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 : +393483993748
E-mail : *ric.aragona@gmail.com*

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 2019: 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" 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" at University of Trento (Italy).
- February 2011 - January 2012: post-doc fellowship "Transformation Groups and Applications" at "Sapienza" University of Rome (Italy).

Teaching experience

- Since November 2019: Tutor of the following PhD students:
  - Margherita Paolini (SSD MAT/02, topic: Representation Theory);
  - Jessica Alessandrì (SSD Mat/02, topic: Elliptic curves).
- Since February 2013: I supervised as first advisor and second advisor:
  - 16 MSc theses in Mathematics and Information and Automation 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).

– 3 BSc theses in Mathematics:

* Ilaria Zilio (University of Trento), *Polynomials on Finite Fields*, advisor: Prof. Massimiliano Sala.
* Lorenzo Di Lisio (University of L'Aquila), *Curve ellittiche e applicazioni crittografiche*, advisor Dr. Riccardo Aragona.
* Michela Ettorre (University of L'Aquila), *Aspetti algebrici e sicurezza crittografica di un algoritmo di tokenizzazione ?*, advisor Dr. Riccardo Aragona.

– 1 BSc theses in Computer Science:

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

- 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

During Ph.D., my research interests are been focused upon two specific topics: representations of finite-dimensional algebras and quiver representations. In particular, I studied the behavior of the invariants for the actions of products of classical groups on the variety of symmetric quiver representations [22,23,24]. Moreover I went into more depth the theory of Cluster algebras and the theory of Cluster Categories.
Then I worked with Alessandro D'Andrea ("Sapienza" University of Rome) and Francesco Vaccarino (Politecnico di Torino) about the connection of Representation theory with Algebraic Statistics (applied to

Phylogenetics), Computer Science and Dynamical Systems (applied to modeling and simulations of natural, biological and social systems). In particular, we studied Sequential Dynamical Systems (SDS), using techniques regarding Representation Theory and Semigroup Theory [21]. Together with Alessandro D'Andrea we then continued these studies [5].
Currently I am dealing with some aspects of Algebraic Cryptography, I am mainly focusing on the application of Group Theory to Symmetric Cryptography; in particular, I am interested on the following topics:

- **Permutation group methods for block cipher security**, In 1,[9,13,15,1620,27] we study the groups generated by the encryption functions of block ciphers and in [6,25] we investigate some group-theoretical properties of the key-schedule of block ciphers. Moreover, we describe some properties of the components, both linear and non-linear, acting within block ciphers useful to prevent some their weaknesses. We have also designed a new block cipher structure (Wave-shaped ciphers) within which it is possible to insert a non-linear component optimal from the point of view of differential cryptanalysis and then we proved to be resistant to some algebraic attacks based on Group Theory [10]. We also showed that the group generated by the round functions of the AES cipher cannot be embedded into a linear group acting on a vector space W, unless the dimension of W is huge, making this embedding useless in practice [12]. Recently in [3,4,8,26], we study the relationships between elementary abelian regular subgroups, Sylow 2-subgroups and a certain normaliser chain in the symmetric group $\mathrm{Sym}(\mathbb{F}_n^2)$, in view of the interest for their applications in symmetric cryptography.
- **Fully Homomorphic Encryption (FHE)**. In [19,28] we compute two bounds on the size of the secret key for the FHE scheme over the integers of van Dijk et al. (DGHV scheme) to decrypt correctly a ciphertext after a fixed number of additions and a fixed number of multiplication. Moreover we improve the original bound on the dimension of the secret key for a general circuit.
- **Cryptanalysis on block ciphers**. In [18] we introduce a slight improvement to the Partial Sum Attack (one of the most powerful attacks, independent of the key schedule, against reduced-round versions of AES) which lowers the number of chosen plaintexts needed to successfully mount it and which can be carried out completely in practice.
- **Asymmetric Cryptography**. In [17] we provide a rigorous analysis of the RSA cryptographic keys employed in the Certification Authority (CA) to certify the keys exchange during some financial transactions. In particular, we provide an attacker model useful to determine the optimal length and cryptoperiod of RSA moduli used by such CAs. In detail, we base our analysis on the execution times of the attacks known in literature, which depend also on the computational power of the attacker. In [2] we present a novel elliptic-curve based solution, derived from the previously released cryptographic protocol TAKS.
- **Attribute Based Encryption**. In [11] we propose a new *key-policy revocable-storage attribute- based encryption (RS-ABE) scheme*, i.e. a public-key encryption scheme which employs some attributes to manage the access to a certain document using a keys depending on these attributes and in which we introduce user revocation. Moreover, we prove its security in term of indistinguishability under a chosen-plaintext attack (IND-CPA).
- **Tokenization**. In [14] we propose a tokenization algorithm and we provide some formal proofs of security for it, which imply our algorithm satisfies the most signicant security requirements described in tokenization guide-lines of *Payment Card Industry Security Standard Council (PCI SSC)*.
- **Information Theory**. In [7] we derive from the entropy theorem a simple proof of a pointwise inequality first stated by Ornstein and Shields.

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 [17].

- **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 [11].

Publications

1. R. Aragona, R. Civino, *On invariant subspaces in the Lai-Massey scheme and a primitivity reduction*, Mediterranean Journal of Mathematics, 18(4), 165 (2021).
2. 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, Online First, 1-20 (2021)
3. R. Aragona, R. Civino, N. Gavioli, C. M. Scoppola, *Rigid commutators and a normalizer chain*, Monatshefte für Mathematik, Online First, 1-25 (2021)
4. R. Aragona, R. Civino, N. Gavioli, C. M. Scoppola, *A chain of normalizers in the sylow 2-subgroups of the symmetric group on 2n letters*, to appear in Indian Journal of Pure and Applied Mathematics, 1-13 (2020)
5. 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).
6. 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).
7. 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).
8. 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).
9. R. Aragona, A. Meneghetti, *Type-Preserving Matrices and Security of Block Ciphers*, Advances in Mathematics of Communications 13(2), 235-251(2019).
10. 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).
11. R. Aragona, F. Giacon, M. Sala, *A proof of security for a key-policy RS-ABE scheme*, JP Journal of Algebra, Number Thoery and Applications 40(1), pp. 29 - 90 (2018).
12. 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).
13. 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].
14. 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).
15. 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).
16. 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).
17. 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).
18. 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`.
19. 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).
20. 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).
21. R. Aragona, A. D'Andrea, *Hecke-Kiselman Monoids of Small Cardinality*, Semigroup Forum 86(1), pp. 32-40 (2013).

22. R. Aragona, *Semi-invariants of Symmetric Quivers of Finite Type*, Algebras and Representation Theory 16(4), pp. 1051-1083 (2013).
23. R. Aragona, *Semi-invariants of Symmetric Quivers of Tame Type*, Algebras and Representation Theory 15(6), pp. 1215-1260 (2012).
24. 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

25. R. Aragona, R. Civino, F. Dalla Volta,*On the primitivity of the AES key-schedule*, submitted to Journal of Algebra, 2021.
26. R. Aragona, R. Civino, N. Gavioli, C. M. Scoppola, *Unrefinable partitions into distinct parts in a normalizer chain*, submitted to Monatshefte für Mathematik, 2021.

Proceedings

27. 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).
28. 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

- 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 Dr. 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.
- 4 December 2019: "Group Theoretical Approach for Symmetric Encryption", at University of L'Aquila, organized by Prof.ssa Francesca Guarguaglini and Prof. Lucio Bedulli.
- 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 Dr. 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.

Abroad periods

I went to Northeastern University of Boston MA (USA) to work with Professor Jerzy Weyman in the following periods:

- October-December 2007.
- October-December 2008.
- January-February 2010.

Organizing tasks

- Responsible for "Street Science" of the Department of Information Engineering, Computer Science and Mathematics of University of L'Aquila
- 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
- Member of Organizing Local Committee of the national congress "UMI-CIIM" - University of L'Aquila October 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.
- Da May 2019: 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.

Representation tasks

- Representative of Post-Docs at the Department of Mathematics of the University of Trento.

Editing and refereeing activity

- Editor volume *Algebra for Cryptography* of the book series *Collectio Ciphrarum* published by Aracne.
- Referee for *Applicable Algebra in Engineering, Communication and Computing*, *Mediterranean Journal of Mathematics* and *Matematicki Vesnik*.
- Reviewer for *Mathematical Reviews* and *Zentralblatt MATH*.

Further scientific activities

- Member of "Unione Matematica Italiana".
- 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".
- Participates in the following projects:
  - PRIN 2015 "Group theory and applications", scientific manager Prof. Andrea Lucchini (Prot. 2015TW9LSR).
  - PRIN 2007 "Teoria delle rappresentazioni: aspetti algebrici e geometrici", scientific manager Prof. Riccardo Salvati Manni (Prot. 20074S8FZR_002, 22/09/2008-2010).

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.

Fellowships and awards

- March 2017: Grant for post-doc position from University of Trento, cofunded by the Department of Information Engineering, Computer Science and Mathematics of University of L'Aquila, within the Project of National Interest PRIN 2015..
- September 2014: Grant for teaching assistant for *Algebraic Cryptography* (SSD MAT/02), given by Prof. Sala at University of Trento (Italy).
- September 2013: Grant for teaching assistant for *Cryptography* (SSD MAT/02), given by Prof. Sala at University of Trento (Italy).
- January 2013: Grant for post-doc position from University of Trento.
- September 2012: Teacher's contract for *Preparatory course of Mathematics* at Faculty of Engineering, "Sapienza" University of Rome (Italy).
- May 2012: Grant for marking and encoding of mathematics test of OECD-PISA 2012 from INVALSI.
- February 2011: Grant for post-doc position from "Sapienza " University of Rome.
- October 2005: Grant for Ph.D. from University of Rome "Tor Vergata".

Conferences, Summer Schools and Workshops

- June 2019: "SandGAL 2019 - Semigroups and Groups, Automata, Logics" (Cremona, Italy).
- May 2019: "Crittografia nella Vita Reale" (L'Aquila, Italy).
- May 2019: "PQCifris 2019" (Roma, Italy).
- May 2019: "CifrisChain 2019" (Roma, Italy).
- October 2018: "La De Cifris incontra Roma" (Roma, Italy).
- March 2018: "Ischia Group Theory" (Ischia, Italy).
- June 2017: "The 13th International Conference on Finite Fields and their Applications" (Gaeta, Italy).
- November 2016: "Cryptography Workshop BunnyTN 7" at University of Trento.
- December 2015: "Cryptography Workshop BunnyTN 6" at University of Trento.
- September 2015: Conference "XX Congresso dell'Unione Matematica Italiana" (Siena, Italy).
- June 2015: "MEGA 2015 (Effective Methods in Algebraic Geometry)" (Trento, Italy).
- April 2015: Conference "The Ninth International Workshop on Coding and Cryptography 2015 (WCC 2015)" (Paris, France).
- December 2014: "Cryptography Workshop BunnyTN 5" at University of Trento.
- May 2013: "Cryptography Workshop BunnyTN 4" at University of Trento.
- October 2012: Conference "Convegno Nazionale Incontri con la Matematica n° 26. La didattica della matematica: insegnamento e apprendimento a confronto" (Castel San Pietro Terme (BO), Italy).
- September 2012: Conference "Seminario per gli autori delle prove del Servizio Nazionale di Valutazione (SNV)" (Rome, Italy).
- June 2011: Conference "Claudio 70" (Rome, Italy).
- February-March 2011: Workshop "Algebre e Gruppi di lacci" ("Loop Algebras and Loop Groups"), organized by Professors Alessandro D'Andrea and Andrea Maffei at "La Sapienza" University of Rome.

- June 2010: Conference "Incontro Nazionale di Algebra Moderna" (Rome, Italy).
- September 2009: Confenrence "MJdR" (Roma, Italy).
- June 2009: Conference "The Interplay of Algebra and Geometry" (Cortona, Italy).
- July 2008: Summer school "Socrates intensive programme GAMAP" (Antwerp, Belgium).
- June 2008: Conference "Symmetries in mathematics and physics" (Cortona, Italy).
- September 2007: Conference "Una giornata di Algebra a Roma: a conference in memory of Olivia Rossi Doria" (Rome, Italy).
- July 2007: Summer School "Rencontres mathématiques de Glanon 11^e édition" (Glanon, France).
- May 2007: Conference "Perspectives in Auslander-Reiten Theory" (Trondheim, Norvegia).
- April 2007: Conference "Rappresentazioni, gruppo simmetrico e schemi di Hilbert" (Rome, Italy).

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, 20/5/2021 Riccardo Aragona