
- October 2018, Journées C2, Assois, France.

Awards and Grants

2019 **Student Travel Grant ISIT'19**.

2018 **Merit Award 2018 for master students**, *University of Trento*, Italy.

Active Involvement in Scientific Activities

2022 **Member of the ANR Project Barracuda**.
The goal of this project is to bring together researchers specialized in coding and cryptography on the one hand and in number theory and algebraic geometry on the other hand to work on cryptographic problems requiring the introduction of advanced algebraic structures and/or techniques, such as distributed storage, multiparty computation or zero-knowledge disclosure proofs.

2021 **Reviewer of the proceedings of ISSAC'21 and of the journal IEEE Transaction on Information Theory**.

2020 **Member of the Organizing Committee of STACS 2020**, *Montpellier, France*, Website developer.

Scientific Dissemination

2022 **Animator of a research atelier at the *Rendez-vous des jeunes mathématiciennes et informaticiennes***, *Inria-Saclay, France*.
Event aiming to arise interest in research in mathematics and computer science to young high school girls.

2018 **Member of the Organizing Committee of MAth.en.JEANS**, *Montpellier, France*.
Conference that aims to let secondary and high school students discover the research in math.

Technical Skills

Languages C++, C, Java, C#, .NET, HTML/CSS, Javascript, Magma, Python, sagemath, Matlab, RStudio, The Coq Proof Assistant, scheme

Extra-Curricular Activities

Languages: English (B2), French (C1), Italian (Mother Tongue)

Others: I love to sing, I am a black belt in karate, I have been a volunteer for disables for many years.