

Elia Onofri

Postdoctoral Researcher · KAUST — CEMSE Division

Scientific Committee & Professor · MDA, Roma Tre
Member · De Cifris (Italian Cryptography Association)
Member · Mensa International
Coordinator · SIG Intellect Research, Mensa Italy



RESEARCH FOCUS

Cryptography, (cyber)security & privacy as a foundation: from algebraic cryptanalysis and post-quantum constructions to privacy-preserving protocols.

Graph theory, applied mathematics, and artificial intelligence as a passion: from combinatorial structure and numerical modelling to learning systems and graph-based methods.

Turn mathematical structure into something you can prove, compute, or see as a mission.

Current work spans hallucination characterisation and detection in language models, AI-generated content fingerprinting via signal analysis, and the design of privacy-preserving cryptographic protocols. Earlier work addressed macroscopic traffic and pedestrian flow modelling, multi-scale simulation of biological and immune systems, and mathematical modelling of water transport and stone decay in cultural heritage conservation.

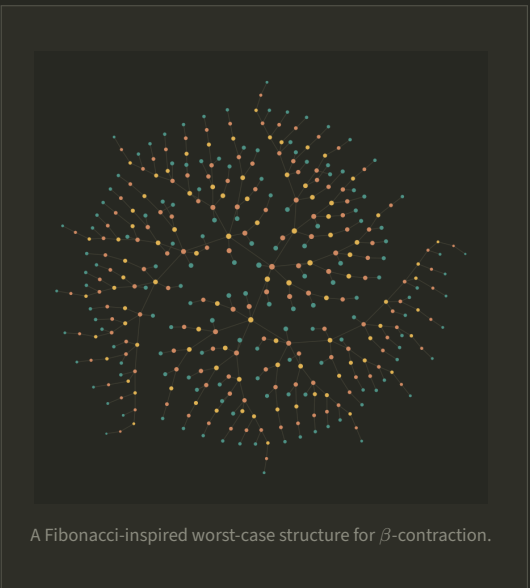
CONTACT

✉ EMAIL elia.onofri@kaust.edu.sa
✉ EMAIL elia.onofri@cnr.it
✉ EMAIL eonofri@uniroma3.it
🏠 HOME www.eliaonofri.it

Thuwal (KSA) · Rome (Italy)

IDENTIFIERS

🆔 ORCID [0000-0001-8391-2563](https://orcid.org/0000-0001-8391-2563)
📖 SCHOLAR [7IAjzLEAAAAJ](https://scholar.google.com/citations?user=7IAjzLEAAAAJ)
📄 SCOPUS [57215199778](https://scopus.com/authid/detail.url?authorID=57215199778)
🐙 GITHUB [eOnofri04](https://github.com/eOnofri04)
🌐 LINKEDIN [elia-onofri-80b403173](https://www.linkedin.com/in/elia-onofri-80b403173)



METRICS

152

Citations

2

i10-index

12

Proceedings

9

Students supervised

6

h-index

13

Journal articles

41

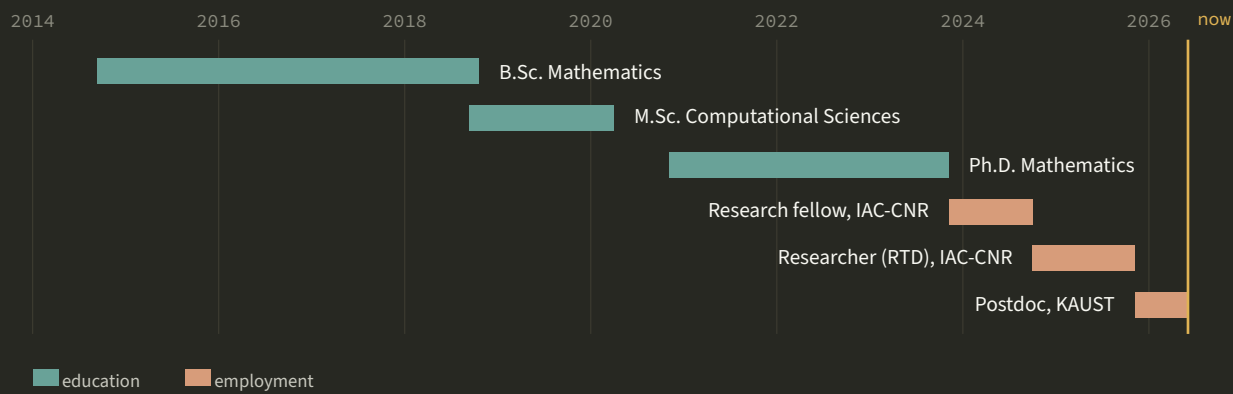
Invited talks

3

Erdős number

Citations via OpenAlex, anchored to indexed DOIs
· updated 2026-10-12

EXPERIENCE AT A GLANCE



EDUCATION

1 November 2020
31 October 2023

Doctor of Philosophy

Mathematics (Ph.D.), *Magna cum Laude*

Roma Tre University

*Piazzale S. L. Murialdo, 1
00146, Rome, Italy
Tel. (+39) 06-5733 8254/03*

- Thesis Title: ML- and graph-based methods for data analysis and prediction: applications in vehicular traffic, pedestrian dynamics, and computational biology
- Supervisors: Filippo CASTIGLIONE (BRC-TII), Emiliano CRISTIANI (IAC-CNR), Marco PEDICINI (Roma Tre)
- Dissertation committee: Roberto NATALINI (IAC-CNR), Fosca GIANNOTTI (SNS Pisa), Vincenzo BONIFACI (Roma Tre)
- Defence Date: November 8th, 2023
- DOI: 10.13140/RG.2.2.32948.36489.

September 2018
March 2020

Master's Degree

Computational Sciences (M.Sc.), *Magna cum Laude*

Roma Tre University

- Curriculum: Cryptography and Security
- Thesis Title: "A Computational Investigation of the Cube Attack in General Finite Fields"
- Supervisor: Marco PEDICINI
- Defence Date: March 18th, 2020
- Final Mark: 110/110 *cum Laude*

September 2014
October 2018

Bachelor's Degree

Mathematical Sciences (B.Sc.)

Roma Tre University

- Curriculum: Mathematics for scientific calculus
- Thesis Title: "About resolution of algebraic systems over finite fields: Buchberger Algorithm, Gröbner bases and Computational Complexity"
- Supervisor: Marco PEDICINI
- Defence Date: October 18th, 2018
- Final Mark: 104/110

SCHOOLS AND COURSES

1 November 2024 30 November 2024	Training course Technology Transfer and Patent Protection <i>IAC–CNR, H2IOSC project</i> Instructed by Andrea Scilletta, IP Sextnat s.r.l.
17 June 2024 21 June 2024	Summer school 2nd CINI Summer School on HPC and Emerging Technologies <i>Trento University, Trento, Italy</i> WEBSITE: hpc-summer-school-24 disi.unitn.it 
13 June 2022 17 June 2022	Summer school Summer School on real-world crypto & privacy <i>Šibenik, Croatia (Org. by Radboud University, Nijmegen, Netherlands)</i> WEBSITE: summerschool-croatia.cs.ru.nl/2022/ 
6 June 2022 10 June 2022	Summer school Boston Differential Privacy Summer School <i>Boston University, Boston (MA), USA</i> WEBSITE: bostondataprivacy.github.io/summerschool 
1 September 2019 30 November 2019	Scholar internship Foundation of High Performance Computing <i>Scuola Internazionale Superiore di Studi Avanzati di Trieste (SISSA)</i> Lectures from the master in High Performance Computing (ref. Luciano TERESI)

WORK EXPERIENCES

RESEARCH

19 October 2025 current	Postdoctoral Researcher <i>King Abdullah University of Science and Technology (KAUST)</i> <i>Computer, Electrical and Mathematical Science and Engineering (CEMSE) Division</i> <i>Box 4700, Thuwal 23955-6900, Saudi Arabia (KSA)</i> Conduct research in applied mathematics and computer science to identify and address biases and (cyber)security threats in large language model (LLM) platforms across diverse operational contexts (ref. Roberto DI PIETRO, project BAS/1/1701-01-01, Uncovering and Addressing Bias in LLM Interactions)
3 October 2024 17 November 2025	Researcher (RTD), III Level <i>National Research Council of Italy (CNR)</i> <i>Istituto per le Applicazioni del Calcolo ‘M. Picone’ (IAC), Naples Operating Center</i> <i>Via Pietro Castellino 111, 80131, Naples, Italia</i> Research activities in mathematical modelling, data analysis, implementation, and parallelisation of algorithms based on mathematical models (ref. Gabriella BRETTI, project PNRR H2IOSC CUP B63C22000730005)
1 November 2023 2 October 2024	Research fellow with research grant (type A) <i>National Research Council of Italy (CNR)</i> <i>Istituto per le Applicazioni del Calcolo ‘M. Picone’ (IAC)</i> <i>Via dei Taurini 19, 00185, Rome, Italy</i> Development of a mathematical and computational multi-scale model for the in-silico simulation of the immune system response (ref. Paolo TIERI, project PRAESIIDIUM G.A. 101095672)

1 September 2022
31 October 2022

Occasional provision of services

The Solomon R. Guggenheim Foundation

Peggy Guggenheim Collection

Venier dei Leoni Palace, Dorsoduro 701, 30123, Venice, Italy

Develop of a pedestrian dynamics simulation. Measurement of the room occupancy inside the museum. Optimisation of visitors flows, to reduce thermohygrometric fluctuations to better preserve artworks (ref. Luciano PENSABENE)

15 October 2019
15 April 2020

Post-laurea research activity

Roma Tre University

Development and implementation of topological structures for point cloud management (ref. Alberto PAOLUZZI)

June 2019
October 2019

Student internship

National Research Council of Italy (CNR)

Istituto per le Applicazioni del Calcolo 'M. Picone' (IAC)

Development of a software to gather, manage and analyse data from pedestrian tracking in IoT environment (ref. Emiliano CRISTIANI)

TEACHING

A.Y.s 2022 – 2025

Substitute Teaching

“Roma Tre” University

Courses for mathematical sciences B.Sc. degree (L-35) and computational sciences M.Sc. degree (LM-40):

- *IN400 - Module A - Python Programming* [INF/01] (A.Y. 2024/25, L-35, LM-40)

Courses for the master in data analytics (MDA, second level, post-M.Sc.):

- *Cryptography: Case Study* [INF/01] (A.Y. 2026, MDA)
- *Foundations of Cryptography* [INF/01] (A.Y. 2026, MDA)

Courses for the master in data analytics (MDA, first level, post-B.Sc.):

- *Cryptography: Case Study* [INF/01] (A.Y. 2026, MDA)
- *Foundations of Cryptography* [INF/01] (A.Y. 2026, MDA)
- *Cryptography I* [INF/01] (A.Y. 2025, MDA)
- *Cryptography: Case Study* [INF/01] (A.Y. 2025, MDA)
- *Cryptography II* [INF/01] (A.Y. 2024, MDA)
- *Cryptography II* [INF/01] (A.Y. 2023, MDA)

A.Y.s 2020 – 2025

Supplementary Teaching (didattica integrativa)

“Roma Tre” University

Courses for mathematical sciences B.Sc. degree (L-35) and computational sciences M.Sc. degree (LM-40):

- *IN110 - Algorithms and data structure* [INF/01] (A.Y. 2024/25, L-35)
- *CR410/B - Public key cryptography* [MAT/02] (A.Y. 2023/24, LM-40)
- *IN110 - Algorithms and data structure* [INF/01] (A.Y. 2023/24, L-35)
- *CR410/B - Public key cryptography* [MAT/02] (A.Y. 2022/23, LM-40)
- *IN110 - Algorithms and data structure* [INF/01] (A.Y. 2021/22, L-35)
- *IN110 - Algorithms and data structure* [INF/01] (A.Y. 2020/21, L-35)

A.Y.s 2018–2023

Tutoring Teaching (Tutoraggio)

“Roma Tre” University

Tutor for mathematics and physics bachelor degree (L-30, L-35):

- *IN110 - Algorithms and data structure* (A.Y. 2022/23, L-35)
- *ad personam support for 1st year* (June 2021 – October 2022, L-30/L-35)
- *IN110 - Algorithms and data structure* (summer A.Y. 2020/21, L-35)
- *AM210 - Mathematical analysis 3* (A.Y. 2018/19, L-35)

TECHNICAL SKILLS



expert



proficient



familiar

OPERATING SYSTEMS

OSX Apple iOS Linux Microsoft Windows Android Docker

PROGRAMMING LANGUAGES

C Python Java C++ (scientific) Julia SQL/SQLite/PostgreSQL Markup
Markdown CUDA Bash Rust Pascal XCode Lambda Calculus Node

SCIENTIFIC COMPUTING

MATLAB Mathematica Jupyter NumPy/SciPy OpenMP/MPI PARI/GP
Torch

SOFTWARE

Latex Office IWork VS Code Eclipse

ACADEMIC / SCIENTIFIC COMPETENCES

Cryptography Cybersecurity Machine Learning Graph Theory ABM / Multiscale
Object Oriented Artificial Intelligence Comp. Biology Comp. Topology

OTHERS

Git LLMs Mentorship Team Building UML Blockchain 2D/3D Graphics
Video Editing Cloud/HPC Network

PUBLICATIONS

✉ marks the corresponding author.

Journal Articles

- [1] Pietro Centorrino, Alessandro Corbetta, Emiliano Cristiani✉, and Elia Onofri. *Managing crowded museums: visitors flow measurement, analysis, modeling, and optimization*. In: Journal of Computational Science, Elsevier 53 (Apr. 2021), pp. 1–17. ISSN: 1877-7503. DOI: 10.1016/j.jocs.2021.101357.
- [2] Filippo Castiglione, Christine Nardini, Elia Onofri✉, Marco Pedicini, and Paolo Tieri. *Explainable drug repurposing approach from biased random walks*. In: IEEE/ACM Transactions on Computational Biology and Bioinformatics (July 2022), pp. 1009–1019. DOI: 10.1109/TCBB.2022.3191392.
- [3] Flavio Lombardi and Elia Onofri✉. *Some results on colored network contraction*. In: Journal of Ubiquitous Systems and Pervasive Networks, IASK 17.2 (Dec. 2022), pp. 91–98. DOI: 10.5383/JUSPN.17.02.006.
- [4] Marco Cianfriglia, Elia Onofri✉, Silvia Onofri, and Marco Pedicini. *Fourteen years of cube attacks*. In: Applicable Algebra in Engineering, Communication and Computing, Springer Nature (May 2023), pp. 1–43. DOI: 10.1007/s00200-023-00602-w.
- [5] Alberto Paoluzzi✉, Vadim Shapiro, Antonio DiCarlo, Giorgio Scorzelli, and Elia Onofri. *Finite algebras for solid modeling using Julia's sparse arrays*. In: Computer-Aided Design, Elsevier 155 (Feb. 2023), p. 103436. ISSN: 0010-4485. DOI: 10.1016/j.cad.2022.103436.
- [6] Maya Briani, Emiliano Cristiani, and Elia Onofri✉. *Inverting the Fundamental Diagram and Forecasting Boundary Conditions: How Machine Learning Can Improve Macroscopic Models for Traffic Flow*. In: Advances in Computational Mathematics (ACOM), Elsevier 50 (115 Dec. 2024), pp. 1–30. DOI: 10.1007/s10444-024-10206-8.
- [7] Marco Cianfriglia, Elia Onofri✉, and Marco Pedicini. *mR_{LWE}-CP-ABE: a revocable CP-ABE for post-quantum cryptography*. In: Journal of Mathematical Cryptology (JMC), De Gruyter 18.1 (Feb. 2024), pp. 20230026–32. ISSN: 1862-2984. DOI: 10.1515/jmc-2023-0026.
- [8] Maria Catrambone✉, Emiliano Cristiani, Cristiano Riminesi, Elia Onofri, and Luciano Pensabene Buemi. *Assessing the Combined Influence of Indoor Air Quality and Visitor Flow Toward Preventive Conservation at the Peggy Guggenheim Collection*. In: Atmosphere, MDPI AG 16.7 (July 2025), p. 860. ISSN: 2073-4433. DOI: 10.3390/atmos16070860.
- [9] Davide Moretti✉, Elia Onofri, and Emiliano Cristiani. *Detection of anomalous vehicular traffic and sensor failures using data clustering techniques*. In: International Journal of Data Science and Analytics (Aug. 2025). ISSN: 2364-4168. DOI: 10.1007/s41060-025-00869-x.
- [10] Elia Onofri✉ et al. *A general multi-stratum model for a nanofunctionalized releasing capsule: an experiment-driven computational study*. In: Mathematical Biosciences and Engineering (MBE), AIMS 23 (Nov. 2025), pp. 1–21. DOI: 10.3934/mbe.2026001.
- [11] Maurantonio Caprolu✉, Roberto Di Pietro, Flavio Lombardi, and Elia Onofri. *Toward Estimating Speculation in a Cryptocurrency Transaction Network: The Polkadot Case Study*. In: Computer Networks, Elsevier (Mar. 2026), p. 112166. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2026.112166.

- [12] Lorenzo Gasparini, Elia Onofri , Martina Palmucci, and Marco Pedicini. *Cross-primitive comparison in CP-ABE: Bilinear Pairing vs. Lattices*. In: Journal of Mathematical Cryptology (JMC), De Gruyter (Mar. 2026). DOI: 10.1515/jmc-2025-0051.
- [13] Enrico Mastrostefano  et al. *Granuloma-Like Structures in Tuberculosis: A Critical Review of Their Biology, Quantitative Behavior, and Translational Use*. In: FEMS Microbiology Reviews [To appear] (2026).

Conference Proceedings

- [14] Pietro Centorrino, Alessandro Corbetta, Emiliano Cristiani , and Elia Onofri. *Measurement and analysis of visitors' trajectories in crowded museums*. In: International Conference on Metrology for Archaeology and Cultural Heritage (IMEKO TC-4). IMEKO:2019-83. Florence, Italy: International Conference on Metrology for Archaeology and Cultural Heritage, Dec. 2019, pp. 423-428.
- [15] Flavio Lombardi and Elia Onofri . *Graph contraction on attribute-based coloring*. In: Procedia Computer Science, Elsevier 201 (Apr. 2022). The 13th International Conference on Ambient Systems, Networks and Technologies (ANT) / The 5th International Conference on Emerging Data and Industry 4.0 (EDI40), pp. 429-436. ISSN: 1877-0509. DOI: 10.1016/j.procs.2022.03.056.
- [16] Elia Onofri  and Alessandro Corbetta. *RSSi-based visitor tracking in museums via cascaded AI classifiers and coloured graph representations*. In: Collective Dynamics 6 (Jan. 2022), pp. 1-17. DOI: 10.17815/CD.2021.131.
- [17] Elia Onofri  and Marco Pedicini. *Novel notation on cube attack*. In: Collectio Cipharrum, De Cifris Cryptanalysis selected papers from the ITASEC2020 workshop (Mar. 2022). Ed. by Aracne, pp. 25-30. DOI: 10.53136/97912599486565.
- [18] Enrico Mastrostefano, Alessandro Ravoni , Elia Onofri, Paolo Tieri, and Filippo Castiglione. *Harnessing computational models to uncover the role of the immune system in tuberculosis treatment*. In: 2023 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). Dec. 2023, pp. 3725-3732. DOI: 10.1109/BIBM58861.2023.10385440.
- [19] Maurantonio Caprolu , Roberto Di Pietro, Flavio Lombardi, and Elia Onofri. *Characterizing Polkadot's Transactions Ecosystem: methodology, tools, and insights*. In: 2024 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS). July 2024. DOI: 10.1109/DAPPS61106.2024.00016.
- [20] Lorenzo Gasparini, Elia Onofri , Martina Palmucci, and Marco Pedicini. *Comparing Lattices and Bilinear Parings in CP-ABE*. In: FCIR25 Acta. Vol. 8. De Cifris Koine. De Cifris Press, Nov. 2025, pp. 81-87. ISBN: 979-12-81863-07-1. DOI: 10.69091/koine/vol-8-P10.
- [21] Elia Onofri , Sofia Bizzarro, Sandro Tassa, Michela Czech, and Gabriella Bretti. *StoneVerse: Models and Methods in Cultural Heritage. The Open-Science Platform for Reproducible Modelling of Stone Decay*. In: Digital Heritage. The Eurographics Association, Sept. 2025. DOI: 10.2312/DH.20253236.
- [22] Paola Stolfi, Elia Onofri , and Gabriella Bretti. *Estimating Cultural Heritage Processes Using Approximate Bayesian Computation*. In: Digital Heritage. Ed. by Stefano Campana et al. The Eurographics Association, 2025. ISBN: 978-3-03868-277-6. DOI: 10.2312/dh.20253258.
- [23] Maurantonio Caprolu , Elia Onofri, Omar Eldesouky, and Roberto Di Pietro. *Nominated Proof of Stake: A Reality Check*. In: 8th edition of the IEEE International Conference on Blockchain and Cryptocurrency. June 2026. DOI: 10.1109/ICBC67748.2026.11575543.
- [24] Emanuele Ricco, Elia Onofri , Lorenzo Cima, Stefano Cresci, and Roberto Di Pietro. *A Geometric Analysis of Small-sized Language Model Hallucinations*. In: Forty-Third International Conference on Machine Learning (ICML 2026) [To appear]. Submitted. arXiv:2602.14778. ICML. July 2026.
- [25] Elia Onofri , Andrea De Salve, Paolo Mori, Laura Emilia Maria Ricci, and Roberto Di Pietro. *COD-ssi: Enforcing Mutual Privacy for Credential Oblivious Disclosure in Self Sovereign Identity*. In: Computer Security - ESORICS 2026, 31st European Symposium on Research in Computer Security. Cham: Springer Nature Switzerland, 2027, pp. 212-232. DOI: 10.1007/978-3-032-38695-3_11.

Abstracts & Posters

- [26] Alessandro Corbetta , Emiliano Cristiani, Marina Minozzi, Elia Onofri, and Federico Toschi. *Optimizing museums' experience via trajectory analysis of visitors*. In: Proceedings of Traffic and Granular Flow 2019, Univ. de Navarra. Poster. July 2019. DOI: 10.13140/RG.2.2.33071.56489.
- [27] Marco Cianfriglia, Elia Onofri , and Marco Pedicini. *mR_{LWE}-CP-ABE: a revocable CP-ABE for post-quantum cryptography*. In: CIFRIS23 ACTA (14-15 dec 2023), De Cifris Press. Long abstract. Apr. 2024, pp. 1-2. ISBN: 979-12-81863-00-2. DOI: 10.69091/koine/vol-1-M14.
- [28] Alessandro Ravoni  et al. *Studying long-lasting diseases using an agent-based model of the immune response*. In: Book of Abstracts of the Fourth Edition of the Young Applied Mathematicians Conference. Long Abstract. Roma - ITA: CNR edizioni, Sept. 2024, pp. 120-122. ISBN: 978 88 8080 642 4. DOI: 10.48227/YAMC-2024.

- [29] Massimo Bernaschi, Gabriella Bretti, Pasqua D'Ambra, Elia Onofri , and Massimiliano Pedone. *AMELIA: A High-Performance Computing Infrastructure for Advanced Research*. In: Book of Abstracts of the Fifth Edition of the Young Applied Mathematicians Conference. Long Abstract (Poster). Roma – ITA: CNR edizioni, Sept. 2025, pp. 206–208. ISBN: 978 88 8080 779 7. DOI: 10.48227/YAMC-2025.
- [30] Elia Onofri  and Gabriella Bretti. *Modelling Percolation and Stone Decay in Cultural Heritage through StoneVerse*. In: Book of Abstracts of the Fifth Edition of the Young Applied Mathematicians Conference. Long Abstract. Roma – ITA: CNR edizioni, Sept. 2025, pp. 53–56. ISBN: 978 88 8080 779 7. DOI: 10.48227/YAMC-2025.

Other Contributions

- [31] Gianmaria Del Monte, Elia Onofri, Giorgio Scorzelli, and Alberto Paoluzzi . *Local congruence of chain complexes*. In: arXiv preprint (May 2020). arXiv:2004.00046.
- [32] Marco Cianfriglia, Elia Onofri , Silvia Onofri, and Marco Pedicini. *Ten years of cube attacks*. In: IACR eprints (Feb. 2022). ePrint:2022/137, pp. 1–30.
- [33] Pietro Centorrino, Emiliano Cristiani , Pietro Ferrara, Danilo Macchion, and Elia Onofri. *Measurement and analysis of the visitors behavior in the Peggy Guggenheim Collection*. Technical report. IAC-CNR, Feb. 2023, pp. 1–12.
- [34] Stefano Baraldo, Elia Onofri , and Marco Pedicini. *Three Points in a Row: Runs, Serve, and the Nulls That Mislead in Tennis*. In preparation. arXiv:2609.XXXX. 2026.

As Editor

- [35] Elia Onofri and Gennaro Auricchio, eds. *Book of Abstracts of the Fourth Edition of the Young Applied Mathematicians Conference*. IT: CNR Edizioni, Oct. 2024. ISBN: 9788880806424. DOI: 10.48227/YAMC-2024.
- [36] Elia Onofri, Caterina Millevoi, and Elena Bachini, eds. *Book of Abstracts of the Fifth Edition of the Young Applied Mathematicians Conference*. IT: CNR Edizioni, Nov. 2025. ISBN: 9788880807797. DOI: 10.48227/YAMC-2025.

Theses

- Elia Onofri. *About the resolution of algebraic systems over finite fields: Buchberger algorithm, Gröbner bases and computational complexities*. B.Sc. Thesis in Mathematics. Roma Tre University, Oct. 2018.
- Elia Onofri. *A Computational Investigation of the Cube Attack in General Finite Fields*. M.Sc. Thesis in Computational Sciences "cum Laude". Roma Tre University, Mar. 2020.
- Elia Onofri. *ML- and graph-based methods for data analysis and prediction: Applications in vehicular traffic, pedestrian dynamics, and computational biology*. Ph.D. Thesis in Mathematics "cum Laude". Roma Tre University, Oct. 2023. DOI: 10.13140/RG.2.2.32948.36489.

Under Review

- Elia Onofri . *On γ -Contraction and β -Contraction: A Unified Framework for Colour-Preserving Graph Reduction*. In: arXiv preprint (Jan. 2025). Submitted. arXiv:2404.12080.
- Emanuele Ricco, Elia Onofri , Lorenzo Cima, Stefano Cresci, and Roberto Di Pietro. *PRISM: Phase-enhanced Radial-based Image Signature Mapping framework for fingerprinting AI-generated images*. In: arXiv preprint (Sept. 2025). Submitted. arXiv:2509.15270.
- Gabriella Bretti, Maurizio Ceseri, Elia Onofri , and Matteo Paoluzzi. *Structural Identifiability and Comparative Calibration of Water Retention Curves for Imbibition in Porous Media*. In: arXiv preprint (Feb. 2026). Submitted. arXiv:2602.23932.
- Elia Onofri , Andrea Ciccotelli, and Roberto Di Pietro. *I-(OT)²: A Client-optimal Oblivious Transfer Protocol for IoT devices*. In: arXiv preprint (June 2026). Submitted. arXiv:2606.02344.
- Elia Onofri  and Roberto Di Pietro. *RAIM: Robust Aggregation of Inexpensive Models for Hallucination Detection*. In: arXiv preprint (2026). Submitted. arXiv:2609.39229.
- Alessandro Ravoni  et al. *Multiscale modelling of drug–host–pathogen interaction: quantifying drug and immune contributions to treatment response*. In: bioRxiv preprint (2026). Submitted. DOI: 10.64898/2026.08.30.744418.
- Alessandro Ravoni  et al. *Quantifying drug and immune contributions to treatment response using integrated PBPK-PKPD and agent-based modelling*. Submitted. 2026.

- Emanuele Ricco , Elia Onofri, Vincenzo Sammartino, and Roberto Di Pietro. *Consensus and Factual Dynamics in Large Populations of Interacting Language Models*. In: arXiv preprint (2026). Submitted. `arXiv:2609.39211`.
- Paola Stolfi, Elia Onofri , and Gabriella Bretti. *Bayesian methods for the identification of model parameters for water transport in porous media*. In: arXiv preprint (2026). Submitted. `arXiv:2603.29859`.

RESEARCH ACTIVITY

INVITED VISITINGS

January 2025		King Abdullah University of Science and Technology (KAUST), Saudi Arabia
May 2024		Scuola Normale Superiore (SNS), Pisa, Italy
April 2024		King Abdullah University of Science and Technology (KAUST), Saudi Arabia

PROJECTS PARTICIPATION

2024–2025		Humanities and cultural Heritage Italian Open Science Cloud (H2IOSC). NextGenerationEU – NRRP M4C2 – Project code IR0000029 – CUP B63C22000730005
2025		MODA: Integrating MODEL-based and DATA-Driven Methods for Multiscale Biological Systems. INdAM – GNCS, CUP E53C24001950001
2024		Numerical modeling and high-performance computing approaches for multiscale models of Complex Systems. INdAM – GNCS, CUP E53C23001670001
2021–2024		European Regimen Accelerator for Tuberculosis (ERA4TB). Grant Agreement n. 853989, H2020-JTI-IMI2-2018-15-two-stage

AWARDS

2024		Award CDE DTC Lazio 2024 – first edition first prize for the best P.h.D. thesis in “HUB 3: Technologies for resources design and management” category.
------	--	---

EDITORIAL CAREER

since July 2020		Review Editor Security, Privacy and Authentication – Frontiers in Communications and Networks.
since 2020		External reviewer (journals) • Transactions on Dependable and Secure Computing, IEEE (2026) • Frontiers In Communications And Networks, Frontiers (2026, 2025) • Journal of Mathematical Cryptology, De Gruyter (2026, 2025) • Pervasive and Mobile Computing, Elsevier (2025, 2024) • Journal on Computing and Cultural Heritage, ACM (2025) • Frontiers in Computer Science, Frontiers (2025) • Scientific Reports, Nature (2025) • Computer Communications, Elsevier (2024) • Journal of Security and Communication Networks, Hindawi (2022, 2021, 2020) • Frontiers in Immunology, Frontiers (2022)

since 2020

External reviewer (conferences)

- International Conference on Learning Representations (ICLR 2026)
- Young Applied Mathematicians Conference (YAMC 2026)
- IEEE Conference on Communications and Network Security (CNS 2026)
- Annual Conference on Neural Information Processing Systems (NeurIPS 2026)
- European Symposium on Research in Computer Security (ESORICS 2026)
- International Conference on Machine Learning (ICML 2026)
- Annual IEEE International Conference on Sensing, Communication, and Networking (SECON 2026)
- IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2026)
- IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGrid 2026)
- IEEE International Conference on Bioinformatics and Biomedicine (BIBM 2024)
- International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2024)
- International Conference on Ambient Systems, Networks and Technologies (ANT 2022, 2021)
- International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2021, 2020)

SCIENTIFIC AND ORGANISATION COMMITTEES

October 2025
current

Scientific Committee

Master in Data Analytics

Roma Tre University. WEBSITE: master-data-analytics.it 

3 December 2026
6 December 2026

PC Member

Workshop "Network Science and Artificial Intelligence for Biomedicine & Health informatics" (NET-AI-BHI), "IEEE Bioinformatics & Biomedicine Conference" (BIBM) (Ed. 5th)

Dallas, TX, USA WEBSITE: sites.google.com/unicz.it/net-ai-bhi-2026 

14 September 2026
18 September 2026

General Program Chair

Sixth Young Applied Mathematicians Conference (YAMC-2026)

Turin, Italy. WEBSITE: yamc.it 

15 December 2025
18 December 2025

PC Member

Workshop "Network Science and Artificial Intelligence for Biomedicine & Health informatics" (NET-AI-BHI), "IEEE Bioinformatics & Biomedicine Conference" (BIBM) (Ed. 4th)

Wuhan, China

22 September 2025
26 September 2025

Program & Organising Committee

Fifth Young Applied Mathematicians Conference (YAMC-2025)

Padua, Italy. WEBSITE: sites.google.com/view/yamc2025 

February 2025
March 2025

Organiser

Kitware Visualization Toolkit (VTK), 30 hours

Course organised at IAC-CNR as part of the H2IOSC project

22 September 2025
26 September 2025

Scientific Committee

IXH24 – Italian XRPL Hackathon 2024

Parallel session for secondary schools

Rome, Italy. WEBSITE: decifris.it/ixh24 

3 December 2024
6 December 2024

PC Member

Workshop "Network Science and Artificial Intelligence for Biomedicine & Health informatics" (NET-AI-BHI), "IEEE Bioinformatics & Biomedicine Conference" (BIBM) (Ed. 3rd)

Lisbon, Portugal

16 September 2024
20 September 2024

Program & Organising Committee

Fourth Young Applied Mathematicians Conference (YAMC-2024)

Rome, Italy. WEBSITE: sites.google.com/view/yamc2024 

2022
2024

Program & Organising Committee

Tè di Matematica

Seminar cycle [ITA]

Roma Tre University. WEBSITE: ricerca.mat.uniroma3.it/seminari/te_di_matematica 

2022 2024	Program & Organising Committee <i>Junior Seminars</i> An official Ph.D. students seminar cycle Roma Tre University. WEBSITE: ricerca.mat.uniroma3.it/seminari/junior_seminars 
2021 2022	Program & Organising Committee <i>General Topics in Mathematics (GTM)</i> An unofficial Ph.D. students seminar cycle Roma Tre University. WEBSITE: sites.google.com/view/gtm-r3 
22 March 2022 25 March 2022	PC member (Systems Security and Privacy) <i>13th International Conference on Ambient Systems, Networks and Technologies (ANT)</i> Porto, Portugal. WEBSITE: cs-conferences.acadiau.ca/ant-22 
23 March 2021 26 March 2021	PC member (Systems Security and Privacy) <i>12th International Conference on Ambient Systems, Networks and Technologies (ANT)</i> Warsaw, Poland. WEBSITE: cs-conferences.acadiau.ca/ant-21 
1 November 2021 4 November 2021	PC member (Security, Privacy, and Trust) <i>12th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN)</i> Leuven, Belgium. WEBSITE: cs-conferences.acadiau.ca/euspn-21 
2 November 2020 5 November 2020	PC member (Security, Privacy, and Trust) <i>11th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN)</i> Madeira, Portugal. WEBSITE: cs-conferences.acadiau.ca/euspn-20 

INVITED LESSONS AND SPEECHES

9 July 2026	A Geometric Analysis of Small-sized Language Model Hallucinations, ICML'26 (Seoul, South Korea)
14 May 2026	Git. A 40-minute primer for researchers, CRI-Lab (KAUST, Saudi Arabia)
22 April 2026	Quantum & Post-Quantum Cryptography, Invited Talk @ CRI-Lab Quantum Masterclass (KAUST, Saudi Arabia)
14 April 2026	I(OT) ² , Invited Lesson @ Applied Cryptography Course (KAUST, Saudi Arabia)
6 October 2025	Mathematical Modelling of Imbibition in Porous Media: From Diffusion Equations to the StoneVerse Platform, Math4cult2025 (IAC, Rome, Italy)
25 September 2025	Modelling Percolation and Stone Decay in Cultural Heritage through StoneVerse, YAMC 25 (Padua, Italy)
22 September 2025	AMELIA: A High-Performance Computing Infrastructure for Advanced Research (Poster), YAMC 25 (Padua, Italy)
10 September 2025	StoneVerse: The Open-Science Platform for Reproducible Modelling of Stone Decay, Digital Heritage 25 (Siena, Italy)
25 February 2025	Models and Methods in Cultural Heritage: The Open-Science StoneVerse Platform, Giornate IAC AdR 7 (CNR, Rome, Italy)
17 February 2025	mRLWE-CP-ABE: a Recoverable CP-ABE Protocol for Post-Quantum Cryptography, Graduate Seminar CEMSE (KAUST, Saudi Arabia)
14 February 2025	Adversarial Examples in Machine Learning: Taxonomy and Insights, CySec Group Meeting TGIT (KAUST, Saudi Arabia)
21 January 2025	On the Modelling of Granuloma-Like Structures: An Overview from In-Vitro to In-Silico Modelling, MDN Winter Semester (Sapienza University of Rome, Italy)
2 December 2024	Introduction to Python: a discussion on advantages and criticalities (IN490 course invited talk, Roma Tre University)

6 May 2024	Managing pedestrian flows in crowded museums: a mathematical perspective from data gathering to optimisation (PYSANUM: Pisan Young Seminars in Applied and Numerical Mathematics, SNS, Pisa, Italy)
18 April 2024	β -contraction: a Framework for Contracting Coloured Networks. Use Cases and Applications (KAUST, Saudi Arabia)
15 April 2024	A gentle introduction to Fully Homomorphic Encryption (Applied Cryptography invited lesson, KAUST, Saudi Arabia)
1 February 2024	Multi-scale and ML-aided models for vehicular traffic (Heterogeneity on the Road, Padua University)
15 December 2023	mRLWE-CP-ABE: a revocable CP-ABE for post-quantum cryptography (Cifris'23, Consob, Rome)
19 September 2023	Managing crowded museums (YAMC-2023, Siena University)
18 September 2023	A gentle introduction to clustering (Mini-course, YAMC-2023, Siena University)
10 May 2023	How machine learning can improve macroscopic models for traffic state estimation and forecast (Junior Seminars, Roma Tre University)
13 April 2023	Validate <i>in silico</i> modelling of GLS (ERA4TB Workshop, Rome)
20 December 2022	A brief introduction to Multi-threading and Multi-processing: Pthreads, OpenMP and MPI (IN490 course invited talk, Roma Tre University)
25 October 2022	In-Silico Granulomas: preliminary results (ERA4TB, IDMIT, Paris)
21 September 2022	AI for Traffic Data Analysis (YAMC-2022, Arenzano)
20 September 2022	Basics in Traffic Modelling (Mini-course, YAMC-2022, Arenzano)
8 July 2022	A brief introduction on Differential Privacy (DBU Smol Talks, IAC-CNR, Rome)
28 February 2022	On tweakable black-box polynomials: the cube attacks family (GTM seminars, Roma Tre University)
24 January 2022	Attribute-based colouring and its applications in reducing problem's size (GTM seminars, Roma Tre Univ.)
14 December 2021	A brief introduction to Multi-threading and Multi-processing: Julia Parallel Computing (IN490 course invited talk, Roma Tre University)
13 December 2021	The role of the applied mathematician: optimise pedestrian flows in crowded museums (GTM seminars, Roma Tre University)
7 December 2021	A brief introduction to Multi-threading and Multi-processing: Pthreads, OpenMP and MPI (IN490 course invited talk, Roma Tre University)
29 November 2021	RSSi-based visitor tacking in museums via cascaded AI classifiers, (PED21, online)
25 November 2021	On real-world implementation of RSA cryptosystem: HandsOn (CR410 course invited talk, Roma Tre Univ.)
18 November 2021	On real-world implementation of RSA cryptosystem: Theory (CR410 course invited talk, Roma Tre University)
14 May 2021	Macroscopic vehicular traffic simulations and linear programming problems (IN440 course invited talk, Roma Tre University)
1 July 2021	About Existence of Adversarial Examples in Neural Network Classification problems with Small Hamming Distance (GTM seminars, Roma Tre University)
10 December 2020	ML-based Algorithms and Models for Analysing Heterogeneous Data (Young researchers day, IAC-CNR).
23 May 2019	Snowden Backdoor. https://matematicafisica.uniroma3.it/articoli/pre-snowden-backdoor-298/
29 April 2019	A brief description about Proof Nets: the bridge between Modern Logic and Computer Science.
18 January 2019	A brief presentation about Hamilton's Ideals.

ACADEMIC COMPETITIONS

10 May 2019	MOR19 Team (R. Musto, E. Onofri, E. Rocchi) <i>Catch the Mark 2019</i> First classified
15 December 2018	ACOP18 Team (L. Andrianaivo, P. Collagè, E. Onofri, M. Parsi) <i>Cryptowars 2018</i> Fourth classified in both sections (Theoretic/Applied Cryptography)

CONFERENCE ATTENDANCE (AS SPEAKER)

14 September 2026 18 September 2026	<i>Thirty-first European Symposium on Research in Computer Security (ESORICS 2026)</i> Rome, Italy
6 July 2026 11 July 2026	<i>Forty-Third International Conference on Machine Learning (ICML'26)</i> Seoul, South Korea
6 October 2025 8 October 2025	<i>Mathematical tools for Cultural Heritage (Math4cult2025)</i> Rome, Italy
22 September 2025 26 September 2025	<i>Fifth Young Applied Mathematicians Conference</i> Padua, Italy
8 September 2025 13 September 2025	<i>Digital Heritage '25</i> Siena, Italy
24 February 2025 25 February 2025	<i>IAC Days '25</i> Rome, Italy
16 September 2024 20 September 2024	<i>Fourth Young Applied Mathematicians Conference</i> Rome, Italy
1 February 2024 2 February 2024	<i>Heterogeneity on the Road</i> Padua, Italy
14 December 2023 15 December 2023	<i>1st congress of the Italian association of cryptography (Cifris23)</i> Rome, Italy
18 September 2023 22 September 2023	<i>Third Young Applied Mathematicians Conference</i> Siena, Italy
12 April 2022 14 April 2022	<i>Host immune system-pathogen interactions: Challenges and Opportunities (ERA4TB-WP5 workshop)</i> Rome, Italy.
18 September 2022 22 September 2022	<i>Second Young Applied Mathematicians Conference</i> Arenzano (Genoa), Italy
26 April 2022 28 April 2022	<i>Modelling of drug-disease-host interactions and prediction of antibacterial activity of drug combinations in humans (ERA4TB-WP5 workshop)</i> Rome, Italy
29 November 2021 30 November 2021	<i>Pedestrian and Evacuation Dynamics Conference 2021</i> Melbourne, Australia (online)

FUNDING AND GRANTS

2024	INdAM-GNCS Grant No. E53C23001670001 for Organising Workshops, Schools, and Conferences
------	---

STUDENTS

current	Master Degree in Computational Sciences (LM-40) <i>Simone Maione</i> TbD Internal supervisor: Flavio Lombardi
current	Master Degree in Computational Sciences (LM-40) <i>Michela Rossi</i> TbD Internal supervisor: Flavio Lombardi
current	Master Degree in Mathematics (LM-40) <i>Davide Sabatini</i> TbD
7 March 2025	Master Degree in Computational Sciences (LM-40) <i>Vallifuoco Augusta Gioia</i> Estensione di uno Schema KP-ABE basato su Reticoli: Implementazione e Analisi del Meccanismo di Revoca
13 January 2025	Master Degree in Computational Sciences (LM-40) <i>Serena Massarone</i> A Systematic Analysis of Scale-Free Effects on Coloured Graph Contraction
25 January 2024	Master Degree in Computational Sciences (LM-40) <i>Davide Moretti</i> About clustering of time series – A case study with traffic data by Autostrade Alto Adriatico S.p.A. Internal supervisor: Vincenzo Bonifaci
19 October 2023	Master Degree in Computational Sciences (LM-40) <i>Francesca Bacco</i> Investigating Coloured Graph Contraction for Analyzing Large Graphs Internal supervisor: Flavio Lombardi
13 July 2023	Laurea Triennale in Matematica (L-35) <i>Valerio Ardizio</i> Sugli schemi di <i>Secret Sharing</i> Internal supervisor: Francesca Merola
26 October 2022	Master Degree in Computational Sciences (LM-40) <i>Francesca Giulianelli</i> Homomorphic Encryption: an application to Linear Regression Internal supervisor: Marco Pedicini

AFFILIATIONS

October 2024 current	Researcher <i>IAC-CNR node of the CINI national laboratory on HPC</i>
March 2023 current	Young member <i>Italian assoc. “De Componendis Cifris” (DeCifris)</i>
August 2022 current	Adjunct member <i>Italian assoc. “Gruppo di Informatica” (GrIn)</i>
May 2013 current	Coordinator of the SIG Intellect Research (Ricerca sull’Intelligenza) <i>Mensa Italy</i>

January 2022	Affiliate
December 2025	<i>National Group for Scientific Computing, Istituto Nazionale di Alta Matematica “Francesco Severi”, (INdAM – GNCS)</i>
January 2021	Student member
December 2025	<i>International Association for Cryptologic Research (IACR)</i>
May 2021	Associate researcher
October 2023	<i>Institute for applied mathematics “M. Picone”, National Research Council (IAC–CNR)</i>

I authorise the processing of the personal data contained in this CV under Regulation (EU) 2016/679 (GDPR) and Italian Legislative Decree 196/2003.

October 12th 2026, Thuwal

Elia Onofri
Signature