



Ilaria Zappatore

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

“The important thing is not to stop questioning. Curiosity has its own reason for existing.”- Albert Einstein

Personal Information

Birthplace: Taranto (Italy)

Birthdate: May 18, 1990

Citizenship: Italian

Research Interests

Algebraic Coding Theory, Computer Algebra, Cryptography

Education

- November 2020 **Post-Doc**, team GRACE, LIX (Laboratoire d'Informatique de l'École Polytechnique), INRIA Saclay-Île-de-France, France, subject: “Computing the discrete logarithm over finite fields using Reed-Solomon codes” team GRACE.
Now
- 2017 **Ph.D. program in Computer Science**, LIRMM, University of Montpellier, France, Supervisors: Laurent Imbert, Eleonora Guerrini, Romain Lebreton.
October 2020 Thesis: “Simultaneous Rational Function Reconstruction and Applications to Algebraic Coding Theory.”
- 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

Teaching

- 2019–2020 **Teaching assistant 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 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 at the University of Montpellier, France.**
- Programmation Linéaire (TP, L3),
 - Programmation Applicative (Scheme) (TP L2),
 - Programmation Impérative (C++) (TP, L1)

Internships

February–July 2016 **AliasLab S.p.A.**, *Via Cremona 27/6*, Mantova, Italy, Analysis and implementation in the Blockchain field also focusing on the study of other Altchains such as Ethereum, BigChainDB, Multichain.
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.

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, work in progress

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

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

Research Talks

- 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'équipe GRACE, Inria-Saclay*, (December).
- 2020 **Algorithm-Based Fault Tolerant Technique for Polynomial Linear System Solving by Evaluation-Interpolation**.
- decembre 2020, Invited Talk, Groupe de Travail de l'équipe GRACE, INRIA-Saclay,
 - novembre 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

- 2019 **Student Travel Grant ISIT'19**.
- 2018 **Merit Award 2018 for master students**, *University of Trento*, Italy.

Active Involvement in Scientific Activities

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