



Matteo ACCLAVIO

Curriculum Vitae et Studiorum

Personal informations

Name Matteo
Family name ACCLAVIO
Place and date of birth
Nationality
Professional address
Telephone
Email
Web site

Current position

since 6/2020 **Postdoc**, University of Luxembourg, team : "Security and Trust of Software Systems"

Professional experiences

- 12/2019 - **Research engineer**, Télécom SudParis and LIX-École polytechnique, research grant title : "Linking Focusing and Automated Theorem Proving"
- 5/2020
- 12/2019 - **Adjunct Professor**, American University of Paris, Course : "Intro to computer programming II" (Object Oriented Programming)
- 5/2020
- 1/2019 - **Assegnista di ricerca**, Università Roma Tre, research grant title : "Research laboratories for the renewal of mathematical teaching"
- 12/2019
- 10/2017 - **Postdoc position in proof theory**, Inria Saclay, France, research grant title : "Structural and Computational Proof Theory"
- 11/2018
- 01/2017 - **Assistant lecturer [ATER plein temps]**, Université Caen Normandie, France
- 06/2017
- 09/2015 - **Assistant lecturer [ATER plein temps]**, Aix-Marseille Université, France
- 08/2016
- 10/2012 - **Ph.D with teaching duties**, Aix-Marseille Université, France
- 08/2015

Formation

- 10/2012–
12/2016 **Ph.D. in mathematics**
Supervisor : Yves Lafont (I2M, Institut de Mathématiques de Marseille)
Titre : *String diagram rewriting : applications in category and proof theory*.
Jury members : Willem Heijltjes (referee), Samuel Mimram (referee), Vito Michele Abrusci, Pierre-Louis Curien, Miriam Quatrini, Luigi Santocanale, Lorenzo Tortora De Falco.
- 02/2011 –
02/2013 **Franco-italian master curricula in logic (M1 + M2 + M2)**, *Università degli studi Roma Tre/Université d'Aix-Marseille II*, (Roma/Marseille) :
– **Master MDFI : “Mathématiques Discrètes et Fondements de l’Informatique” (Master degree in discrete mathematics and computer science) (M2, 10/2011 – 06/2012)**, Université d'Aix-Marseille II, Marseille
Master thesis : “Comparing various proofs of the Novikov-Boone theorem based on rewriting”
Supervisors : Lorenzo Tortora de Falco / Yves Lafont
Final grade : 14,44/20.
– **Laurea magistrale in matematica (Master degree in mathematics) (M1 + M2, 02/2011 – 02/2013)**, Università degli studi Roma Tre, Roma
Master thesis : “Undecidability of the word problem for groups : the point of view of rewriting theory ”
Supervisors : Lorenzo Tortora de Falco / Yves Lafont
Final grade : 110/110 *cum laude*.
- 09/2006–
02/2011 **Laure Triennale in Matematica (Bachelor degree in mathematics)**, *Università degli studi Roma Tre*, Roma.
Bachelor thesis : “Algoritmi efficienti per la soluzione del problema Clique”
[Efficient algorithms for clique problem solution]
Supervisor : Professeur Marco Liverani
Final grade : 98/110 .
- 07/2006 **Maturità Scientifica (High school leaving qualification in scientific studies)**, *Liceo Scientifico Statale “Federigo Enriques”*, Roma.
Final grade : 95/100.

Publications

- submitted Matteo Acclavio, Roberto Maieli. *Logic Programming with Multiplicative Structures*
- submitted Matteo Acclavio, Ross Horne and Lutz Straßburger. *An Analytic Propositional Proof System on Graphs*. <https://arxiv.org/abs/2012.01102>
- to appear Matteo Acclavio. *Exponentially Handsome Proof Nets and Their Normalization*. Postproceeding of Linearity & TLLA 2020
- to appear Matteo Acclavio, Giulio Guerrieri. *A Deep Inference System for Differential Linear Logic* (extended version). Postproceeding of Linearity & TLLA 2020
- 09/2021 Matteo Acclavio, Davide Catta and Lutz Straßburger. *Game semantics for constructive modal logics*. Tableaux2021, https://link.springer.com/chapter/10.1007/978-3-030-86059-2_25
- 07/2020 Matteo Acclavio, Ross Horne and Lutz Straßburger. *Logic Beyond Formulas : A Proof System on Graphs*. LICS2020, <https://hal.inria.fr/hal-02560105>
- 01/2020 Matteo Acclavio, Roberto Maieli. *Generalized Connectives for Multiplicative Linear Logic*. CSL2020; <https://drops.dagstuhl.de/opus/volltexte/2020/11649/pdf/LIPICS-CSL-2020-6.pdf>
- 09/2019 Matteo Acclavio, Lutz Straßburger. *On Combinatorial Proofs for Modal Logics*. Tableaux 2019, https://doi.org/10.1007/978-3-030-29026-9_13
- 07/2019 Matteo Acclavio, Lutz Straßburger. *On Combinatorial Proofs for Logics of Relevance and Entailment*. Wollic 2019, https://doi.org/10.1007/978-3-662-59533-6_1
- 07/2018 Matteo Acclavio, Lutz Straßburger. *From Syntactic Proofs to Combinatorial Proofs*. IJCAR 2018, https://doi.org/10.1007/978-3-319-94205-6_32

- 05/2018 Matteo Acclavio. *Proof diagrams for multiplicative linear logic : syntax and semantics*. Journal of Automata Reasoning, <https://doi.org/10.1007/s10817-018-9466-4>
- 06/2016 Matteo Acclavio. *Proof diagrams for multiplicative linear logic*. In EPTCS 238 and in Proceeding of Linearity 2016, <https://arxiv.org/abs/1606.09016>

Preprints

- 04/2021 Matteo Acclavio, Davide Catta and Lutz Straßburger. *Towards a Denotational Semantics for Proofs in Constructive Modal Logic*. <https://hal.archives-ouvertes.fr/hal-03201439/>
- 07/2018 Matteo Acclavio. *Gli stage Hippocampe : dall'esperienza dell'IREM di Marsiglia a quella dell'Università Roma Tre*. preprint, <http://matteoacclavio.com/Archive/RapportoHippocampe.pdf>
- 06/2015 Matteo Acclavio. *A constructive proof of coherence for symmetric monoidal categories using rewriting*. preprint, <https://arxiv.org/abs/1606.01722v2>

Talks

An updated list of my talk is available at <https://matteoacclavio.com/Math.html?page=research#Talks>

Teaching activities

- 2021-2022 University du Luxembourg :
- **Lecturer** : Security Protocols (Master course in computer science, 6h) ;
 - **Lecturer** : Distributed Systems (Bachelor course in computer science, 8h) ;
- 2020-2021 University du Luxembourg :
- **Lecturer** : Network Security (Master course in computer science, 2h) ;
 - **Lecturer** : Security2 (Bachelor course in computer science, 12h) ;
 - **Lecturer** : Security Protocols (Master course in computer science, 2h) ;
- 2020 American University of Paris :
- **Lecturer** : Intro to computer programming II [object oriented programming using JAVA] (Majour course in computer science, 56h) ;
- 2019 Università degli studi Roma Tre :
- **TD[Exercise sessions]** : Teoremi sulla logica 1 (Master students from Mathematics and from Philosophy - 12h) [Logic] ;
 - **Stages Hippocampe** : "I nodi" , "Biliardi matematici" , "Automi, grammatiche e macchine a registri" , "Giochi di carte" (15h+15h+15h+15h) ;
 - **Masterclass** : "Masterclass di logica" , "Masterclass di Geometria" [One-day hight school classes on advanced mathematics] (6h+6h) ;
- 2018 Università degli studi Roma Tre :
- **Stages Hippocampe** : "Biliardi matematici" (15h), "Automi, linguaggi e modelli di calcolo" (15h)
- 2017 ATER, Université de Caen (FR) :
- **TD [Exercise sessions]** Analyse 1 (Licence 1 Maths, Semester 2 - 52h) [Analysis] with Pr. Pierre Casevitz.
 - **TD [Exercise sessions]** Mathématiques (Licence 1 Info/MIASHS, Semester 2 - 38h) [Mathematics] with Pr. Francoise Lambert and Chamroukhi Faicel.

2015-2016 4th Ph.D year, ATER, Aix-Marseille Université (FR) :

- **CM [Lecturer]** Passerelle pour les maths (St. Charles, Licence 1 Maths/Info, Semester 1 - 20h)[Introductory tutorials for first year students].
- **CM + TD [Lecturer + Exercise sessions]** Géométrie et Arithmétique 1 (St. Charles, Licence 1 Maths/Info, Semester 1 - 20h+20h)[Geometry and arithmetics].
- **CM [Lecturer]** Introduction á l'analyse (St. Jerome, Parcours PEIP, Semester 1 - 35h)[Introduction to mathematical analysis] together with Pr. Lorenzo Brasco.
- **TD [Exercise sessions]** Géométrie et Arithmétique 1 (St. Charles , Licence 1 Maths/Info, Semester 1 - 20h+20h+20h) with Pr. Christophe Pittet, Pr. Yves Lafont, Pr. Tomasz Miernowski.
- **Stages Hippocampe** : "Les polyédres" (12h).

2012-2015 1st Ph.D year, Aix-Marseille Université :

- **TD [Exercise sessions]** Géométrie et Arithmétique 1 (2014-2015, St. Charles , Licence 1 Maths/Info, Semester 1 - 20h+20h) with Pr. Glenn Merlet.
- **TD [Exercise sessions]** Géométrie et Arithmétique 1 (2013-2014, St. Charles, Licence 1 Maths/Info, Semester 1 - 20h+20h) with Pr. Glenn Merlet.
- **TD [Exercise sessions]** Algèbre linéaire 1 (2012-2013, Luminy et St.Charles, Licence 1 Maths/Info, Semester 2 - 20h+20h)[Linear algebra 1] with Pr. Guillaume Rond and Pr. Paul Donato.
- **Stages Hippocampe** : "Matématiques et arts" (12h), "Matrices" (12h), "Maths en embuscades" (12h), "Nœuds" (12h). "Maths á la carte" (12h), "L'infini" (12h).

2008-2010 During my bachelor :

- **Teaching support (tutorial)** (24h each year) for the course "Algebra 2 : groups, rings and fields" of Pr. F. Tartarone (2008) and Pr. F. Pappalardi (2009 and 2010).
- **Teaching support (tutorial)** (30h each year) for the course "Geometria 1 : liner algebra" of Pr. E. Sernesi (2009) and Pr. L. Caporaso (2010).

Third Mission Activities

<http://matteoacclavio.com/Pop.html>

I was the organizer and promoter of "Stages Hippocampe" (<http://matteoacclavio.com/HippocampeProject.html>) at the Mathematics and Physics Department of Roma Tre University from 2016 to 2019.

- 2019 **Masterclass in Geometria [math lab for high-school]** : One day university courses on geometry : group theory, symmetries, plane isometries, plane wallpaper groups classification . Università Roma Tre (IT).
- 2019 **Masterclass in Logica [math lab for high-school]** : One day university courses on logic : logical connectives, boolean functions and boolean circuits, history of computer science from Leibniz to von Newman architecture. Università Roma Tre (IT).
- 2019 **Liceo Matematico [math lab for high-school]** : Three lessons on algorithms, logical connectives, truth and boolean circuits. Liceo Cannizzaro (IT).
- 17-21/6/19 **Professione Ricercatore** : teaching during summer school for high-school students (<https://scuoladimatematicaefisica.wordpress.com/>)
- 2019 **Stages Hippocampe** :
 - I nodi ;
 - Biliardi matematici ;
 - Automi, Grammatiche e Macchine a Registri ;
 - Matematica e carte da gioco ;Project manager and stage teacher/supervisor, Università degli studi Roma Tre (IT).
- 2019 **Liceo Matematico [math lab for high-school]** : Three lessons on plane tessellation and wallpaper groups and on platonic solids, football balls and Euler characteristic. Liceo Cannizzaro (IT).

- 5/2018 **Salon Culture & Jeux Mathématiques 2018, Paris (FR).**
- 14/3/2018 **Pourquoi les Grecs ne pouvaient-ils pas calculer π ?** : popularization talk at Marseille Pi-Day
- 2018 **Stages Hippocampe** :
 — Biliardi matematici ;
 — Automi, linguaggi e modelli di calcolo ;
 Project manager and stage teacher/supervisor, Università degli studi Roma Tre (IT).
- 5/2017 : **Salon Culture & Jeux Mathématiques 2017, Paris (FR).**
- 1-6/2017 **Labosaique Project events** (<https://www.lmno.cnrs.fr/equipes/dcm/labosaique>),
 LMNO- Université Caen Normandie (FR).
- 2016 **Stages Hippocampe** :
 — L'infinito ;
 — Poligoni e Poliedri ;
 Project manager and stage teacher/supervisor, Università degli studi Roma Tre (IT).

Langues

Italian (native) ; English (proficient) ; French (proficient) ; Spanish (basic).

Computer skills

Programming C, javascript, JAVA, Python, \LaTeX
 Other Office suit, HTML, CSS
 \LaTeX packages proofzilla (<https://matteoacclavio.com/Math.html?page=research#Tools>)

Curriculum Vitae

Nome: Alessandro Aloisio

Studi/Titoli

- aprile 2008 **Dottorato di Ricerca in “Ricerca Operativa”**, XX ciclo, con borsa di studio, conseguito il 3 aprile 2008, presso l'Università degli Studi di Roma “La Sapienza”, Dipartimento di Statistica, Probabilità e Statistiche Applicate (<http://www.dpsa.uniroma1.it/>), tutor: Prof. Claudio Arbib. Titolo tesi: “On pattern minimization and related problems in cutting stock”.
- luglio 2005 Scuola estiva ADONET/CIM, titolo: “Geometric and Algebraic Approaches for Integer Programming”, Dip. di Statistica e Ricerca Operativa, Facoltà di Scienze, Università di Lisbona, Portogallo.
- ottobre 2003 Università degli Studi di L'Aquila (Italia), Dipartimento di Informatica, (www.di.univaq.it), **laurea in Informatica (5 anni)**, voto **110/110 cum laude**, indirizzo “modelli decisionali” (Ricerca Operativa - MAT/09), tesi su “Un approccio esatto per il problema di taglio unidimensionale”, relatori Prof. Claudio Arbib e Dott. Fabrizio Marinelli.
- ottobre 1999 Università di Lisbona, Facoltà di Scienze, Dip. di Informatica, progetto **Erasmus**
luglio 2000

Contratti di Ricerca , assegni di ricerca o equivalenti

- 2020-2021 15/09/2020 – in corso. **Assegno di ricerca** presso il **Gran Sasso Science Institute (GSSI)** (IT). Supervisore Prof. Michele Flammini.
Alessandro Aloisio ha continuato il lavoro iniziato presso il Gran Sasso Science Institute e l'Università degli Studi di L'Aquila su aspetti algoritmici di social choice e game theory. Ha inoltre approfondito aspetti di fixed parameter tractability theory, specialmente riguardo al problema dell'edge-colouring.
- 2020-2021 15/06/2020 – 14/09/2020. Collaborazione scientifica presso il **Gran Sasso Science Institute (GSSI)**, “Stability and efficiency issues in coalition and group activity selection games.”. Supervisore Prof. Michele Flammini.
- 2019-2020 01/06/2019 – 31/05/2020. **Assegno di ricerca** presso l'**Università degli Studi di L'Aquila** (IT). Supervisore Prof. Guido Proietti.
Alessandro Aloisio ha continuato il lavoro iniziato presso il Gran Sasso Science Institute e su aspetti algoritmici di social choice e game theory. Ha inoltre approfondito aspetti di fixed parameter tractability theory, specialmente riguardo al problema dell'edge-colouring.
- 2018-2019 08/03/2019 – 07-04-2019. Collaborazione scientifica presso il **Gran Sasso Science Institute (GSSI)**, “Algorithmic aspects in social choice and game theory – 3rd part”. Supervisore Prof. Michele Flammini.
- 2018-2019 07/01/2019 – 08/03/2019. Collaborazione scientifica presso il **Gran Sasso Science Institute (GSSI)**, “Algorithmic aspects in social choice and game theory - 2nd part”. Supervisor eProf. Michele Flammini.

- 2018-2019 10/10/2018 – 31/12/2018. Collaborazione scientifica presso il **Gran Sasso Science Institute (GSSI)**, “Algorithmic aspects in social choice and game theory”. Supervisore Prof. Michele Flammini.
- 2013-2018 01/09/2013 – 31/05/2018. **Assegno di ricerca** presso l'**Università degli Studi di L'Aquila** (IT). Supervisore Prof. Paola Inverardi.
La posizione è stata finanziata con il **progetto MIUR Art. 10**, DM 593 - Prot MIUR DM38036. L'obiettivo principale di tale progetto è stato studiare ed applicare tecnologie avanzate basate su reti wireless di sensori per il monitoraggio ed il controllo.
Alessandro Aloisio ha lavorato anche sul progetto di ricerca europeo **European Defence Agency Project TACTICal Service oriented architecture (TACTICS)**. Gli obiettivi principali di tale progetto sono stati: definire una architettura orientata a servizi (SOA) compatibile con i vincoli di reti radio per ambienti militari tattici; studiare metodi fattibili per adattare servizi SOA ai vincoli delle reti radio per ambienti militari tattici; dimostrare la capacità della Tactical Service Infrastructure (TSI) studiata di offrire servizi ad
Alessandro Aloisio ha inoltre studiato l'Optimal Selection Problem of the QoS-Aware Service Composition. L'applicazione reale di tale problema è identificare e scegliere in modo efficiente servizi web necessari per realizzare un servizio web composto.
- 2008-2009 12/06/2009-12/10/2009. **Contratto di ricerca temporaneo** presso l'Univerità di Salerno, dipartimento di Matematica ed Informatica, settore disciplinare MAT/09 (“Operational Research”). Prof. R. Cerulli. Electronic Build Research Project – POR Campania Mis. 3.17. Argomenti: graph colouring, and matching problems.

Esperienze lavorative in ambito ICT e ricerca

- 2011-2013 13/01/2011 - 31/12/2013. Dopo aver vinto un concorso nazionale nell'area di **informatica**, è stato assunto con un contratto a tempo pieno presso la “Struttura Tecnica di Missione” (S.T.M.), (O.P.C.M n.3833 del 22/12/2009). Dal 01/04/2012 la STM è diventata “Ufficio Coordinamento Ricostruzione” (U.C.R.). Alessandro Aloisio ha ricevuto due Attestati di lodevole servizio firmati dal “Commissario delegato per la ricostruzione”.
- 2010-2011 01/11/2010 - 12/01/2011. Assunto presso la “Struttura di Missione Espropri” – Dipartimento della Protezione Civile Nazionale (Presidente del Consiglio dei Ministri) nell'area di **informatica**. L'Aquila, Italia.
- 2010 01/02/2010 - 31/10/2011. Assunto presso la “Struttura per la Gestione dell'Emergenza” (S.G.E.), Commissario Delegato per La Ricostruzione (art. 1 OPCM 3833/2009), nell'area di **informatica**. Selezione pubblica O.P.C.M 3755/2009. Scuola della Guardia di Finanza, L'Aquila, Italia.
- 2009-2010 01/08/2009 - 31/01/2010. Assunto presso la Protezione Civile Nazionale. (Presidente del Consiglio dei Ministri) nell'area di **informatica**. Selezione pubblica (art.10 O.P.C.M. 3755/2009).
Alessandro Aloisio ha ricevuto un certificato di Pubblica benemerenzia firmato dal Capo del Dipartimento della Protezione Civile Nazionale, DPCM 19/12/2008.
- 2009 FORMIT (Fondazione per la Ricerca sulla Migrazione e sulla Integrazione delle Tecnologie) - Ente morale riconosciuto con Status Consultivo dell'ECOSOC delle Nazioni Unite- contratto a progetto in ambito **ICT** (Information and communication Technology), per un “**Servizio di Supporto decisionale continuativo allo Stato Maggiore della Difesa**”, per il **Ministero della Difesa**.

- 2009 FORMIT – contratto a progetto in ambito **ICT** (Information and communication technology) – **progetto europeo SMART-SEC** on *Critical Communication and Information Infrastructures* (CIIIs) – progetto europeo WIEWER – *Video intelligence software in Europe*. Ha svolto una analisi della situazione attuale dei Paesi Europei utilizzando algoritmi di **data-clustering**. Ha sviluppato 2 database per la gestione dei dati relativi ai progetti.
- Luglio 2009 **Commissario di matematica applicata** (A048) per gli Esami di Stato 2008/09, presso la scuola Statale I.T.C. “G. Galilei” di Avezzano.
- 2008-2009 12/06/2009-12/10/2009. **Contratto di ricerca temporaneo** presso l’Univerità di Salerno, dipartimento di Matematica ed Informatica, settore disciplinare MAT/09 (“Operational Research”). Prof. R. Cerulli. Electronic Build Research Project – POR Campania Mis. 3.17. Argomenti: graph colouring, and matching problems.
- 2006-2008 Partecipazione al **progetto di ricerca europeo** n. COOP-CT-2006-032998, SCOOP – SHEET CUTTING AND PROCESS OPTIMIZATION for furniture enterprises.
Sviluppo di modelli di programmazione matematica e schemi di decomposizione per cutting, packing, scheduling e in-process inventory control. In particolare, ha affrontato i problemi di minimizzazione dei setup e di minimizzazione degli open stack, sia nel caso generale che in una serie di casi particolari in cui è limitato il numero di part type appartenenti allo stesso pattern. Inoltre, ha sviluppato algoritmi efficienti per la risoluzione di tali modelli di **programmazione matematica**.
- 2004- 2005 Nous Informatica S.r.l Roma e **Università degli Studi di L’Aquila** (in collaborazione con **Accenture S.p.a. Roma**), Proff. F. Rossi e S. Smriglio, **Models and algorithms for back-office activities in a big call centre (Wind S.p.a.)**.
Alessandro Aloisio ha studiato un caso reale della gestione dei case in un back office di un call-center di grandi dimensioni (Wind S.p.a.). Gli operatori del back office lavorano le richieste (case) dei clienti che non possono essere soddisfatte dagli operatori addetti al contatto diretto con la clientela. I case vengono suddivisi per tipo e priorità formando delle code di lavorazione.
Il problema è stato modellato come un particolare tipo di Job Shop Scheduling con vincoli di tipo start-start. L’obiettivo è quello di decidere come assegnare i case agli operatori in modo da minimizzare i tempi di attesa dei clienti. Alessandro Aloisio ha, quindi, sviluppato algoritmi efficienti per la risoluzione del problema.

Pubblicazioni - Riviste internazionali

- 1) Alessandro Aloisio, Alfredo Navarra: *Budgeted constrained coverage on bounded carving-width and series-parallel multi-interface networks*. Internet of Things 11 (2020)
- 2) Alessandro Aloisio, Alfredo Navarra: *Constrained Connectivity in Bounded X-Width Multi-Interface Networks*. Algorithms 13(2): 31 (2020)
- 3) Alessandro Aloisio, Alfredo Navarra, Leonardo Mostarda: *Energy consumption balancing in multi-interface networks*. Journal of Ambient Intelligence and Humanized Computing (2019)
- 4) Alessandro Aloisio, Claudio Arbib, Fabrizio Marinelli: *Cutting stock with no three parts per pattern: Work-in-process and pattern minimization*. Discrete Optimization 8(2): 315-332 (2011)
- 5) Alessandro Aloisio, Claudio Arbib, Fabrizio Marinelli: *On LP relaxations for the pattern minimization problem*. Networks 57(3): 247-253 (2011)

Pubblicazioni - Conferenze e workshop internazionali

- 1) Alessandro Aloisio, Michele Flammini, Bojana Kodric, Cosimo Vinci, *Distance Polymatrix Coordination Games*, Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, IJCAI 2021, (2021- Accepted)
- 2) Alessandro Aloisio, Vahan Mkrtchyan (2021) *Algorithmic Aspects of the Maximum 2-edge-colorable Subgraph Problem*. In: Barolli L., Woungang I., Enokido T. (eds) Advanced Information Networking and Applications. AINA 2021. vol 227. Springer, Cham.
https://doi.org/10.1007/978-3-030-75078-7_24
- 3) Alessandro Aloisio, Michele Flammini, Cosimo Vinci. *The Impact of Selfishness in Hypergraph Hedonic Games*. The Thirty-Fourth AAAI Conference on Artificial Intelligence AAAI 2020, 1766-1773, (2020)
- 4) Alessandro Aloisio, Alfredo Navarra. *Budgeted Constrained Coverage on Series-Parallel Multi-interface Networks*. AINA 2020, Advances in Intelligent Systems and Computing, 458-469 (2020).
- 5) Alessandro Aloisio: *Coverage Subject to a Budget on Multi-Interface Networks with Bounded Carving-Width*. WAINA 2020, Advances in Intelligent Systems and Computing, 937-946, (2020).
- 6) Matteo Micheletti, Roberto Gagliardi, Fausto Marcantoni, Alessandro Aloisio: *Unequal Rotating Energy Efficient Clustering for Heterogeneous Devices (UREECHD)*. WAINA 2020, Advances in Intelligent Systems and Computing, 917-925, (2020).
- 7) Alessandro Aloisio, Alfredo Navarra, Leonardo Mostarda: *Distributing Energy Consumption in Multi-Interface Series-Parallel Networks*. WAINA2019, Advances in Intelligent Systems and Computing, Kunibiki Messe, Matsue, Japan, March 27 - 29, (2019).
- 8) Alexander Perucci, Marco Autili, Massimo Tivoli, Alessandro Aloisio, Paola Inverardi: *Distributed Composition of Highly-collaborative Services and Sensors in Tactical Domains*. Proc. of the 7th Int'l Conf. in Software Engineering for Defence Applications, SEDA, Roma, Italy, June 7-8, (2018).
- 9) Alessandro Aloisio, Alfredo Navarra: *Balancing Energy Consumption for the Establishment of Multi-Interface Networks*. SOFSEM 2015, Pec pod Sněžkou, Czech Republic, January 24-29, (2015).
- 10) Alessandro Aloisio, Marco Autili, Alfredo D'Angelo, Antti Viidanoja, Jérémie Leguay, Tobias Ginzler, Thorsten Lampe, Luca Spagnolo, Stephen D. Wolthusen, Adam Flizikowski, Joanna Sliwa: *TACTICS: TACTICal Service Oriented Architecture*. The 3rd International Conference in Software Engineering for Defence Applications, SEDA, Roma, Italy, September 22-23, (2014).
- 11) Alessandro Aloisio, Claudio Arbib, Fabrizio Marinelli: *A Note on LP Relaxations for the 1D Cutting Stock Problem with Setup Costs*. 7th Cologne-Twente Workshop on Graph and Combinatorial Optimization, Gargnano, Italy, May 13-15, (2008).

Pubblicazioni - Conferenze italiane

- 1) Alessandro Aloisio, Paola Inverardi, Vittorio Cortellessa, Sebastiano Schillaci: *Smart Naval Ports: an SOA approach*. I-CiTies 2015, Palermo, Italy, October 29-30, (2015).

Pubblicazioni informali

- 1) Alessandro Aloisio, Vahan Mkrtchyan: *On the fixed-parameter tractability of the maximum 2-edge-colorable subgraph problem*. CoRR abs/1904.09246 (2019).

Pubblicazioni - Short and Extended Abstracts

- 1) Claudio Arbib, Alessandro Aloisio, Fabrizio Marinelli, *Cutting Stock with No Three Parts per Patterns: Work-in-Process and Pattern Minimization*, XXXIX Conference, AIRO2008, Ischia-I, September 7–11, (2008).
- 2) Claudio Arbib, Alessandro Aloisio, Fabrizio Marinelli, *Cutting Stock with No Three Parts per Patterns: Work-in-Process and Pattern Minimization*, 5th ESICUP Meeting, L'Aquila-I, April 20–22, (2008).
- 3) Alessandro Aloisio, Claudio Arbib, Fabrizio Marinelli: *On hierarchical waste-and-pattern minimization with two part types per stock item*. 3rd meeting ESICUP, Porto, Portugal, March 16–18, (2006).

Pubblicazioni - Rapporti tecnici

- 1) Claudio Arbib, Alessandro Aloisio, Fabrizio Marinelli, *On LP Relaxations for 1-Dimensional Cutting Stock with Setup Costs*, Dep. of Computer Science, University of L'Aquila, Italy, TRCS 001/2008.
- 2) Claudio Arbib, Alessandro Aloisio, Fabrizio Marinelli, *Cutting Stock with No Three Parts per Patterns: Work-in-Process and Pattern Minimization*, Dep. of Computer Science, University of L'Aquila, Italy, TRCS 002/2008.

Progetti di ricerca dove Alessandro Aloisio è stato coinvolto

1. TACTICS. (<https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/06/20/tactics-project-completed>). European Defence Agency (EDA). Attività: ricerca; scrittura di deliverable; partecipazione a quasi tutti i meeting; coordinamento con gli altri partner, ecc.
2. Art. 10. Prot MIUR DM38036. Attività: ricerca; scrittura di deliverable; partecipazione a quasi tutti i meeting; coordinamento con gli altri partner, ecc.
3. SCOOP (http://www.scoop-project.net/view_doc.php?id_sez=1&view_type=1&ord=1) FET EU, FP6. Attività: ricerca negli ambiti di Algoritmi e Ricerca operativa; scrittura di deliverable; partecipazione ai meeting, ecc.
4. SMART-SEC. Supported by the DG Information Society and Media of the European Commission. Attività: ricerca in ambito analisi dei dati (metodi numerici); scrittura di deliverable, coordinamento, presentazioni.
5. VIEWER. Supported by the Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks Programme of the European Commission, DG Home Affairs. Attività: ricerca in ambito analisi dei dati (metodi numerici); scrittura di deliverable, coordinamento, presentazioni.

Partecipazione a meeting internazionali

TACTICS project: Bonn (Germany), at FKIE (Wachtberg), 09-12/12/2014; Rome (Italy), TELEDIFE, 31/03/2015-01/04/2015; Zegrze (Poland), at Military Communication Institute (MCI), 05-10/05/2015; Bydgoszcz (Poland), at ITTI Sp. z.o.o., 16-21/06/2015; Stoccarda-Ditzinger (Germany), at Thales Deutschland, 8-11/09/2015; Gjøvik (Norway), at Gjøvik University College, 12-18/10/2015; Rome (Italy), Selex, 4-6/11/2015; Zegrze (Poland), at Military Communication Institute (MCI), 23-26/02/2016; Rome (Italy), at Finmeccanica, 5-6/03/2016.

Partecipazione a meeting nazionali

Art. 10 project: Chieti (Italy), at Thales, 10/09/2013; 16/03/2014; 19/05/2014; 14/07/2014; 11/11/2014; 15/11/2014; 21/09/2015; 05/10/2015; 15/02/2016; 21/06/2016; Livorno, North Tyrrhenian Sea Port Authority, 17-18/09/2014; L'Aquila (Italy), University of L'Aquila, 05/02/2014.

Interessi nella Ricerca e Attività scientifica

Main research interests: Combinatorial Optimization; Approximation Algorithms; Game Theory; Graph Problems; Parameterized Complexity Theory; Graph Colouring; Network Problems; Algorithms for Distributed Systems and Networks; Operational Research; Integer Programming.

Attività didattiche a livello universitario in Italia o all'estero

- 1) Anno accademico 2020-2021, Gran Sasso Science Institute (GSSI), Italy, "Intr. Parameterized Complexity Theory" – Advanced Doctorate Course for PhD students, dieci ore, in inglese, Maggio 2021.
- 2) Anno accademico 2015-2016, Università degli Studi di L'Aquila, Italia, "Software Architecture", otto ore di lezione in inglese su SOA;
- 3) Anno accademico 2015-2016, Università degli Studi di L'Aquila, Italia, "Software Architecture", assistenza agli studenti per la realizzazione di un progetto SOA.
- 4) Anno accademico 2014-2015, University of L'Aquila, Italy, "Advanced Software Architecture", nove ore di lezione in inglese su SOA.
- 5) Anno accademico 2014-2015, University of L'Aquila, Italy, "Software Architecture", assistenza agli studenti per la realizzazione di un progetto SOA, "The Naval Port System Case Study".
- 6) Anno accademico 2014-2015, University of L'Aquila, Italy, "Software Architecture", assistenza agli esami.
- 7) Corso di dottorato (2004-2007). Assistenza agli esami, assistenza agli studenti, seminari, presso l'Università degli Studi di L'Aquila, Dipartimento di Informatica, MAT/09.

Attività di relatore a Congressi e Convegni Nazionali e Internazionali

1. *relatore al congresso IJCAI 2021, tenutosi a virtual-Motreal Canada, August 19 - 26, 2021;*
2. *relatore al congresso WAINA 2021, tenutosi a Ryerson University, Toronto, Canada, May 12 - 14, 2021;*
3. *relatore al congresso SOFSEM 2015, tenutosi a Pec pod Sněžkou, Czech Republic, January 24-29, (2015)*
4. *relatore al congresso I-CiTies 2015, tenutosi a Palermo, Italy, October 29-30, (2015).*
5. *relatore al congresso The 3rd International Conference in Software Engineering for Defence Applications, SEDA, tenutosi a Roma, Italy, September 22-23, (2014).*
6. *relatore al congresso 3rd meeting ESICUP, tenutosi a Porto, Portugal, March 16–18, (2006).*

Attività di revisione

Revisione di articoli a conferenze e riviste internazionali come AAAI, IJCAI, EC, SOFSEM, SAGT, ecc.

Conoscenze tecniche acquisite

Programmazione software in ambienti: Windows, Unix e Linux

Tecnologie per lo sviluppo Web: PHP, Javascript, JQuery, Ajax, XML, HTML, CSS,

WSDL, SOAP, BPEL, XPath, Symfony

Linguaggi di programmazione: C, C++, Java, Python, PHP, Prolog, Visual Basic, Pascal

Ambienti di sviluppo: Visual Studio, NetBeans, Eclipse, C++ Builder

Software systems modelling languages: UML 2.0

Database: linguaggio SQL, MySQL, Oracle, Access, Microsoft SQL server

Software di ottimizzazione: Cplex, Lingo
Software di simulazione: Arena
Software matematici: Matlab, GeoGebra, Maxima

Lingue

Italian (native), English (fluente), Portuguese (intermedio)

L'Aquila 02/09/2021

Alessandro Aloisio

Marco Cianfriglia

Curriculum Vitae

Esperienze

Dal 2017 **Assegnista di ricerca**, IAC-CNR - Istituto per le Applicazioni del Calcolo, Roma.

Progettazione e sviluppo di un framework in grado di testare efficientemente su GPU la sicurezza dei cifrari a flusso rispetto al *Cube Attack*.

Studio, progettazione e sviluppo di soluzioni efficienti e distribuite per l'analisi e l'indicizzazione di grandi moli di dati eterogenei.

Studio e sviluppo di soluzioni efficienti per *password guessing* e *password strength meter*.

Studio, progettazione e sviluppo di soluzioni distribuite ed efficienti per calcolo simbolico relativo ai polinomi che rappresentano cifrari a flusso.

Progettazione e sviluppo di un tool efficiente per identificare il set di nodi critici, come definiti dal *Critical Node Detection Problem*, su grafi di grandi dimensioni.

Sviluppo e progettazione di codici efficienti e ad alto grado di parallelismo, capaci di sfruttare a pieno sistemi distribuiti e acceleratori (GPU).

Ottimizzazione e analisi di sicurezza di codice esistente.

Studio e sviluppo di soluzioni di *Virtual Machine Introspection* (VMI).

Configurazione e manutenzione di sistemi in produzione.

Supporto alle attività di analisi ed estrazione dati in ambito forense su pc e smartphone.

Dal 2017 **Consulente ICT**.

Attività di consulenza in ambito security, digital forensics, recupero dati.

2014–2017 **Borsa di studio di dottorato**, Università degli Studi di Roma Tre, Roma.

Vincitore borsa di studio del M.I.U.R.

Vincitore borsa del programma *HiPEAC Industrial PhD Mobility Programme*.

Associato all'Istituto per le Applicazioni del Calcolo -CNR.

2014 **Borsa di studio di ricerca**, IAC-CNR - Istituto per le Applicazioni del Calcolo, Roma.

Studio, progettazione e sviluppo di soluzioni efficienti e distribuite per l'analisi e l'indicizzazione di grandi moli di dati eterogenei.

Progettazione e sviluppo del porting delle procedure di analisi e tokenizzazione di testi di *Clucene* su GPU; *Clucene* è la versione C++ di *Lucene*, la libreria *standard-de-facto* per indicizzazione.

Attività svolte anche nell'ambito del progetto ISODAC - Indexing and Search Of Data Against Crime finanziato all'interno del programma *UE Prevention of and Fight against Crime (ISEC)- DG Home Affairs*.

Formazione

2014–2017 **Dottore di Ricerca in Matematica - Crittografia e sicurezza delle informazioni**, Università degli Studi di Roma Tre, Roma.

Tesi Titolo: *Exploiting GPUs to speed up cryptanalysis and machine learning*.

Relatori: Prof. Massimo Bernaschi

Ho progettato e sviluppato il *Kite-Attack*, una variante del *Cube Attack*, un attacco algebrico presentato da Dinur e Shamir. Questa variante permette di sfruttare a pieno la potenza computazionale offerta dalle GPU. Ho inoltre progettato e sviluppato il framework GPU di crittoanalisi basato sul kite-attack.

05-08/2017 **Research internship**, Dividiti L.T.D, Cambridge (Regno Unito).

Internship finanziato dal programma *HiPEAC Industrial PhD Mobility Programme*

Ho sviluppato un framework per l'ottimizzazione automatica di librerie scientifiche per applicazioni Data-driven utilizzando tecniche di Machine Learning. Ho inoltre lavorato all'ottimizzazione di codice per nuove architetture system-on-chip, ad esempio ARM.

2011–2013 **Laurea Magistrale in Informatica (110/110 e lode)**, *Università degli Studi di Roma La Sapienza*, Roma.

Tesi Titolo: *Text analysis on Graphics Processing Unit*.

Relatore: Prof. Massimo Bernaschi

Ho progettato e sviluppato un modulo GPU per analisi e tokenizzazione efficiente di testi. Il modulo è stato integrato all'interno di CLucene, il porting C++ di Lucene

2005–2011 **Laurea Triennale in Informatica (105/110)**, *Università degli Studi di Roma "La Sapienza"*, Roma.

Tesi Titolo: *Virtualization Security: definition, implementation and evaluation of kernel protection mechanisms of a Windows guest*.

Relatore: Prof. Luigi V. Mancini

Ho progettato e sviluppato un modulo per monitorare le strutture del kernel di un guest Windows sfruttando le potenzialità offerte dalle recenti tecnologie di virtualizzazione.

Esperienze di Insegnamento e seminari

2021 **Programmazione di Sistema**, Laurea Triennale in Informatica, Università degli Studi di Roma La Sapienza

2021 **Introduction to HPC**, HPC Summer School 2021, Libera Università di Bolzano

2019 **Security Management**, Master in Cybersecurity - School of Law, LUISS Guido Carli

2018 **Abilità informatiche e telematiche** Laurea Magistrale in informazione, editoria e giornalismo, Università degli Studi Roma Tre

2018 **Digital and Mobile forensics**, Cyber Accademy, Università degli Studi di Modena e Reggio Emilia

2018 **Forensics on Android**, Master in Digital Forensics e Tecnologie Cyber, Università degli Studi di Modena e Reggio Emilia

2016 **Laboratorio di analisi dei sistemi compromessi**, Master di I livello in Cybercrime ed Informatica Forense, Università degli Studi di Roma La Sapienza

Lingue

Italiano **Madrelingua**

Inglese **Conoscenza avanzata della lingua scritta e parlata (C1)**

Competenze Informatiche

Sistemi Operativi Unix, Windows, OSX, Android

Virtualizzazione Qemu-KVM, XEN, VirtualBox, Vmware

Linguaggi C, C++, CUDA-C, OpenCL, Java, Python, PHP, BASH, SQL

Basi di Dati MySQL, PostgreSQL, SQLite

Sistemi di versioning SVN, GIT

Calcolo parallelo e GPGPU CUDA-C, OpenCL, MPI, OpenMP

Certificazioni

2021 GIAC Reverse Engineering Malware (GREM)

Invited talk

ITASEC 2020 - Workshop su crittanalisi

Europol Forensic Expert Forum 2019 - HPC and forensics

Presentazioni, Conferenze, Seminari, Corsi

CISPA Digital Summer School, Coding Techniques & Advanced Post-Quantum Cryptography, 2021
11st International Workshop on Security and High Performance Computing Systems (SHPCS 2017), Genova, Italia
UK Manycore Developer Conference (UKMAC 2017), Warwick, Regno Unito
Summer School on Effective High Performance Computing 2016, Lugano, Svizzera
Summer School on Computer Security and Privacy 2016, Pula, Italia
Summer School on Real World Crypto and Privacy 2015, Sibenik, Croazia
Introduction to Parallel Computing with MPI and OpenMP - 2014, Roma, Italia
Midterm workshop of the Indexing and Searching of Data Aimed at Fighting Crime project (ISODAC), 2014, Roma, Italia

Pubblicazioni

- 2021 Guarino S.; Mastrostefano E., Bernaschi M., Celestini A., Cianfriglia M., Torre D., Zastrow L.R., *Inferring Urban Social Networks from Publicly Available Data*, 2021 Future Internet
- 2021 Guarino S.; Mastrostefano E., Celestini A., Bernaschi M., Cianfriglia M., Torre D., Zastrow L.R., *A Model For Urban Social Networks*, 2021 Computational Science ICCS 2021
- 2021 D. Pasquini, M. Cianfriglia, G. Ateniese and M. Bernaschi, *Reducing Bias in Modeling Real-world Password Strength via Deep Learning and Dynamic Dictionaries*, 2021 USENIX Security '21
- 2021 P. S. Labini, M. Cianfriglia, D. Perri, O. Gervasi, G. Fursin, A. Lokhmotov, C. Nugteren, B. Carpentieri, F. Zollo, and F. Vella, *On the Anatomy of Predictive Models for Accelerating GPU Convolution Kernels and Beyond*, 2021 ACM Transactions on Architecture and Code Optimization
- 2019 A. Celestini, M. Cianfriglia, E. Mastrostefano, A. Palma, F. Castiglione, and P. Tieri, *Critical nodes reveal peculiar features of human essential genes and protein interactome*. 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)
- 2019 M. Cianfriglia, S. Guarino, M. Bernaschi, F. Lombardi, and M. Pedicini, *Kite attack: reshaping the cube attack for a flexible GPU-based maxterm search*. Journal of Cryptographic Engineering
- 2017 M. Cianfriglia and S. Guarino, *Cryptanalysis on GPUs with the Cube Attack: Design, Optimization and Performance Gains*. 2017 International Conference on High Performance Computing Simulation - HPCS 2017
- 2017 M. Cianfriglia, S. Guarino, M. Bernaschi, F. Lombardi, and M. Pedicini, *A Novel GPU-Based Implementation of the Cube Attack*. Applied Cryptography and Network Security. ACNS 2017. Lecture Notes in Computer Science, vol 10355. Springer, Cham.
- 2016 G. Totaro, M. Bernaschi, G. Carbone, M. Cianfriglia, and A. Di Marco, *ISODAC: a High Performance Solution for Indexing and Searching Heterogeneous Data*, Journal of Systems and Software
- 2014 M. Bernaschi, M. Cianfriglia, A. Di Marco, A. Sabellico, G. Me, G. Carbone, and G. Totaro, *Forensic disk image indexing and search in an HPC environment*, 2014, International Conference on High Performance Computing Simulation - HPCS 2014

Peer Reviewer

- PC Member EUSPN-2016 - The 7th International Conference of Emerging Ubiquitous Systems and Pervasive Networks
- PC Member ANT-2017 - The 8th International Conference on Ambient Systems, Networks and Technologies
- PC Member EUSPN-2017 - The 8th International Conference of Emerging Ubiquitous Systems and Pervasive Networks
- PC Member ANT-2018 - The 9th International Conference on Ambient Systems, Networks and Technologies
- PC Member EUSPN-2018 - The 9th International Conference of Emerging Ubiquitous Systems and Pervasive Networks
- PC Member ANT-2019 - The 10th International Conference on Ambient Systems, Networks and Technologies
- PC Member EUSPN-2019 - The 10th International Conference of Emerging Ubiquitous Systems and Pervasive Networks
- PC Member ANT-2020 - The 11th International Conference on Ambient Systems, Networks and Technologies
- PC Member EUSPN-2020 - The 11th International Conference of Emerging Ubiquitous Systems and Pervasive Networks

PC Member EUSPN-2021 - The 12th International Conference of Emerging Ubiquitous Systems and Pervasive Networks
PC Member ANT-2021 - The 12th International Conference on Ambient Systems, Networks and Technologies
PC Member ANT-2022 - The 13th International Conference on Ambient Systems, Networks and Technologies
Reviewer MATCOM - Journal of Mathematics and Computers in Simulation
Reviewer International Journal of High Performance Computing Applications
AEC Member SC18 - The International Conference on High Performance Computing, Networking, Storage, and Analysis 2018 - Artifact Evaluation member of *IA*³
AEC Member PPOP-2019 - Principles and Practice of Parallel Programming 2019 - Artifact Evaluation
AEC Member SC21 - The International Conference on High Performance Computing, Networking, Storage, and Analysis 2021

Informazioni aggiuntive

Vincitore concorso per tecnologo tempo determinato presso Istituto Nazionale di Geofisica e Vulcanologia, bando n. 2TEC-RM1-01-2019, DDAP n. 44 del 28/01/2019

Autorizzo il trattamento dei miei dati personali presenti nel curriculum vitae ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 e del GDPR (Regolamento UE 2016/679).

Lorenzo Grassi

Curriculum Vitae

Research Experience and Current Position

- From 01/03/2020 – **PostDoc in Symmetric Cryptography**
Now Radboud University, Nijmegen (Netherlands)
◦ *Supervisor:* Prof. Joan Daemen – ESCADA Team
- From 27/04/2019 **PostDoc in Symmetric Cryptography**
to 29/02/2020 IAIK, University of Technology of Graz, Graz (Austria)
◦ *Analysis and Design of Symmetric Cryptographic Algorithms*
◦ *Supervisor:* Prof. Christian Rechberger
- From 01/09/2015 **PhD in Symmetric Cryptography**
to 26/04/2019 IAIK, University of Technology of Graz, Graz (Austria)
◦ *Title of the Thesis:* “Cryptanalysis of AES-like Ciphers and Reviving Old Design Ideas for New Constructions”
◦ *Supervisor:* Prof. Christian Rechberger
◦ *Analysis and Design of Symmetric Cryptographic Algorithms*

Impact

- No. publications:* **24**
No. citations: **641** (Google Scholar – 15/08/2021)
h-index: **12** (Google Scholar – 15/08/2021)

Teaching

- Winter Semester 2019/2020 *Applied Cryptography 1*, Master’s Course, 2 Lectures & Exercise: “Symmetric Primitives – Cryptanalysis” and “Asymmetric Primitives – Factoring, RSA”
- Summer Semester 2018/2019 *Applied Cryptography 2*, Master’s Course, 2 Lectures: “Block Ciphers: Differential Cryptanalysis” and “Block Ciphers: Advanced Differential Cryptanalysis”
- Winter Semester 2018/2019 *Applied Cryptography 1*, Master’s Course, 1 Lecture & Exercise: “Block Ciphers: Design and Analysis”
- Summer Semester 2017/2018 *Applied Cryptography 2*, Master’s Course, 2 Lectures: “Block Ciphers: Differential Cryptanalysis” and “Block Ciphers: Advanced Differential Cryptanalysis”
- Winter Semester 2017/2018 *Applied Cryptography 1*, Master’s Course, 2 Lecture & Exercise: “Block Ciphers: Design and Analysis” and “Stream Ciphers”
- Summer Semester 2016/2017 *Applied Cryptography 2*, Master’s Course, 2 Lectures: “Block Ciphers: Differential Cryptanalysis” and “Block Ciphers: Advanced Differential Cryptanalysis”

Other Professional Activities

Program Committee: FSE/ToSC 2021/2022

External Reviewer for top-level conferences, including Crypto, Eurocrypt, Asiacrypt, FSE/ToSC, SAC, among others

Education

- 10/2011- **Master Degree's in Mathematics**
 27/02/2014 University of the Study of Milano (Italy)
- *Final grades:* 110/110 cum laude (i.e., the highest possible grade in the Italian system)
 - *Title of the thesis:* "Classical and relativistic dynamics of extrasolar planetary systems"
 - *Supervisors:* Prof. Antonio Giorgilli and Dr. Marco Sansottera
 - *Main subjects of study:* Cryptography, Mathematical physics, Mathematical analysis, Programming and Stochastic calculus
- 09/2008-10/2011 **Bachelor's degree in Mathematics for Applications**
 University of the Study of Milano (Italy)
- *Title of the thesis:* "Analisi di due algoritmi per la stima delle correlazioni nei cataloghi di galassie" (Analysis of two algorithms for the estimation of statistical correlations for galaxies and clusters)
 - *Supervisors:* Prof. Andrea Carati

Work Experiences

- 11/06/2015 - **Internship at Accenture – Security**
 03/07/2015 Milano (Italy)
- 23/06/2014 - **Internship at STMicroelectronics – Cryptographer**
 22/12/2014 Agrate Brianza (Italy)
- *Side Channel Attacks* on *unmasked/masked AES* smart cards and their countermeasures (leakages: power consumption and photons emission).
 - *Tutor:* Eng. Guido Marco Bertoni (AST Security Lab).
- 07/04/2014 - **Internship at CSP S.p.A. – Java/J2EE Programmer**
 03/06/2014 Milano (Italy)
- Theoretical lectures and practical exercises to improve the knowledge of the Java Platform (Java Enterprise Edition).

Main Recent Publications

Full list of publications: <https://dblp.org/pid/166/8773-1.html>

- FSE/ToSC 2021 L. Grassi, C. Rechberger, M. Schofnegger: "*Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer*". DOI: 10.46586/tosc.v2021.i2.314-352
- EUROCRYPT 2021 C. Dobraunig, L. Grassi, A. Guinet, D. Kuijsters "*Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields*". DOI: 10.1007/978-3-030-77886-6_1
- USENIX 2021 L. Grassi, D. Khovratovich, C. Rechberger, A. Roy, M. Schofnegger: "*Poseidon: A New Hash Function for Zero-Knowledge Proof Systems*".
- ASIACRYPT 2020 M. Eichlseder, L. Grassi, R. Lüftenegger, M. Øygarden, C. Rechberger, M. Schofnegger, Q. Wang: "*An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC*". DOI: 10.1007/978-3-030-64837-4_16
- EUROCRYPT 2020 L. Grassi, R. Lüftenegger, C. Rechberger, D. Rotaru, M. Schofnegger: "*On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy*". DOI: 10.1007/978-3-030-45724-2_23
- ASIACRYPT 2019 M. Albrecht, C. Cid, L. Grassi, D. Khovratovich, R. Lüftenegger, C. Rechberger, M. Schofnegger: "*Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC*". DOI: 10.1007/978-3-030-34618-8_13

- FSE/ToSC 2018 L. Grassi: *"Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES"*. DOI: 10.13154/tosc.v2018.i2.133-160
- ASIACRYPT 2018 L. Grassi, M. Naya-Plasencia, A. Schrottenloher: *"Quantum Algorithms for the k -xor Problem"*. DOI: 10.1007/978-3-030-03326-2_18
- CRYPTO 2018 C. Dobraunig, M. Eichlseder, L. Grassi, V. Lallemand, G. Leander, E. List, F. Mendel, C. Rechberger: *"Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit"*. DOI: 10.1007/978-3-319-96884-1_22
- EUROCRYPT 2017 L. Grassi, C. Rechberger and S. Rønjom: *"A New Structural-Differential Property of 5-Round AES"*. DOI: 10.1007/978-3-319-56614-6_106
- FSE/ToSC 2016 L. Grassi, C. Rechberger and S. Rønjom: *"Subspace Trail Cryptanalysis and its Applications to AES"*. DOI: 10.13154/tosc.v2016.i2.192-225
- ASIACRYPT 2016 M.R. Albrecht, L. Grassi, C. Rechberger, A. Roy and T. Tiessen: *"MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity"*. DOI: 10.1007/978-3-662-53887-6_7
- CCS 2016 L. Grassi, C. Rechberger, D. Rotaru, P. Scholl and N. P. Smart: *"MPC-Friendly Symmetric Key Primitives"*. DOI: 10.1145/2976749.2978332

Languages

Italian Mother tongue

English Fluent

Computer Skills

Programming Languages C (advanced knowledge), C++ (intermediate knowledge), Java (basic knowledge)

Software LaTeX (good knowledge), SageMath (intermediate knowledge)

Curriculum vitae di Paolo Pistone

*Dipartimento di Informatica - Scienza e Ingegneria,
V. Mura Anteo Zamboni 7,
Università di Bologna*

INFORMAZIONI PERSONALI

Nome Paolo PISTONE

Sito Web

POSIZIONI RICOPERTE

Ott. 2019-	Assegnista di ricerca all'interno del progetto ERC DIAPASoN diretto da Ugo Dal Lago, Dipartimento di Informatica-Scienza e Ingegneria, Università di Bologna, Italia
Set. 2018- Set. 2019	Ricercatore Post-doc, Wilhelm Schickard Institute für Informatik, Università di Tübingen, Germania
Set. 2016-Ago. 2018	Assegnista di ricerca, Dipartimento di Matematica e Fisica, Università Roma Tre, Italia
Ott. 2015-Ago. 2016	Attaché temporaire d'enseignement et recherche (ATER), Institut de Mathématiques de Marseille, Università di Aix-Marseille, Francia
Gen. 2012-Mar. 2015	Studente di dottorato presso l'Institut de Mathématiques de Marseille, Università di Aix-Marseille e l'(ex) Dipartimento di Filosofia, Università Roma Tre, Francia/Italia

FORMAZIONE

Gen. 2012-Aug 2016	Dottorato in cotutela in Filosofia e Matematica, Università Roma Tre e Università di Aix-Marseille, Italia/Francia
Set. 2009- Lug. 2011	Laurea Magistrale in Scienze Filosofiche, titolo della tesi "Verso una sintassi trascendentale: ricerche sui fondamenti della logica attraverso la logica lineare e i suoi sviluppi", direttore V. M. Abrusci, Università Roma Tre, Italia

TESI DI DOTTORATO

Titolo	On proofs and types in second order logic
Co-supervisors	Jean-Yves Girard, Vito Michele Abrusci
Discussione	27 Marzo 2015, Università Roma Tre, Italia
Reviewers	Giuseppe Longo (CNRS), Jean-Baptiste Joinet (Université Lyon 3), Thomas Streicher (Università di Darmstadt)
Commissione	Vito Michele Abrusci (Università Roma Tre), Pierre-Louis Curien (CNRS, Université Paris 7), Jean-Yves Girard (Université d'Aix-Marseille), Jean-Baptiste Joinet (Université Lyon 3), Simone Martini (Università di Bologna), Enrico Moriconi (Università di Pisa)

PREMI

Nov. 2016	Prix de thèse 2016 d'Aix-Marseille Université, premio per le migliori tesi di dottorato dell'Università d'Aix-Marseille.
Mag. 2012	Premio TESI 3+2 AILA, premio per le migliori tesi di Laurea Magistrale in logica da parte dell' Associazione Italiana per la Logica e le sue Applicazioni.

ALTRI TITOLI

Lug. 2019	Abilitazione Nazionale di II Fascia, SSD MFIL-02.
Feb. 2016	“Qualification aux fonctions de Maître de Conférences”, sezioni 25 (“Mathématiques”), 27 (“Informatique”) e 17 (“Philosophie”)

PUBBLICAZIONI IN RIVISTE, CONFERENZE E VOLUMI INTERNAZIONALI CON PEER-REVIEW

Rivista	Pistone, Tranchini L., Petrolo, M. The naturality of natural deduction (II). On atomic polymorphism and generalized propositional connectives, accettato per pubblicazione in <i>Studia Logica</i> , pre-print disponibile a https://arxiv.org/abs/1908.11353 , forthcoming (vd. lettera di accettazione in allegato).
Rivista	Pistone, On completeness and parametricity in the realizability semantics of System F, <i>Logical Methods in Computer Science</i> , 15(4), pp. 6:1-6:54, 2019.
Rivista	Tranchini L., Pistone, Petrolo M., The naturality of natural deduction. <i>Studia Logica</i> , vol. 107, Issue 1, pp. 195-231, 2019.
Rivista	Pistone, Polymorphism and the obstinate circularity of second order logic, a victims' tale. <i>The Bulletin of Symbolic Logic</i> , vol. 4 Issue 2, pp. 1-52, 2018.
Rivista	Pistone, Petrolo M., On paradoxes in normal form. <i>Topoi</i> , 38(3), pp. 605-617, 2018.
Conferenza	Antonelli, M., Dal Lago, U., Pistone, On Counting Propositional Logic and Wagner's Counting Hierarchy, <i>Proceedings ICTCS 2021</i> , forthcoming (vd. lettera di accettazione in allegato).
Conferenza	Pistone, On Generalized Metric Spaces for the Simply Typed Lambda-Calculus, <i>Proceedings LICS 2021</i> , IEEE Computer Society, pp. 1-14, 2021.
Conferenza	Pistone, Tranchini L. What's Decidable about Atomic Polymorphism?, <i>Proceedings FSCD 2021</i> , LIPIcs, Volume 195, pp. 27:1-27:23, 2021.
Conferenza	Antonelli M., Dal Lago U., Pistone On Measure Quantifiers in First-Order Arithmetic, <i>Proceedings CiE 2021</i> , LNCS vol. 12813, pp. 12-24, 2021.
Conferenza	Pistone, Tranchini L. The Yoneda Reduction of Polymorphic Types, <i>Computer Science Logic 2021 (CSL2021)</i> , LIPIcs, Volume 183, pp. 35:1-35:22, 2021.
Conferenza	Geoffroy G., Pistone A Partial Metric Semantics of Higher-Order Types and Approximate Program Transformations, <i>Computer Science Logic 2021 (CSL2021)</i> , LIPIcs, Volume 183, pp. 35:1-35:18, 2021.
Conferenza	Pistone, Proof nets, coends and the Yoneda isomorphism, In <i>Proceedings Linearity-TLLA 2018</i> , arXiv:1904.06159; EPTCS 292, 2019, pp. 148-167; doi:10.4204/EPTCS.292.9, 2019.
Conferenza	Pistone, On dinaturality, typability and $\beta\eta$ -stable models, <i>2nd International Conference on Formal Structures for Computation and Deduction (FSCD 2017)</i> , Leibniz International Proceedings in Informatics (LIPIcs), vol. 84, pp. 29:1-29:17, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2017.
Conferenza	Aubert C., Bagnol M., Pistone, Seiller T., Logic Programming and Logarithmic Space, in <i>Programming Languages and Systems, 12th Asian Symposium APLAS 2014, Singapore</i> , vol. 8858 delle Lecture Notes in Computer Science, pp. 39-57, Springer, 2014.
Volume	Pistone, Tranchini L. Intensional Harmony as Isomorphism, accettato per il volume <i>Peter Schroeder-Heister on Proof-Theoretic Semantics</i> , edito da Thomas Piecha e Kai Wehmeier, Outstanding Contributions to Logic, Springer, (preprint disponibile a http://logica.uniroma3.it/pistone/Harmony.pdf), forthcoming

Volume	Pistone, Petrolo M., A normal paradox, in Arazim P. and Lávička T., editors, <i>The Logica Yearbook 2016</i> , p.173-184, College Publications, London, 2017.
Volume	Pistone, On the “no-deadlock criterion”: from Herbrand’s theorem to Geometry of Interaction, in <i>New Developments in Logic and Philosophy of Science</i> , SILFS series, College Publications, 2016.
Volume	Pistone, Rule-following and the limits of formalization: Wittgenstein’s considerations through the lens of logic, in <i>From Logic to Practice, Italian Studies in the Philosophy of Mathematics</i> , vol. 308 dei Boston Studies in the Philosophy and History of Science, Springer, 2015.
Volume	V.M. Abrusci, Pistone, On transcendental syntax: a Kantian program for logic?, in <i>Second Pisa Colloquium in Logic, Epistemology and Philosophy of Language</i> , ETS, Pisa, 2014.

--- PUBBLICAZIONI IN RIVISTE E VOLUMI ITALIANI

Volume	V.M. Abrusci, Pistone, Le direzioni della ricerca logica in Italia: la logica lineare e i suoi sviluppi, in Hykel Hosni, Gabriele Lolli, Carlo Toffalori, editors, <i>Le direzioni della ricerca logica in Italia 2</i> , p. 1-47, Edizioni ETS, Pisa, 2018.
Rivista	Pasquali F., Pistone, L’Hotel di Hilbert e l’imbarazzo della scelta. <i>Archimede</i> , vol. 1/2017, Le Monnier, 2017 (Italian journal on the didactics of mathematics), 2017.
Rivista	Pistone, Dalle regole dell’argomentazione alla logica delle regole. <i>Rivista Italiana di Filosofia Analitica Junior</i> , vol. 1 n. 2, pp. 25-38 (Italian journal for young researchers in analytic philosophy), 2011.

--- PREPRINTS

Preprint	Pistone, From Identity to Difference: a Quantitative Interpretation of the Identity Type, https://arxiv.org/abs/2107.06150 , 2021
Preprint	Lê Thành Dũng, Pistone, Seiller T., Tortora de Falco L., Finite models of polymorphism, complexity and the expressive power of type fixpoints, https://hal.archives-ouvertes.fr/hal-01979009 , 2019
Preprint	Pistone, Proof nets and the instantiation overflow property, https://arxiv.org/abs/1803.09297 , 2018

--- ORGANIZZAZIONE DI EVENTI ACCADEMICI

Scuola	Winter School <i>Logic and Transdisciplinarity</i> , https://conferences.cirm-math.fr/2687.html , CIRM Marsiglia, 7-11 Febbraio 2022 (partecipazione al comitato scientifico).
Workshop	<i>Proofs, Computation and Meaning</i> , http://ls.informatik.uni-tuebingen.de/PCM/ , con Luca Tranchini, Università di Tübingen, Germania [<i>Evento originariamente previsto per Marzo 2020, rimandato (probabilmente) al 2022 a causa della pandemia di Coronavirus.</i>].
Gruppo di lavoro	<i>Groupe de travail sur la syntax transcendente</i> , finanziato dal GDRI-LL, con T. Seiller, at LIPN, Université Paris 13, Francia, Maggio 2018.
Workshop	<i>Beyond Logic</i> , con M. Abrusci, J. Fichot et J.-B. Joinet, Università Roma Tre, Maggio 2015.
Workshop	<i>“Proofs and Types”, 25 years later</i> , con M. Abrusci, Università Roma Tre, Marzo 2015.

ALTRE ATTIVITÀ LEGATE ALLA RICERCA

Partecipazione al program committee di workshop internazionali	- Developments in Implicit Computational complexity & Foundational and Practical Aspects of Resource Analysis (DICE&FOPARA) 2019 - Trends in Linear Logic and Applications (TLLA) 2019.
Partecipazione a gruppi di ricerca internazionali	Membro dell'International Research Network in Linear Logic (IRN-LL), gruppo di ricerca internazionale finanziato dal CNRS (Francia) e dall'INDAM (Italia), https://www.linear-logic.org/en/ .
Reviewer per riviste internazionali	<i>Bulletin of Symbolic Logic</i> , <i>Journal of Philosophical Logic</i> , <i>TOPOI</i> and <i>Studia Logica</i>
Subreviewer per conferenze internazionali	<i>Computer Science Logic (CSL)</i> , <i>Formal Structures of Computation and Deduction (FSCD)</i> , <i>Logic In Computer Science (LICS)</i> and <i>Foundations of Software Science and Computation Structures (FoSSaCS)</i>

COMUNICAZIONI SU INVITO A WORKSHOPS E CONFERENZE

Workshop	<i>From proof to paradox</i> , Campinas University, Brasile, Dicembre 2019.
Workshop	<i>Studies in Mathematical Logic</i> , Sao Paulo University, Brasile, Dicembre 2019.
Workshop	<i>Le même et l'autre : identité, orthogonalité et types</i> , Università Lyon 3, Francia, Novembre 2018.
Workshop	<i>Trends in Linear Logic and Applications (TLLA 2017)</i> , Università di Oxford, Regno Unito, Settembre 2017.
Conferenza	<i>Beyond Logic</i> , ANR "Beyond Logic", Chateau de Cerisy, Francia, Maggio 2017.
Workshop	<i>Consequence and Paradox</i> , Università di Tübingen, Germania, Marzo 2017.
Workshop	<i>Linear Logic and Philosophy</i> , Università Lyon 3, Francia, Novembre 2016.
Workshop	<i>Logic, Philosophy and Computation of Proofs</i> , Università Keio, Tokyo, Giappone, Novembre 2015.
Workshop	<i>Computing, Logic and Types</i> , Università Lyon 3, Francia, Novembre 2015.
Workshop	<i>Modeling hypothetical reasoning: validity, inference and paradoxes</i> , IHPST, Università Paris 1, Francia, Febbraio 2015.
Workshop	<i>Ludics and Philosophy</i> , ANR LOCI, Casa San Bernardo (Roma), Giugno 2014.
Conferenza	<i>Transcendental Syntax: the conditions of possibility of language</i> , Università PUC, Paraty, Brasile, Settembre 2012.
Conferenza	<i>Logic and interactions 2012</i> , CIRM Marseille, Francia, Febbraio 2012.

COMUNICAZIONI RECENTI A SEMINARI

Seminario	Mathematical Foundations Seminar, Università di Bath, Regno Unito, Maggio 2021
Seminario	Équipe MAREL, Università di Montpellier, Francia, Marzo 2021
Seminario	Gruppo di Logica, Università di Verona, Febbraio 2021
Seminario	Gruppo di Logica, Università Roma Tre, Gennaio 29, 2021
Seminario	Séminaire Chocla, LIP, ENS Lyon, Francia, Novembre 2020.
Seminario	Colloquium del Wilhelm Schickard Institut, Università di Tübingen, Germania, Luglio 2019.
Seminario	Équipe PPS, IRIF, Paris 7, Francia, Marzo 2019
Seminario	Séminaire Chocla, LIP, ENS Lyon, Francia, Dicembre 2018

Seminario	Équipe Parsifal, LIX, Palaiseau, Francia, Novembre 2018
Seminario	Équipe LIMD, Université de Savoie, Chambéry, Francia, Novembre 2018
Seminario	Seminario del Dipartimento di Matematica, Università di Lisbona, Portogallo, Settembre 2018
Seminario	Équipe LoVe, LIPN, Università Paris 13, Francia, Giugno 2018
Seminario	Équipe Logik und Sprachtheorie, Universität Tübingen University, Germania, Ottobre 2017.

— ALTRE COMUNICAZIONI A WORKSHOP E CONFERENZE

Conferenza	FSCD 2021, online (video disponibile a https://www.youtube.com/watch?v=DfxtDjzK1d0&list=PL_XBOKjjR0OYGUTRcbHHo8MAuG5-857x5&index=8). Luglio 2021.
Conferenza	LICS 2021, online (video disponibile a https://www.youtube.com/watch?v=ZZd35TFhBwo). Giugno 2021.
Workshop	REPAS meeting 2021, Online. Marzo 2021.
Workshop	PIHOC-PPS-DIAPASoN meeting 2021, Online. Febbraio 2021.
Conferenza	CSL2021, online (video disponibile a https://www.youtube.com/watch?v=PFdBA6AB6tU , dal minuto 53:23). Gennaio 2021.
Workshop	<i>Joint workshop Linearity/Trends in Linear Logic and Applications 2020</i> , workshop affiliated to FSCD 2020, Online, Giugno 2020.
Workshop	<i>Joint workshop PIHOC-PPS-DIAPASoN</i> , IRIF, Université Paris 7, Francia, Febbraio 2020.
Workshop	<i>International Research Network in Linear Logic (IRN-LL)</i> , Università Roma Tre, Italia, Settembre 2019
Conferenza	<i>XXI Congresso dell' Unione Matematica Italiana</i> , Università di Pavia, Settembre 2019
Conferenza	<i>Third Proof-Theoretic Semantics conference</i> , Università di Tübingen University, Marzo 2019
Workshop	<i>Joint workshop GDRI-Crecogi-Elica</i> , IRIF, Università Paris 7, Ottobre 2018.
Workshop	<i>Joint workshop Linearity/Trends in Linear Logic and Applications 2018</i> , workshop affiliated to FSCD 2018, Università di Oxford, Luglio 2018.
Workshop	<i>2nd Meeting of the Groupe De Recherche Internationale en Logique Linéaire</i> , Università Roma Tre, Giugno 2018
Conferenza	<i>Formal Structures of Computation and Deduction (FSCD 2017)</i> , Università di Oxford University, Settembre 2017.
Workshop	<i>Parametricity, Logical Relations and Realizability</i> , workshop affiliato a <i>CSL 2016</i> , Università di Aix-Marseille, Settembre 2016
Conferenza	<i>Congress of Logic, Methodology and Philosophy of Science</i> , Università di Helsinki University, Agosto 2015.
Conferenza	<i>Logic Colloquium</i> , Università di Helsinki, Agosto 2015
Conferenza	<i>Conference on hypothetical reasoning</i> , Università di Tübingen, Agosto 2014.
Conferenza	<i>Logic Colloquium</i> , Vienna University of Technology, Luglio 2014
Conferenza	<i>Triennial Conference of the Italian Society for Logic and Philosophy of Science</i> , Università Roma Tre, Giugno 2014
Workshop	<i>PhDs in Logic VI</i> , Università di Utrecht, Aprile 2014
Conferenza	<i>XXV Meeting of the Italian Association for Logic and Applications</i> , SNS Pisa, Aprile 2014
Conferenza	<i>Mid-term Postgraduate Conference in Logic and Philosophy of Science</i> , Università di Urbino, Maggio 2013
Conferenza	<i>Philosophy of mathematics: from logic to practice</i> , SNS Pisa, Settembre 2012

INSEGNAMENTO

<i>Abbreviazioni</i>	Inf \mapsto Informatica, Mat \mapsto Matematica, Fil \mapsto Filosofia, Gen \mapsto Genomics, Com \mapsto Scienze della Comunicazione.
Laurea Gen	<i>Networks, Security and Databases</i> (24 ore), Università di Bologna, 2021
Master Inf	<i>Fondamenti Logici dell'Informatica</i> (10 ore tutorato), Università di Bologna, 2020
Laurea Gen	<i>Networks, Security and Databases</i> (24 ore), Università di Bologna, 2020
Master Inf	<i>From Denotational Semantics to Linear Logic</i> (30 ore + 30 ore tutorato), Università di Tübingen, Germania, 2019
Master Inf	<i>Introduction to Denotational Semantics</i> (30 hrs), Università di Tübingen, Germania, 2018-2019
Master Mat	<i>IN410-Modelli di Calcolo</i> (12 ore tutorato), Università Roma Tre, 2017-2018
Laurea Comm	<i>Logica e Comunicazione</i> (18 ore tutorale), Università Roma Tre, 2017
Master Mat	<i>IN410-Modelli di Calcolo</i> (12 ore tutorato), Università Roma Tre, 2017
Master Mat	<i>Logique du Second Ordre</i> (12 ore), Università di Aix-Marseille, Francia, 2016
Master Fil	<i>Logique et Mathématiques</i> (18 ore), Università di Aix-Marseille, Francia, 2016
Master Inf	<i>Logique et Théorie du Calcul</i> (12 ore), Università di Aix-Marseille, Francia, 2016
Master Fil	<i>Postulats d'Existence en Mathématiques</i> (18 ore), Università di Aix-Marseille, Francia, 2016
Laurea Inf	<i>Logique et Calculabilité</i> (40 ore tutorato), Università di Aix-Marseille, Francia, 2016
Laurea Mat	<i>Algèbre Linéaire 2</i> (30 ore), Università di Aix-Marseille, Francia, 2015-2016
Master Fil	<i>Introduction aux Mathématiques</i> (12 ore), Università di Aix-Marseille, Francia, 2015-2016

OUTREACH

Teatro	<i>Tournée de π</i> (https://www.piday.fr/) a Parigi (Théâtre des Variétés), Marsiglia (Théâtre du Silo) e Lione (Transbordeurs), 2017.
Conferenza	<i>European Researchers Night</i> , Università Roma Tre, http://nottericerca.uniroma3.it/index.php , 2017
Scuola	<i>Scuola Sperimentale di Comunicazione della Scienza</i> , Libreria Assaggi, http://maddmaths.simai.eu/news-2/scuola-sperimentale-di-comunicazione-della-scienza-201617/ , 2016-2017
Conferenza	<i>European Researchers Night</i> , Università Roma Tre, https://romatrenottericercatori.wordpress.com/ , 2016
Conferenza	<i>Treize minutes Marseille - Jeunes Chercheurs</i> , (video disponibile a https://vimeo.com/167115532), a Marsiglia (Biblioteca Alcazar), 2016
Teatro	<i>Journée de π</i> a Marsiglia (Théâtre de la Criée), 2016
Stage	<i>Stage Hyppocampe</i> , Aix-Marseille University, France, 2016 stage di ricerca di tre giorni per studenti di scuola superiore.
Teatro	<i>Journée de π</i> a Marsiglia (MuCEM), 2016

Curriculum Vitae di **Andrea Ribichini**

Dati Anagrafici

Nome: Andrea

Cognome: Ribichini

Titoli di Studio Conseguiti

29/02/2008 – **Titolo di Dottore di Ricerca in Ingegneria Informatica**
conseguito presso l'Università degli Studi di Roma “La Sapienza”.

04/04/2005 – **Abilitazione all'Esercizio della Professione di Ingegnere**
conseguita presso l'Università degli Studi di Roma “La Sapienza”.

30/10/2002 – **Laurea Quinquennale in Ingegneria Elettronica**
conseguita presso l'Università degli Studi di Roma “La Sapienza”.

21/07/1992 – **Maturità Classica**
conseguita presso il Liceo Ginnasio Statale “Giulio Cesare” di Roma.

Pubblicazioni

in Riviste Internazionali:

- C. Demetrescu, A. Ribichini, M. Schaerf “**Are Italian research assessment exercises size-biased?**”, pubblicato su *Scientometrics* 125 (2020), pagg. 533-549, Springer.

- C. Demetrescu, I. Finocchi, A. Ribichini, M. Schaerf “**On bibliometrics in academic promotions: a case study in computer science and engineering in Italy**”, pubblicato su *Scientometrics* 124 (2020), pagg. 2207-2228, Springer.

- G. Ausiello, P. G. Franciosa, I. Lari, A. Ribichini “**Max flow vitality in general and st-planar graphs**”, pubblicato su *Networks*, volume 74, numero 1 (2019), pagg. 70-78, Wiley.

- C. Demetrescu, F. Lupia, A. Mendicelli, A. Ribichini, F. Scarcello, M. Schaerf “**On the Shapley value and its application to the Italian VQR research assessment exercise**”, pubblicato su *Journal of Informetrics (JOI)*, volume 13, numero 1 (Febbraio 2019), pagg. 87-104, Elsevier.

- C. Demetrescu, A. Ribichini, M. Schaerf “**Accuracy of Author Names in Bibliographic Data Sources: An Italian Case Study**”, pubblicato su *Scientometrics*, volume 117, numero 3 (Dicembre 2018), pagg. 1777-1791, Springer.

- F. Lupia, A. Mendicelli, A. Ribichini, F. Scarcello, M. Schaerf “**Computing the Shapley value in allocation problems: approximations and bounds, with an application to the Italian VQR research assessment program**”, pubblicato su *Journal of Experimental & Theoretical Artificial Intelligence (JETAI)*, volume 30, numero 4 (2018), pagg. 505-524, Taylor & Francis.

- G. Ausiello, P. G. Franciosa, G. F. Italiano, A. Ribichini “**On Resilient Graph Spanners**”, pubblicato su *Algorithmica*, volume 74, numero 4 (Aprile 2016), pagg. 1363-1385, Springer.

- C. Demetrescu, I. Finocchi, A. Ribichini “**Reactive Imperative Programming with Dataflow Constraints**”, pubblicato su *ACM Transactions on Programming Languages and Systems (TOPLAS)*, volume 37, numero 1 (Novembre 2014), articolo n. 3, ACM New York,

NY, USA.

- G. Ausiello, P. G. Franciosa, G. F. Italiano, A. Ribichini **“Computing Graph Spanners in Small Memory: Fault-Tolerance and Streaming”**, pubblicato su *Discrete Mathematics, Algorithms and Applications (DMAA)*, volume 2, numero 4 (2010), pagg. 591-605, World Scientific Publishing Company.

- C. Demetrescu, B. Escoffier, G. Moruz, A. Ribichini **“Adapting Parallel Algorithms to the W-Stream Model, with Applications to Graph Problems”**, pubblicato su *Theoretical Computer Science (TCS)*, volume 411, numero 44-46 (Ottobre 2010), pagg. 3994-4004, Elsevier Science Publishers Ltd. Essex, UK.

- C. Demetrescu, I. Finocchi, A. Ribichini **“Trading Off Space for Passes in Graph Streaming Problems”**, pubblicato su *ACM Transactions on Algorithms (TALG)*, volume 6, numero 1 (Dicembre 2009), pagg. 1-17, ACM New York, NY, USA.

- G. Ausiello, C. Demetrescu, P. G. Franciosa, G. F. Italiano, A. Ribichini **“Graph Spanners in the Streaming Model: an Experimental Study”**, pubblicato su *Algorithmica*, volume 55, numero 2 (Ottobre 2009), pagg. 346-374, Springer New York.

in Proceeding di Conferenze Internazionali:

- G. Ausiello, P. G. Franciosa, G. F. Italiano, A. Ribichini **“On Resilient Graph Spanners”**, in Proceedings of the 21st Annual European Symposium on Algorithms (ESA '13), pagg. 85-96, 2013.

- C. Demetrescu, I. Finocchi, A. Ribichini **“Reactive Imperative Programming with Dataflow Constraints”**, in Proceedings of the 26th ACM International Conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA '11), pagg. 407-426, 2011. All'articolo è stato conferito un riconoscimento come *“OOPSLA Distinguished Paper”*. Questo articolo e' stato anche pubblicato in ACM SIGPLAN Notices, volume 46, issue 10, pagg. 407-426, 2011.

- G. Ausiello, P. G. Franciosa, G. F. Italiano, A. Ribichini **“Computing Graph Spanners in Small Memory: Fault-Tolerance and Streaming”**, in Proceedings of the 16th Annual International Computing and Combinatorics Conference (COCOON '10), pagg. 160-172, 2010.

- G. Ausiello, C. Demetrescu, P. G. Franciosa, G. F. Italiano, A. Ribichini **“Small Stretch Spanners in the Streaming Model: New Algorithms and Experiments”**, in Proceedings of the 15th Annual European Symposium on Algorithms (ESA '07), pagg. 605-617, 2007.

- C. Demetrescu, B. Escoffier, G. Moruz, A. Ribichini **“Adapting Parallel Algorithms to the W-Stream Model, with Applications to Graph Problems”**, in Proceedings of the 32nd International Symposium on Mathematical Foundations of Computer Science (MFCS '07), pagg. 194-205, 2007.

- C. Demetrescu, I. Finocchi, A. Ribichini **“Trading Off Space for Passes in Graph Streaming Problems”**, in Proceedings of the 17th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '06), pagg. 714-

723, 2006.

in Proceeding di Workshop Internazionali:

- F. Lupia, A. Mendicelli, A. Ribichini, F. Scarcello, M. Schaerf
“**Computing the Shapley Value in Allocation Problems: Approximations and Bounds, with an Application to the Italian VQR Research Assessment Program**”, in CEUR Workshop Proceedings, volume 1745, 2016, pp. 27-43 (23rd RCRA International Workshop on Experimental Evaluation of Algorithms for Solving Problems with Combinatorial Explosion, RCRA 2016; November 2016).

Partecipazione a Progetti di Ricerca

Partecipazione, in qualità di *research contributor*, ai seguenti Progetti di ricerca di Rilevante Interesse Nazionale (PRIN):

- Amanda: Algorithmics for MAssive and Networked DAta, MIUR, PRIN 2012.
- AlgoDEEP: Algorithmic Challenges for Data-intensive Processing on Emerging Computing Platforms, MIUR, PRIN 2008.
- MainStream: Algorithms for Massive Information Structures and Data Streams, MIUR, PRIN 2006.
- Algo-Next: Algorithms for the Next Generation Internet and Web: Methodologies, Design and Applications, MIUR, PRIN 2004.

Partecipazione a Conferenze in Qualità di Relatore

Relatore presso il 32nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2007), August 26 - 31, 2007, Český Krumlov, Czech Republic.

Conoscenze Informatiche

Sistemi operativi: Microsoft Windows, GNU Linux.

Linguaggi di programmazione: C, C++, Java, Python, PySpark, PHP, Assembly (Intel x86/x86_64).

Software per il typesetting: LaTeX.

Database: MySQL, MongoDB.

Librerie software ed API: Posix, Qt, Spring Framework.

Ambienti di sviluppo: Eclipse, DataBricks.

Conoscenze Linguistiche

Ottima conoscenza della lingua inglese, parlata e scritta.

Esperienze Lavorative

Occupazione attuale:

(01/05/2021 -): Assegno di Ricerca presso il Dipartimento di Ingegneria Informatica, Automatica e Gestionale “Antonio Ruberti” dell’Università degli Studi di Roma “La Sapienza”, per “Analisi bibliometriche in area

informatica”.

2020 – 2021:

(01/03/2020 – 31/01/2021): Assegno di Ricerca presso il Dipartimento Istituto Italiano di Studi Orientali ISO dell'Università degli Studi di Roma “La Sapienza”, relativo al progetto di ricerca “Sviluppo di un sistema automatizzato di recupero da cataloghi e banche dati, disambiguazione tramite identificativi univoci e indicizzazione di descrizioni bibliografiche in scritture non latine; realizzazione di un metaopac per la ricerca e consultazione di tali dati”.

2019 – 2020:

(01/08/2019 – 31/01/2020): Contratto di lavoro autonomo per “Definizione delle modalità di ingestione, pulizia ed analisi dei dati per i progetti EcoDigit/Anagrafe” presso il Dipartimento di Ingegneria Informatica, Automatica e Gestionale “Antonio Ruberti” dell'Università degli Studi di Roma “La Sapienza”.

(20/03/2019 – 05/06/2019): Ruolo tecnico (area tecnica, tecnico-scientifica ed elaborazione dati), categoria D, posizione economica D1, presso l'Università degli Studi di Roma “La Sapienza”. Dal 01/04/2019 al 05/06/2019 in servizio presso l'Area Supporto Strategico e Comunicazione.

(01/03/2019 – 19/03/2019): Assegno di Ricerca presso il Dipartimento di Ingegneria Informatica, Automatica e Gestionale “Antonio Ruberti” dell'Università degli Studi di Roma “La Sapienza”, relativo al progetto di ricerca “Architetture, tecniche e metodi per l'Anagrafe del distretto Beni Culturali Regione Lazio”.

2014 – 2018:

(01/06/2014 – 31/05/2018): Assegno di ricerca presso il Dipartimento di Fisica dell'Università degli Studi di Roma “La Sapienza”, per l'attività “Supporto VQR”. Sviluppo di software e database per l'analisi e la gestione dei dati previsti dal bando della Valutazione Qualità e Ricerca'.

2013:

(01/03/2013 – 31/10/2013): Contratto di collaborazione coordinata e continuativa per “Progetto e realizzazione sistema per la visualizzazione di reti metaboliche” presso il Dipartimento di Ingegneria Informatica, Automatica e Gestionale “Antonio Ruberti” dell'Università degli Studi di Roma “La Sapienza”.

- Docente a contratto per il corso di “Fondamenti di Informatica” (6 CFU), a.a. 2012/2013, Corso di Laurea in Ingegneria Gestionale, Università degli Studi di Roma “La Sapienza”.

2012:

(01/03/2012 – 30/11/2012): Contratto di collaborazione coordinata e continuativa per “Progetto e sviluppo di software per l'individuazione di proprietà strutturali in ipergrafi rappresentanti reti complesse” presso il Dipartimento di Ingegneria Informatica, Automatica e Gestionale “Antonio Ruberti” dell'Università degli Studi di Roma “La Sapienza”.

2011:

(10/03/2011 – 09/11/2011): Contratto di collaborazione coordinata e continuativa per “Progetto e sviluppo di software per l'individuazione di proprietà strutturali in grafi rappresentanti reti complesse” presso il Dipartimento di Informatica e Sistemistica dell'Università degli Studi di Roma “La Sapienza”.

(10/01/2011 – 18/07/2011): Contratto di collaborazione occasionale per docenza corso IFTS “Tecnico Superiore per le Applicazioni Informatiche” (autorizzato dalla Regione Lazio), modulo “Linguaggi di Programmazione”, presso l'Istituto “G. Meschini” di Roma.

2010:

(01/10/2010 – 31/12/2010): Contratto di collaborazione coordinata e continuativa per “Progetto e sviluppo di una estensione del linguaggio C per la programmazione a vincoli dataflow” presso il Dipartimento di Informatica e Sistemistica dell'Università degli Studi di Roma “La Sapienza”.

- Docente a contratto per il corso di “Fondamenti di Informatica I” (6 CFU), a.a. 2009/2010, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma “La Sapienza”.

- Docente a contratto per il corso di “Fondamenti di Informatica I” (6 CFU), a.a. 2009/2010, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma “La Sapienza” - Sede di Rieti.

- Tutoraggio per il corso di “Basi di Dati”, a.a. 2009/2010, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma “La Sapienza” - Sede di Rieti.

2009:

- Docente a contratto per il corso di “Fondamenti di Informatica I” (6 CFU), a.a. 2008/2009, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma “La Sapienza”.

- Docente a contratto per il corso di “Fondamenti di Informatica I (I modulo)” (6 CFU), a.a. 2008/2009, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma “La Sapienza” - Sede di Rieti.

- Tutoraggio per il corso di “Basi di Dati”, a.a. 2008/2009, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma “La Sapienza” - Sede di Rieti.

2008:

- Docente a contratto per il corso di “Fondamenti di Informatica II” (6 CFU), a.a. 2007/2008, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma “La Sapienza” - Sede di Rieti.

(05/03/2008 – 31/05/2008): Contratto di collaborazione coordinata e continuativa per “Sviluppo e implementazione di algoritmi di data stream per problemi su grafi” presso il Dipartimento di Informatica e Sistemistica dell'Università degli Studi di Roma “La Sapienza”.

- Tutoraggio per il corso di “Fondamenti di Informatica”, a.a. 2007/2008, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma

Curriculum Vitae di **Andrea Ribichini**

“La Sapienza”.

2007:

- Tutoraggio per il corso di “Fondamenti di Informatica”, a.a. 2006/2007, Corso di Laurea in Ingegneria Informatica, Università degli Studi di Roma “La Sapienza”.

2003:

(01/11/2003 – 30/11/2003): Contratto di collaborazione occasionale per “Progettazione e sviluppo del sito Web per il Dottorato di Ricerca in Ingegneria Informatica” presso il Dipartimento di Informatica e Sistemistica dell'Università degli Studi di Roma “La Sapienza”.

(30/01/2003 – 30/04/2003): Contratto di collaborazione occasionale per “Progettazione e sviluppo di una libreria grafica in ambiente Windows” presso il Dipartimento di Informatica e Sistemistica dell'Università degli Studi di Roma “La Sapienza” .

Roma, 23/08/2021