CURRICULUM VITAE ET STUDIORUM
of Riccardo Aragona

Personal Informations

Born in Rome (Italy) on September 18, 1980;
Address: via Siro Corti 53, 00135 Roma, Italy.

Telephone number : +39 0862434723
E-mail : *riccardo.aragona@univaq.it*

Education

- June 2009: Ph.D. in Mathematics at University of Rome "Tor Vergata",
  Title of thesis: *"Semi-invariants of Symmetric Quivers"*, arXiv: 1006.4378v1 [math.RT]
  Advisors: Professor Jerzy Weyman (Northeastern University of Boston) and Professor Elisabetta Strickland (University of Rome "Tor Vergata").
- February 2005: Master Degree in Mathematics at "Sapienza" University of Rome
  Title of thesis: *"Su certi automorfismi di gruppi"* (i.e. "On certain group automorphisms"),
  Advisor: Professor Marialuisa J. de Resmini ("Sapienza" University of Rome).
- July 1999: Diploma di Maturità Classica at Liceo Ginnasio Statale "Terenzio Mamiani" (Rome, Italy).

Positions at University and Scientific Qualification

- Since November 2022: Associate Professor (SSD MAT/02) at the Department of Information Engineering, Computer Science and Mathematics of University of L'Aquila.
- November 2019 - October 2022: Assistant Professor (RTDB , SSD MAT/02) at the Department of Information Engineering, Computer Science and Mathematics of University of L'Aquila.
- Since September 2018: Scientific National Qualification for associate professor.
- February 2018 - October 2019: Assistant Professor (RTDA, SSD MAT/02) at the Department of Information Engineering, Computer Science and Mathematics of University of L'Aquila.
- March 2017 - January 2018: post-doc fellowship "Applications of Group Theory to symmetric cryptography" (SSD MAT/02) at University of Trento (Italy), cofunded by the Department of Information Engineering, Computer Science and Mathematics of University of L'Aquila, within the Project of National Interest PRIN 2015.
- March 2017: Research Contract to manage and organize the advanced academic course "Post-quantum Cryptography" for PhD students and Companies, at University of Trento (Italy).
- February 2017 - December 2021: French scientific qualification for Maître de Conférences in "Applied Mathematics and Applications of Mathematics" (qualification n° 17226304192).
- February 2017 - December 2021: French scientific qualification for Maître de Conférences in "Mathematics" (qualification n° 17225304192).
- January 2013 - January 2017: post-doc fellowship "Encoding for Advanced Electronic Payment" (SSD MAT/02) at University of Trento (Italy).
- February 2011 - January 2012: post-doc fellowship "Transformation Groups and Applications" (SSD MAT/02) at "Sapienza" University of Rome (Italy).
- January-February 2010: visiting position at Northeastern University of Boston MA (USA) invited by Professor Jerzy Weyman.
- October-December 2008: visiting position at Northeastern University of Boston MA (USA) invited by Professor Jerzy Weyman.
- October-December 2007: visiting position at Northeastern University of Boston MA (USA) invited by Professor Jerzy Weyman.

Teaching experience

- Since November 2019: Tutor of the following PhD students of the Doctorate school "Mathematics and Models", University of L'Aquila:
  - Margherita Paolini (XXXV cycle, SSD MAT/02, topic: Representation Theory, Thesis Defense: July 2023);
  - Jessica Alessandrì (XXXVI cycle, SSD MAT/02, topic: Elliptic curves);
  - Ginevra Giordani (XXXVIII cycle, SSD MAT/02, topic: Polynomial Identities);
- Since November 2020: Advisor of the following PhD student of the Doctorate school "Mathematics and Models", University of L'Aquila:
  - Lorenzo Campioni (XXXVI cycle, SSD MAT/02, topic: Combinatorics);
  - Giuseppe Nozzi (XXXVIII cycle, SSD MAT/02, topic: Group Theory).
- Since February 2013: I supervised as first advisor and second advisor the following MSc and BSc Theses:
  - 17 MSc theses in Mathematics, Information and Automation Engineering and Mathematical Engineering.
    1. Daniel Pinter (University of Trento), *Cryptographic applications of number theory to online banking*, advisor: Prof. Massimiliano Sala.
    2. Francesco Aldà (University of Trento), *The Partial Sum Attack on 6-round reduced AES: Implementation and improvement*, advisor: Prof. Massimiliano Sala.
    3. Beatrice Ridolfi (University of Trento), *Cryptanalysis of Bluetooth stream cipher*, advisor: Prof. Massimiliano Sala.
    4. Simona Dimase (University of Trento), *Cryptanalysis of GSM stream ciphers*, advisor: Prof. Massimiliano Sala.
    5. Cecilia Boschini (University of Trento), *NTWO: a post quantum cipher*, advisor: Prof. Massimiliano Sala.
    6. Aaron Gaio, *Some Teaching Experience in Computational Algebra*, advisor: Prof. Massimiliano Sala.
    7. Federico Giacon (University of Padova), *Revising RS-ABE, an encryption scheme for user revocation and attribute-based access*, advisors: Prof. Massimiliano Sala (University of Trento) and Prof. Alberto Tonolo (University of Padova).
    8. Marco Iavernaro (University of Trento), *On some Cryptographic Properties of Vectorial Boolean Functions*, advisor: Prof. Massimiliano Sala.
    9. Patrick Harasser (University of Trento - University of Tübingen), *Cover Attacks on Hyperelliptic Curve Cryptography*, advisors: Prof. Massimiliano Sala (University of Trento) and Prof. Jürgen Hausen (University of Tübingen).
    10. Pasqua Valentina Mauri (University of Trento), *PKI and IBE: authentication method and algebraic background*, advisor: Prof. Massimiliano Sala.
    11. Andrea Zanini (University of Trento), *On Message Authentication Codes and related mathematical problems*, advisor: Prof. Massimiliano Sala.
    12. Ilaria Zappatore (University di Trento), *Primitivity of generalized translation based block ciphers*, advisor: Prof. Massimiliano Sala.
    13. Sara Manni (University di Trento), *Symmetric Authentication Methods for Entities: a Proof of Security for nKerberos*, advisor: Prof. Massimiliano Sala.
    14. Giuseppe Vitto (University di Trento), *The General Number Field Sieve*, advisor: Prof. Massimiliano Sala.
    15. Nicolò Fornari (University di Trento), *Cryptography in the White-Box attack model: some constructions and attacks*, advisor: Prof. Massimiliano Sala.
    16. Marco Carolla (University of L'Aquila), *On a post-quantum SIDH-based Oblivious Transfer and its implementation*, advisor: Dr. R. Aragona, co-advisor: Dr. Federico Pintore (University of Oxford).
    17. Tunmbi Olayemi Okediran (University of L'Aquila/Brno University of Technology), *Type-preserving Matrices and Block Cipher Security*, advisor: Dr. R. Aragona.
  - 6 BSc theses in Mathematics:

1. Ilaria Zilio (University of Trento), *Polynomials on Finite Fields*, advisor: Prof. Massimiliano Sala.
2. Lorenzo Di Lisio (University of L'Aquila), *Curve ellittiche e applicazioni crittografiche*, advisor: Dr. Riccardo Aragona.
3. Michela Ettorre (University of L'Aquila), *Aspetti algebrici e sicurezza crittografica di un algoritmo di tokenizzazione*, advisor: Dr. Riccardo Aragona.
4. Andrea Orsini (University of L'Aquila), *Curve ellittiche e crittografia*, advisor: Dr. Riccardo Aragona.
5. Francesco Di Loreto (University of L'Aquila), *Crittografia multilineare con gruppi nilpotenti*, advisor: Dr. Riccardo Aragona.
6. Settimio Marcello Reyes Felli (University of L'Aquila), *Automorfismi di Coleman di gruppi finiti con 2-sottogruppi di Sylow semidiedrali*, advisor Prof. Riccardo Aragona.

– 1 BSc theses in Computer Science:

7. Lorenzo Camaione (University of L'Aquila), *Monero - Privacy e anonimato sulla blockchain*, advisor: Prof. F. Mignosi.

- March-June 2023: Algebra for Cryptography (60 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for BSc in Mathematics.
- March-June: Algebra for Cryptanalysis (60 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for MSc in Mathematics.
- November-December 2023: Topics in Algebra (30 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for MSc in Mathematics.
- April-June 2023: Algebra for Cryptography (30 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the following Bachelor's degrees and Master's Degrees: BSc in Mathematics and MSc in Mathematics.
- April-June 2023: Advanced Algebra (30 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for MSc in Mathematics.
- February-April 2023: Algebra (60 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for BSc in Mathematics.
- April-June 2022: Cryptography and Coding Theory (30 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the following Master's Degrees: MSc in Mathematical Engineering, MSc in Information and Automation Engineering, MSc in Telecommunications Engineering.
- March 2022: Algebra (9 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the BSc in Mathematics.
- March-June 2022: Algebra for Cryptography (60 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the following Bachelor's degrees and Master's Degrees: BSc in Mathematics, MSc in Mathematical Engineering, MSc in Information and Automation Engineering, MSc in Telecommunications Engineering.
- September 2021: Linear Algebra Foundations (18 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the Pre-Master's Foundation in Applied Mathematics.
- March-June 2021: Algebra (30 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the BSc in Mathematics.
- March-June 2021: Combinatorics and Cryptography (60 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the following Bachelor's degrees and Master's Degrees: BSc in Mathematics, MSc in Mathematical Engineering, MSc in Information and Automation Engineering, MSc in Telecommunications Engineering.
- February-June 2020: Combinatorics and Cryptography (60 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the following Bachelor's degrees and Master's Degrees: BSc in Mathematics, MSc in Mathematical Engineering, MSc in Information and Automation Engineering, MSc in Telecommunications Engineering.
- February-June 2019: Advanced Algebra (4 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the following Master's Degree in Mathematics.

- February-June 2019: Combinatorics and Cryptography (60 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the following Bachelor's degrees and Master's Degrees: BSc in Mathematics, MSc in Mathematical Engineering, Msc in Information and Automation Engineering, MSc in Telecommunications engineering.
- February-June 2018: Algebra (60 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila, for the BSc in Mathematics.
- September-December 2016: I gave some research talks for the students of the course *Advanced Coding Theory and Cryptography* (4 hours) of the MSc degree in Mathematics at the University of Trento.
- October 2016: Lecturer during the course *Advanced Analysis of Block Ciphers* (16 hours) organized by *Laboratorio di Matematica Industriale e Crittografia* at University of Trento (17 - 21 October 2016).
- May 2016: Lecturer during the mini workshop *Bitcoin, Blockchain and their new frontiers* (4 hours) organized by *Laboratorio di Matematica Industriale e Crittografia* at University of Trento (12 - 13 May 2016).
- September-December 2015: I gave some research talks for the students of the course *Advanced Coding Theory and Cryptography* (4 hours) of the MSc degree in Mathematics at the University of Trento.
- September 2015: Lecturer during the course *Trapdoors nei Block Cipher* (16 hours), organized by *Laboratorio di Matematica Industriale e Crittografia* at University of Trento (21 - 25 September 2015).
- September-December 2014: Teaching assistant for *Algebraic Cryptography* (30 hours) at University of Trento (Italy).
- May 2014: I gave some lectures during the course *Laboratorio Didattico* (12 hours) of the BSc degree in Mathematics at the University of Trento.
- October-December 2013: Teaching assistant for *Cryptography* (30 hours) at University of Trento.
- September 2013: Lecturer during the course *Debolezza dei cifrari a blocchi: attacchi recenti e contromisure* (16 hours), organized by *Laboratorio di Matematica Industriale e Crittografia* at University of Trento (9 - 13 September 2013).
- June 2013: I hold a lecture about *Generatori Deterministici di Bit Random* (8 hours) during the course *Sorgenti di Randomicità in Crittografia e Crittoanalisi: Specifiche e Criticità*, organized by *Laboratorio di Matematica Industriale e Crittografia* at University of Trento (3 - 7 Giugno 2013).
- April-May 2013: I gave some lectures during the course *Laboratorio Didattico* (12 hours) of the BSc degree in Mathematics at the University of Trento.
- March-April 2013: Lecturer during the laboratorial part of the course *Computational Algebra* (10 hours) of the MSc degree in Mathematics at the University of Trento.
- September 2012: Teaching contract. *Precorsi di Matematica* (30 hours) at Faculty of Ingineering of "Sapienza" University of Rome.

PhD courses held

- January 2020: PhD course "Group theoretical approach for symmetric encryption" (SSD MAT/02, 10 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila.
- January 2019: PhD course "Permutation Groups and Applications to Cryptography" (SSD MAT/02, 10 hours) at the Department of Information Engineering, Computer Science and Mathematics of the University of L'Aquila.
- March 2017: Lecturer during the PhD course "Post-Quantum Cryptography" (8 hours) at University of Trento (13 - 17 March 2017).

Research interests

Currently I am dealing with Group Theory and some aspects of Algebraic Cryptography, focusing on the application of Group Theory and Number Theory to Symmetric Cryptography.
Since my PhD I have been interested in the following research topics:

- Permutation group methods for block cipher security [4,9,13,16,17,19,20,22,23,27,35].
- Theoretical and combinatorial aspects of Permutation groups [8,11,10,15].

- Theoretical and combinatorial aspects of Lie algebras [3,32].
- Combinatorial aspects of Integer Partitions [5,7,33].
- Representations of finte-dimensional algebras [29,30,31].
- Group Theory and Semigroup Theory [2,12,28].
- Other aspects of Algebraic Cryptography and Information Theory [6,14,18,21,24,25,26,34,36].

Industrial research and research project management

Within the *Laboratorio di Matematica Industriale e Crittografia* of the Department of Mathematics of the University of Trento, whose head is Prof. Massimiliano Sala, I followed some research projects founded by private companies:

- Asymmetric Cryptography, in particular about weak RSA keys, for *Telsy* (Senior Researcher).
- Evaluation of security of some practical encryption systems, for *SGS - Banco Popolare* (Senior Researcher and Project Manager).
- Security aspects in the project "TITAN, un nuovo sistema avanzato di e-payment", for *Poste Italiane* and PayBay Networks (Senior Researcher).
- Evaluation of the optimal lenght of RSA keys using by Certification Authority, for *Consorzio BANCOMAT* (Senior Researcher and Project Manager). From this project we wrote the scientific paper [24].
- Designing of an End-to-End Encryption system, for *Poste Italiane* (Senior Researcher and Project Manager).
- Designing of a Tokenization algorithm and proof of its security, for *TAS Group* (Senior Researcher and Project Manager). From this project we wrote the scientific paper [18].

Publications

1. R. Aragona, R. Civino, N. Gavioli, *A definitely periodic chain in the integral Lie ring of partitions*, Journal of Algebraic Combinatorics, Online First (2024).
2. R. Aragona, *A note to Coleman automorphisms of finite groups with semidihedral Sylow 2-subgroups*, Acta Mathematica Hungarica, 172(2), 2024.
3. R. Aragona, R. Civino, N. Gavioli, *A modular idealizer chain and unrefinability of partitions with repeated parts*, Israel Journal of Mathematics, Online First, (2023).
4. R. Aragona, R. Civino, F. Dalla Volta,*On the primitivity of the AES-128 key-schedule*, Journal of Algebra and its Applications, 22(11) 2350233 (2023), [18 pages].
5. R. Aragona, R. Civino, L. Campioni, M. Lauria, *Verification and generation of unrefinable partitions*, Information Processing Letters, 181, 106361 (2023).
6. R. Aragona, R. Civino, N. Gavioli, M. Pugliese, *An Authenticated Key Scheme over Elliptic Curves for Topological Networks*, Journal of Discrete Mathematical Sciences and Cryptography, 25(8), 2429-2448 (2022).
7. R. Aragona, R. Civino, L. Campioni, M. Lauria, *On the maximal part in unrefinable partitions of triangular numbers*, Aequationes Mathematicae, 96, 1339-1363 (2022).
8. R. Aragona, R. Civino, N. Gavioli, C. M. Scoppola, *Unrefinable partitions into distinct parts in a normalizer chain*, Discrete Mathematics Letters, 8, 72-77 (2022).
9. R. Aragona, R. Civino, *On invariant subspaces in the Lai-Massey scheme and a primitivity reduction*, Mediterranean Journal of Mathematics, 18(4), 165 (2021).
10. R. Aragona, R. Civino, N. Gavioli, C. M. Scoppola, *Rigid commutators and a normalizer chain*, Monatshefte für Mathematik, 196(3), 431-455 (2021).
11. R. Aragona, R. Civino, N. Gavioli, C. M. Scoppola, *A chain of normalizers in the sylow 2-subgroups of the symmetric group on 2^n letters*, Indian Journal of Pure and Applied Mathematics, 52(3), 735-746 (2021)
12. R. Aragona, A. D'Andrea, *Normal form in Hecke-Kiselman monoids associated with simple oriented graphs*, Algebra and Discrete Mathematics 30(2), 161-171 (2020).
13. R. Aragona, M. Calderini, R. Civino, *Some group-theoretical results on Feistel Networks in a long-key scenario*, Advances in Mathematics of Communications 14(4), 727-743 (2020).

14. R. Aragona, F. Marzi, F. Mignosi, M. Spezialetti, *Entropy and Compression: A Simple Proof of an Inequality of Khinchin-Ornstein-Shields*, Problems of Information Transmission, 56(1), 13-22 (2020).
15. R. Aragona, R. Civino, N. Gavioli, C. M. Scoppola, *Regular subgroups with large intersection*, Annali di Matematica Pura ed Applicata, 198(6), 2043-2057 (2019).
16. R. Aragona, A. Meneghetti, *Type-Preserving Matrices and Security of Block Ciphers*, Advances in Mathematics of Communications 13(2), 235-251(2019).
17. R. Aragona, M. Calderini, R. Civino, M. Sala, I. Zappatore, *Wave-Shaped Round Functions and Primitive Groups*, Advances in Mathematics of Communications, 13(1), 67-88 (2019).
18. R. Aragona, F. Giacon, M. Sala, *A proof of security for a key-policy RS-ABE scheme*, JP Journal of Algebra, Number Theory and Applications 40(1), 29-90 (2018).
19. R. Aragona, A. Rimoldi, M. Sala, *A note on an infeasible linearization of some block ciphers*, Journal of Discrete Mathematical Sciences and Cryptography 21(1), pp. 209-218 (2018).
20. R. Aragona, M. Calderini, A. Tortora, M. Tota, *Primitivity of PRESENT and other lightweight ciphers*, Journal of Algebra and Its Applications 17(6), 1850115 (2018), [16 pages].
21. R. Aragona, R. Longo, M. Sala, *Several Proofs of Security for a Tokenization Algorithm*, Applicable Algebra in Engineering, Communication and Computing 28(5), pp. 425-436 (2017).
22. R. Aragona, A. Caranti, M. Sala, *The group generated by the round functions of a GOST-like cipher*, Annali di Matematica Pura ed Applicata 196(1), pp. 1-17 (2017).
23. M. Calderini, D. Maccauro, R. Aragona, M. Sala, *On weak differential uniformity of vectorial Boolean functions as a cryptographic criterion*, Applicable Algebra in Engineering, Communication and Computing 27(5), pp. 359-372 (2016).
24. R. Aragona, F. Gozzini, M. Sala, *A real life project in Cryptography: assessment of RSA keys*, in Springer LNEE, Vol. 358, pp. 197-203, (2015).
25. F. Aldà, R. Aragona, L. Nicolodi, M. Sala, *Implementation and improvement of the Partial Sum Attack on 6-round AES*, in Springer LNEE, Vol. 358, pp. 181-195, (2015).
Cryptology ePrint Archive: `https://eprint.iacr.org/2014/216`.
26. F. Marinelli, R. Aragona, C. Marcolla , M. Sala, *Some security bounds for the key sizes of DGHV scheme*, Applicable Algebra in Engineering, Communication and Computing 25(5), pp. 383-392 (2014).
27. R. Aragona, A. Caranti, F. Dalla Volta, M. Sala, *On the group generated by the round functions of translation based ciphers over arbitrary finite fields*, Finite Fields and Their Applications 25, pp. 293-305 (2014).
28. R. Aragona, A. D'Andrea, *Hecke-Kiselman Monoids of Small Cardinality*, Semigroup Forum 86(1), pp. 32-40 (2013).
29. R. Aragona, *Semi-invariants of Symmetric Quivers of Finite Type*, Algebras and Representation Theory 16(4), pp. 1051-1083 (2013).
30. R. Aragona, *Semi-invariants of Symmetric Quivers of Tame Type*, Algebras and Representation Theory 15(6), pp. 1215-1260 (2012).
31. R. Aragona, *Semi-invarianti di quiver simmetrici*, nota relativa all'argomento della tesi di dottorato, *Bollettino dell'Unione Matematica Italiana. Sez. A: La Matematica nella Società e nella Cultura*, Serie I Vol. III N. 1 (Aprile 2010), pp. 11-14.

Submitted papers

32. R. Aragona, G. Nozzi, *A classification of $\mathbb{F}_{p^k}$-braces using bilinear forms*, submitted to Annali di Matematica Pura e Applicata, 2024.
33. R. Aragona, R. Civino, L. Campioni, *The number of maximal unrefinable partitions*, submitted to Annali di Matematica Pura e Applicata, 2023.

Proceedings

34. P. J. Aswin, K. Jain, R. Aragona, *Performance Comparison of Hybrid Encryption Models*, Proceedings of the 2023 2nd International Conference on Augmented Intelligence and Sustainable Systems, ICAISS 2023, 1196–1203 (2023).
35. R. Aragona, M. Calderini, M. Sala, *An algebraic trapdoor for block ciphers*, extended abstract, Atti Preliminari del XX Congresso dell'Unione Matematica Italiana, p. 396 (2015).

36. F. Marinelli, R. Aragona, C. Marcolla, M. Sala, *Some security bounds for the DGHV scheme*, extended abstract, Book of Abstract YACC 2014, pp. 77-81 (2014).

Work in progress

- R. Aragona, M. Calderini, R. Civino, A. Visconti, *A Lightweight Cipher with Wave-Shaped Round Functions*, in preparation, 2018.

Preprints

- R. Aragona, M. Calderini, M. Sala, *The role of Boolean functions in hiding sums as trapdoors for some block ciphers*, preprint, 2014.
  arXiv: `http://arxiv.org/pdf/1411.7681.pdf`

Science communication articles

- R. Aragona, *Crittografia: gli opposti che si attraggono*, Maddmaths! Matematica Divulgazione Didattica (2019).
  `http://maddmaths.simai.eu/divulgazione/crittografia/`
- A. Lemmo, R. Aragona, *I giocattoli e la scienza: un percorso alla scoperta della luce e non solo*, Resoconto Festival della Luce 2015, Bondeno (FE) 23 - 25 Ottobre 2015.
- R. Aragona, S. Manni, V. Mauri, M. Sala, *End-to-End Encryption: la nuova frontiera nella protezione dei dati*, Agenda Digitale (2015).
- R. Aragona, C. Giberti, M. Sala, *Algebra moderna e segreti antichi*, Sapere, anno 80° n. 4, Edizioni Dedalo (Agosto 2014), pp. 34-38.
- R. Aragona, P. Peterlongo, *Bitcoin: la valuta digitale del futuro*, UNITRENTO Web Magazine (2014).
  `http://webmagazine.unitn.it/eventi/960/bitcoin-la-valuta-digitale-del-futuro`
- R. Aragona, C. Tinnirello, M. Sala, *La matematica delle impronte digitali*, Maddmaths! La SIMAI e la divulgazione della Matematica (2013).
  `http://maddmaths.simai.eu/divulgazione/la-matematica-delle-impronte-digitali/`
- R. Aragona, M. Sala, *Strumenti personali colonna della nuova sicurezza online*, Agenda Digitale (2013).
  `http://www.agendadigitale.eu/ecommerce/409_strumenti-personali-colonna-della-nuova-sicurezza-online.htm`

Invited Talks and Contributed Talks

- 15 December 2023: "Some results on the group generated by the round functions", invited talk, CIFRIS23, CONSOB, Roma, 14 - 15 December 2023.
- 18 October 2023: "Permutation group methods for block cipher security", invited talk, Workshop on Algebra in L'Aquila 2023, University of L'Aquila, 17 - 19 October 2023.
- 6 July 2023: "Automorfismi di Coleman di gruppi finiti con 2-sottogruppi di Sylow semidiedrali", invited talk, Teoria dei Gruppi a Paestum, Hotel Le Palme, Paestum (Salerno, Italy), 6 - 7 July 2023.
- 21 June 2022: "Regular subgroups with large intersection", invited talk, ISCHIA GROUP THEORY 2022, Grand Hotel delle Terme Re Ferdinando, Ischia (Naples, Italy), 20 - 25 June 2022.
- 27 May 2021: "Permutation group methods for block cipher security", online invited talk, CrypTO Conference 2021 organized by Politecnico di Torino.
- 7 December 2020: "A tokenization algorithm for secure digital payments", online talk for University of Campania "Luigi Vanvitelli", invited by Prof. Antonio Tortora.
- 13 February 2020: "Enigma tra intrighi storici e matematici", jontly with Dr. Alice Lemmo, invited by Prof. Francesco Leonetti, at Gran Sasso Science Institute, L'Aquila.
- 7 February 2020: "Group Theoretical Approach for Symmetric Encryption", at University of Rome "Tor Vergata", invited by Prof. Fabio Gavarini.
- 13 June 2019: "Wave-shaped round functions and primitive groups", at the campus of Cremona of the Politecnico Milano, SandGAL 2019.
- 18 April 2017: "The group generated by the round functions of a GOST-like cipher", at University of Salento, invited by Prof. Francesco Catino.

- 10 March 2017 "The group generated by the round functions of a GOST-like cipher", at University of Salerno, invited by Prof. Antonio Tortora.
- 8 March 2017 "A Tokenization Algorithm for Payment: from Mathematics to Industrial Application", at University of Perugia, invited by Massimo Giulietti.
- 3 December 2016: "Giochiamo con la Teoria dei Grafi" (i.e. "Play with Graph Theory"), at Alma Mater Studiorum - University of Bologna, invited by Giorgio Bolondi.
- 24 November 2014: "Homomorphic Encryption and DGHV scheme", at University of Perugia, invited by Massimo Giulietti.
- 15 October 2012: "Sistemi Dinamici Sequenziali, Teoria delle Rappresentazioni e Combinatoria" (i.e. "Sequential Dynamical Systems, Representation Theory and Combinatorics"), at University of Trento, invited by Prof. Massimiliano Sala.
- February 2010: Two talks about "Universal Central Extensions of Loop Algebras and Loop Groups" at "Sapienza" University of Rome, invited by Prof. Alessandro D'Andrea and Prof. Andrea Maffei.
- 16 June 2008: "Semi-invarianti di quiver simmetrici" (i.e. "Semi-invariants of symmetric quivers"), at University of Rome "Tor Vergata", invited by Prof. Fabio Gavarini.
- 5 March 2007: "Una introduzione allo studio delle rappresentazioni di quiver" (i.e. "An introduction to the study of quiver representations"), at University of Rome "Tor Vergata", invited by Prof. Elisabetta Strickland.

Academic Services

- Since 2024: Member of "Commissione Stakeholders" of the BSc and MSc in Mathematics, University of L'Aquila
- Since 2024: Member of "Commissione Didattica" of the Doctorate school "Mathematics and Models" at Department of Information Engineering, Computer Science, and Mathematics - University of L'Aquila
- 2022 - 2023: Member of "Commissione pratiche Studenti" of the MSc in Information and Automation Engineering of the University of L'Aquila.
- Since 2021: Responsible for "Street Science" of the Department of Information Engineering, Computer Science and Mathematics of University of L'Aquila
- Since 2018: Member of the Doctorate Council of the Doctorate school "Mathematics and Models" at Department of Information Engineering, Computer Science, and Mathematics - University of L'Aquila
- October - December 2016: Representative of Post-Docs at the Department of Mathematics of the University of Trento.

Organizing tasks

- Member of Scientific Committee of the conference "Workshop on Algebra in L'Aquila 2023" - University of L'Aquila, 17 – 19 October 2023.
- Member of Scientific Committee of the conference "Cryptography and Coding Theory" - University of Perugia, 21 – 22 September 2023.
- Member of Scientific Committee of the conference "Young Researchers Algebra Conference 2023" - University of L'Aquila, 25 – 29 July 2023.
- Member of Organizing Committee of the conference "Topics in Algebra - a conference in honor of Andrea Caranti and Carlo Scoppola" - University of Trento, 1 – 2 September 2022.
- Member of Organizing Local Committee of the national congress "XXXVI Convegno UMI-CIIM AQ2022" - University of L'Aquila, 6 – 8 October 2022.
- Member of Organizing Committee of the online conference "Cryptography and Coding Theory", organized by the group CRITTOGRAFIA E CODICI (Italian Mathematical Union) and by De Componendis Cifris - University of L'Aquila, September 2021.
- Organization and conducting, jointly with Norberto Gavioli (University of L'Aquila), of workshops on Math Olympics.
- Member of Organizing Committee of the workshop "La De Cifris incontra Perugia" - University of Perugia, 16 October 2019.
- Member of Scientific Committee of the workshop "Algebra for Cryptography" - University of L'Aquila, 10 – 11 October 2019.

- May 2019 - December 2022: Member of Organizing Committee of the cycle of seminars "De Cifris Schola Latina" regarding cryptography and applications, in collaboration with Giulio Codogni and Marco Pedicini (Department of Mathematics and Physics of University of Roma Tre) and Daniele Venturi (Department of Computer Science of "Sapienza" University of Rome).
- Organizer of the workshop "Crittografia nella Vita Reale" - University of L 'Aquila, 14 May 2019.
- Member of Organizing Committee of the workshop "PQCifris 2019" - CONSOB, Rome, 9 May 2019.
- Member of Organizing Committee of the workshop "CifrisChain 2019" - CONSOB, Rome, 9 May 2019.
- Member of Organizing Committee of the workshop "La De Cifris incontra Roma" - University of Roma Tre, 4 October 2018.
- Member of Organizing Committee of "Workshop di Crittografia BunnyTN 7" - University of Trento, 16 November 2016.
- Member of Organizing Committee of "Workshop di Crittografia BunnyTN 6" - University of Trento, 17 December 2015.
- Member of Organizing Committee under the direction of Local committee and Executive committee of the conference "MEGA 2015" (Effective Methods in Algebraic Geometry) - University of Trento, 15 - 19 June 2015. Website: `http://mega2015.science.unitn.it`.
- Member of Organizing Committee of "Workshop di Crittografia BunnyTN 5" - University of Trento 22 November 2014.
- Member of Organizing Committee of "Workshop di Crittografia BunnyTN 4" - University of Trento 22 May 2013.
- Member of Organizing Committee of the conference "Convegno Nazionale Incontri con la Matematica n° 26. La didattica della matematica: insegnamento e apprendimento a confronto", organized by Department of Mathematics of the University of Bologna and Nucleo di Didattica della Matematica di Bologna - Castel San Pietro Terme (BO), 26 - 28 October 2012.
- Member of Organizing Committee of the conference "MJdR" - "Sapienza " University of Rome, 24-25 September 2009.

Editing and refereeing activity

- Referee for *PROGRAMMA VINCI, Bando 2022, Erogazione di finanziamenti a supporto di progetti accademici binazionali tra Francia e Italia*, funded by Università Italo Francese. Website: `https://www.universite-franco-italienne.org/menu-principal/bandi/programma-vinci/bando-2022/`.
- Editor of volume *Algebra for Cryptography* of the book series *Collectio Ciphrarum* published by Aracne, ISBN: 979-12-5994-328-6.
- Referee for *Applicable Algebra in Engineering, Communication and Computing*, *Mediterranean Journal of Mathematics*, *Matematicki Vesnik* and *International Journal of Group Theory*.
- Reviewer for *Mathematical Reviews* and *Zentralblatt MATH*.

Participation in national research projects

- PRIN 2015 "Group theory and applications", scientific manager Prof. Andrea Lucchini (Prot. 2015TW9LSR).
- FUTURO IN RICERCA 2008 "Teoria di Lie e applicazioni", scientific manager Prof. Alberto De Sole (Prot. RBFR08JEXA_001).
- PRIN 2007 "Teoria delle rappresentazioni: aspetti algebrici e geometrici", scientific manager Prof. Riccardo Salvati Manni (Prot. 20074S8FZR_002, 22/09/2008-2010).

Further scientific activities

- Member of the Scientific Committee of "Associazione Nazionale De Componendis Cifris"
- Member of the group CRITTOGRAFIA E CODICI (Italian Mathematical Union)
- Member of "Unione Matematica Italiana" (Italian Mathematical Union).
- Member of Gruppo INDAM "GNSAGA - Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni".

- Member of the national cryptographic association "De Componendis Cifris".

Further science communication activities

- Mathematics laboratory "Enigma tra intrighi storici e matematici", invited by Prof. Annaluna Coco, at IIS Patini Liberatore - L'Aquila, 18 November 2020.
- Organizer, jointly with Prof. Carlo Maria Scoppola and Prof.ssa Debora Amadori, of "Street Science" for the Department of Information Engineering, Computer Science and Mathematics of University of L'Aquila - L'Aquila, September 2018 and September 2019.
- Organizer, jointly with Dott.ssa Ceria, of "La ricerca va in città" for Department of Mathematics of the University of Trento, 30 September 2016.
- Organizer, jointly with Prof. Andrea Caranti, of "La Notte dei Ricercatori 2015" for Department of Mathematics of the University of Trento, 25 September 2015.
- Organizer, jointly with Prof. Andrea Caranti, of "La Notte dei Ricercatori" for Department of Mathematics of the University of Trento - Museo delle Scienze di Trento "MUSE", 26 September 2013.
- From 2013 to 2017: Speaker during the events "Porte Aperte" organized by the Department of Mathematics of the University of Trento for high school students.
- As freelance for Formath Project (s.r.l. of Bologna dealt with transfer knowledge, science communication and popular science), I designed, organized and attended some popular science workshops for primary and secondary schools and for public audience.

Other work experiences

- June 2012- July 2012 : Marking and encoding of mathematics tests of OECD-PISA 2012 at Istituto nazionale per la valutazione del sistema educativo di istruzione e di formazione (INVALSI).
- October 2010- June 2011: Teaching assistant. Mathematics in the english language Middle and High school "Rome International School" (General Certificate of Secondary Education-GCSE, International Baccalaureate-IB).

Language Skills

Proficient english (writing, speaking).

Computer skills

LaTeX, Microsoft Office, MAGMA.

Roma, 25/105/2024 Riccardo Aragona