CURRICULUM VITAE ET STUDIORUM

ROBERTO SEGALA

January 2025

Personal Information:

Name: Roberto Segala.

Date of Birth: January 24, 1968, Legnago (VR), Italy.

Current position: Professor of Computer Science (full professor), Department of Computer Science, University of Verona, Italy

Office Address: Dipartimento di Informatica - Università di Verona, Strada Le Grazie 15, 37134 Verona, Italy (Tel. +39 045 8027997, Fax. +39 045 8027982, Mob. +39 328 8606224).

E-mail: `roberto.segala@univr.it` (URL: `http://profs.sci.univr.it/~segala`).

Home Address: Via Oberdan 4, 37040 Legnago (VR) (Tel. +39 0442 26170).

Citizenship: Italy

Education:

1995 Massachussetts Institute of Technology, Cambridge, MA, USA Ph.D. in Electrical Engineering and Computer Science, Thesis Title: Modeling and Verification of Randomized Distributed Real-Time Systems (thesis advisor Prof. Nancy Lynch)

Jun. 92 Massachussetts Institute of Technology, Cambridge, MA, USA Master in Electrical Engineering and Computer Science, Thesis Title: A Process Algebraic view of I/O Automata (thesis advisor Prof. Nancy Lynch).

Jul. 91 Scuola Normale Superiore, Pisa, Italy Diploma in Computer Science.

Jul. 91 Università degli Studi di Pisa, Italy Laurea in Computer Science. Graduated with 110/110 cum laude. Thesis title: Algebre di Processi come Automi con Input e Output (thesis advisor Prof. Rocco De Nicola).

Work Experience

University of Verona - Department of Computer Science
Full Professor since 01/11/05. Teaching duties: Algorithms and Data Sturctures, Cryptography, Security.

University of Verona - Department of Computer Science
Associate Professor from 01/10/01 to 31/10/05. Teaching duties: Algorithms and Data Sturctures, Cryptography, Security.

University of Bologna - Department of Computer Science
Ricercatore: July 1995 - October 2001. Teaching duties: Algorithms and Data Sturctures, Basic Complexity Theory, Cryptography.

Massachusetts Institute of Technology, Cambridge, MA, USA
Research Assistant: September 1991 - August 1995; Teaching Assistant: January 1993 - May 1993; Visiting Scholar: September 1990 - December 1990.

Hewlett Packard Laboratories, Bristol, U.K.
Summer Research Associate: September 1989 - November 1989. Developed a macro notation for the abstract data type language ACT ONE; used the notation to map the language ASN.1 (ISO 8824/CCITT X.208) onto ACT ONE.

IBM Science Center, Rome, Italy
Summer Programmer: October 1988 - November 1988. Developed an editor of vocal spectrum in C to be used for the study of voice synthesis techniques.

Private Consulting, Verona, Italy
Written programs in BASIC, PASCAL and C, and developed simple digital control circuits for small companies in the area of Verona, Italy, 1986 - 1991.

Research Interests:

Semantics of concurrency: Mathematical models for the description of the behavior of concurrent and distributed systems: labeled transition systems, Petri nets, event structures. Languages for the description of processes and their semantics: *interleaving* approach and *truly concurrent* approach.

Models for the specification and verification of concurrent systems: Preorder relations to express notions of implementation: testing preorders, fair preorder, quiescent preorder, failure preorder, simulation relations. Models for specification and verification: state charts, input/output automata, trace structures, temporal logic of actions, process algebras. Study of safety and liveness properties.

Models for the description of timed systems: Timed process algebras, timed automata, hybrid systems, notions of regularity for timed automata. Study and analysis of time deadlocks and Zeno behaviors.

Models for the description of concurrent randomized systems: Study of nondeterminism in probabilistic environments, properties of probabilistic algorithms, schedulers and "adversaries", simulation methods.

Models for the description of hybrid systems: integration of continuous and discrete behaviors,trace semantics, simulation techniques, liveness, receptivity, compositionality. Integration of resutls from control theory.

Verification of concurrent, real-time, randomized systems: Verification of correctness, study of the time complexity of randomized distributed algorithms. Techniques based on traces, invariants, simulations. Modular verification.

Security: Cryptographyc algorithms, payment protocols, authentication protocols, multilevel security. Protocol validation.

Model checking: Model checking techniques for real-time, hybrid and probabilistic systems. BDD technology. Integration with theorem proving.

1 Research Activity

Publications

Thesis Work

[1] "Modeling and Verification of Randomized Distributed and Real-Time Systems" R. Segala, Ph.D. Thesis, Massachusetts Institute of Technology, May 1995. Available as Technical Report number MIT/LCS/TR-676.

[2] "A Process Algebraic view of I/O Automata", R. Segala, Master Thesis, Massachussetts Institute of Technology, June 1992. Available as Technical Report number MIT/LCS/TR-557.

[3] "Algebre di Processi come Automi con Input e Output", R. Segala, tesi di laurea, Dipartimento di Informatica, Università di Pisa, July 1991.

Books

[4] "The Theory of Timed Automata", second edition, D. Kaynar, N. Lynch, R. Segala, F. Vaandrager, Synthesis Lecture on Computer Science, Morgan & Claypool Publishers, 137 pages, 2010.

[5] "The Theory of Timed Automata", D. Kaynar, N. Lynch, R. Segala, F. Vaandrager, Synthesis Lecture on Computer Science, Morgan & Claypool Publishers, 123 pages, April 2006. ISBN 159829010X.

Papers in International Journals

[6] "A computable and compositional semantics for hybrid systems", D. Bresolin, P. Collins, L. Geretti, R. Segala, T. Villa, S. Gonzalez, *Information and Computation*, 300, pages 105–189, 2024.

[7] "Task-structured probabilistic I/O automata", R. Canetti, L. Cheung, D. Kaynar, M. Liskov, N. Lynch, O. Pereira, R. Segala, *Journal of Computer and System Sciences*, 94, pages 63–97, 2018

[8] "Probabilistic Logical Characterization", H. Hermanns, A. Parma, R. Segala, B. Wachter, L. Zhang, *Information and Computation*, 209(2), pages 154–172, 2011.

[9] "A quantitative doxastic logic for probabilistic processes and applications to information-hiding", S. Kramer, C. Palamidessi, R. Segala, A.Turrini, C. Braun, *Journal of Applied Non-classical Logics*, 19(4), pages 489–516, 2009.

[10] "Analyzing Security Protocols Using Time-Bounded Task-PIOAs", Ran Canetti, Ling Cheung, Dilsun Kirli Kaynar, Moses Liskov, Nancy A. Lynch, Olivier Pereira, Roberto Segala, *Discrete Event Dynamic Systems* 18(1), pages 111-159, 2008.

[11] "Observing Branching Structure through Probabilistic Contexts", N. Lynch, R. Segala, F. Vaandrager, in *SIAM Journal on Computing* 37(4), pages 977–1013, 2007.

[12] "Dynamic Load Balancing with Group Communication", S. Dolev, R. Segala, A. Shvartsman, in *Theoretical Computer Science* 369, pages 348–360, 2006. Extended journal version of [53].

[13] Switched PIOA: Parallel Composition via Distributed Scheduling, L. Cheung, N. Lynch, R. Segala, F. Vaandrager, in *Theoretical Computer Science*, 365, pages 83–108, 2006.

[14] "Hybrid I/O Automata", N. Lynch, R. Segala, F. Vaandrager, *Information and Computation*, 185, pages 105–157, 2003. Extended journal version of [49].

[15] "Automatic Verification of Real-Time Systems With Discrete Probability Distributions", M. Kwiatkowska, G. Normann, R. Segala, e J. Sproston, in *Theoretical Computer Science*, 282, pages 101–150, 2002. Extended journal version of [54].

[16] "Verification of the Randomized Consensus Algorithm of Aspnes and Herlihy: a Case Study", A. Pogosyants, R. Segala, e N. Lynch, *Distributed Computing* 13(3), July 2000.

[17] "Liveness in Timed and Untimed Systems", R. Gawlick, R. Segala, J. Søgard Andersen, e N. Lynch, *Information and Computation*, 141(2):119–171, 1998. Extended journal version of [63].

[18] "Quiescence, Fairness, Testing, and the Notion of Implementation", R. Segala, in *Information and Computation*, 138(2):194–210, November 1997. Extended journal version of [65].

[19] "Probabilistic Simulations for Probabilistic Processes", R. Segala and N. Lynch, in *Nordic Journal of Computing*, 2(2):250–273,1995. Journal version of [61] invited by the organizers of CONCUR94.

[20] "A Comparison of Simulation Techniques and Algebraic Techniques for Verifying Concurrent Systems", N. Lynch and R. Segala, in *Formal Aspects of Computing*, 7(3):231–265,1995. Extended journal version of [64].

[21] "A Process Algebraic View of I/O Automata", R. De Nicola and R. Segala, in *Theoretical Computer Science*, 138:231–265, 1995.

Invited Papers

[22] "Time-Bounded Task-PIOAs: A Framework for Analyzing Security Protocols", R. Canetti, L. Cheung, D. Kaynar, M. Liskov, N. Lynch, O. Pereira, R. Segala, in Proceedings of the 20th International Symposium on Distributed Computing (DISC '06), Stockholm, Sweden, LNCS 4167, pages 238-253, September 2006.

[23] "Probability and Nondeterminism in Operational Models of Concurrency", R. Segala, in Proceedings of the 17th International Conference on Concurrency Theory (CONCUR '06), Bonn, Germany, LNCS 4137, pages 64-78, August 2006.

[24] "Verification of Probabilistic Distributed Algorithms", R. Segala, invited paper on an LNCS volume about FMPA 2000 (Formal Methods and Performance Analysis, Euro Summer School on Trends in Computer Science), LNCS 2090, pages 232–260, 2001.

[25] "The Essence of Coin Lemmas", R. Segala, *Workshop on Probabilistic Methods in Verification* (PROBMIV), Indianapolis, USA, June 1998. A revised paper appears on ENTCS, volume 22, selected papers from PROBMIV.

[26] "Compositional Verification of Randomized Distributed Algorithms", R. Segala, in *Proceedings of Compositionality: The Significant Difference*, Malente/Holstein, Germany, LNCS 1536, pages 515–540, September 1997.

[27] "Verification of the Randomized Consensus Algorithm of Aspnes and Herlihy: a Case Study", A. Pogosyants, R. Segala, and N. Lynch, in *Proceedings of the Workshop on Distributed Algorithms (WDAG)*, Saarbrücken, Germany, LNCS 1320, pages 22–36, September 1997.

Papers in Proceedings of International Conferences

[28] "Recent Results on Computable and Compositional Semantics for Hybrid Systems", D. Bresolin, P. Collins, L. Geretti, R. Segala, T. Villa, *OVERLAY 2024*, pages 23–29, 2024.

[29] "A computable and compositional semantics for hybrid automata", D. Bresolin, P. Collins, L. Geretti, R. Segala, T. Villa, S. Zivanovic Gonzalez, *Proceedings of Hybrid Systems, Computation and Control*, pagine 1–11, 2020.

[30] "Random Measurable Selections", J. Goubault-Larrecq, R. Segala, *Horizons of the Mind. A Tribute to Prakash Panangaden - Essays Dedicated to Prakash Panangaden on the Occasion of His 60th Birthday*, pages 343–362 2014.

[31] "World Automata: a compositional approach to model implicit communication in hierarchical Hybrid Systems", M. Capiluppi, R. Segala, *Procedings of HAS*, pages 58–72, 2013.

[32] "Modelling Implicit Communication in Multi-Agent Systems with Hybrid Input/Output Automata", M. Capiluppi, R. Segala, *Proceedings of GandALF*, pages 1–14, 2112.

[33] "Reasoning about Probabilistic Security Using Task-PIOAs", A. Jaggard, C. Meadows, M. Mislove, R. Segala, *Proceedings of ARSPA-WITS*, pagine 2-22, 2010.

[34] "Conditional Automata: A Tool for Safe Removal of Negligible Events", R. Segala, A. Turrini, *Proceedings of CONCUR 2010*, pages 539-553, 2010.

[35] "Approximated Computationally Bounded Simulation Relations for Probabilistic Automata", R. Segala, A. Turrini, *Proceedings of the 20th IEEE Computer Security Foundations Symposium*, Venice, pages 140-156, July 2007.

[36] "Logical Characterizations of Bisimulations for Discrete Probabilistic Systems", A. Parma, R. Segala, *Proceedings of the 10th International Conference on Foundations of Software Science and Computational Structures (FOSSACS)*, Braga, Portugal, LNCS 4423, pages 287-301, April 2007.

[37] "Task-Structured Probabilistic I/O Automata", R. Canetti, L. Cheung, D. Kaynar, M. Liskov, N. Lynch, O. Pereira, R. Segala, in *Proceedings the 8th International Workshop on Discrete Event Systems (WODES'06)*, Ann Arbor, Michigan, July 2006.

[38] "Using Task-Structured Probabilistic I/O Automata to Analyze Cryptographic Protocols", R. Canetti, L. Cheung, D. Kaynar, M. Liskov, N. Lynch, O. Pereira, R. Segala, in *Proceedings of the Workshop on Formal and Computational Cryptography (FCC '06)*, pages 34–39, July 2006.

[39] "Comparative Analysis of Bisimulation Relations on Alternating and Non-Alternating Probabilistic Models", R. Segala, A. Turrini, in *Proceedings of the Second International Conference on the Quantitative Evaluation of Systems (QEST) 2005*, Torino, Italy, pages 44–53, September 2005.

[40] "Stochastic Transition Systems for Continuous State Spaces and Nondeterminism", S. Cattani, M. Kwiatkowska, G. Norman, R. Segala, in *Proceedings of the 8th International Conference on Foundations of Software Science and Computational Structures (FOSSACS)*, Edinburgh, UK, LNCS 3441, pages 125–139, April 2005.

[41] "Axiomatization of Trace Semantics for Stochastic Nondeterministic Processes", A. Parma e R. Segala, in *Proceedings of the First International Conference on Quantitative Evaluation of SysTems (QEST), Twente, The Netherlands*, pages 294–303, September 2004.

[42] "Switched Probabilistic Automata", L. Cheung, N. Lynch, R. Segala, F. Vaandrager, in *Proceedings of the First International Colloquium on Theoretical Aspects of Computing (ICTAC), Guiyang, China*, September 2004.

[43] "A Framework for Modeling Timed Systems with Restricted Hybrid Automata", D. K. Kaynar, N. Lynch, R. Segala, e F. Vaandrager, in *RTSS 2003: The 24th IEEE International Real-Time Systems Symposium, Cancun, Messico*, pages 166–177, December, 2003.

[44] "Compositionality for Probabilistic Automata", N. Lynch, R. Segala e F. Vaandrager, in *Proceedings of CONCUR 03*, LNCS 2761, pages 208–221, September 2003.

[45] "Decision Algorithms for Probabilistic Bisimulation", S. Cattani, R. Segala, in *Proceedings of CONCUR02*, LNCS 2421, pages 371–385, August 2002.

[46] "Coin Lemmas with Random Variables", K. Folegati and R. Segala, in *Proceedings of PAPM/PROBMIV 2001*, Aachen, Germany, LNCS2165, pages 71–86, September 2001.

[47] "Automated Verification of a Randomized Distributed Consensus Protocol Using Cadence SMV and PRISM", M. Kwiatkowska, G. Norman, and R. Segala, in *Proceedings of CAV 2001*, Paris, France, LNCS 2102, pages 194–206, July 2001.

[48] "Axiomatizations for Probabilistic Bisimulation", E. Bandini and R. Segala, in *Proceedings of ICALP 2001*, Crete, Grece, LNCS 2076, pages 370–381, July 2001.

[49] "Hybrid I/O Automata Revisited", N. Lynch, R. Segala, F. Vaandrager, in *Proceedings of Hybrid Systems: Computation and Control*, Rome, LNCS 2034, pages 403–417, March 2001.

[50] "Verifying Quantitative Properties of Continuous Probabilistic Real-Time Graphs", M. Kwiatkowska, G. Normann, R. Segala, and J. Sproston, in *Proceedings di CONCUR*, LNCS 1877, pages 123–137, August 2000.

[51] "Verifying Soft Deadlines with Probabilistic Timed Automata" di M. Kwiatkowska, G. Normann, R. Segala, e J. Sproston, in *Proceedings di WAVe00*, Giugno 2000.

[52] "Symbolic Model Checking of Concurrent Probabilistic Processes Using MTBDDs and the Kronecker Representation", L. de Alfaro, M. Kwiatkowska, G. Norman, D. Parker and R. Segala, in Proceedings di TACAS 2000, Berlin, LNCS 1785, April 2000.

[53] , "Dynamic Load Balancing with Group Communication", S. Dolev, R. Segala, and A. Shvartsman, in Proceedings di International Colloquium on Structural Information and Communication Complexity (SIROCCO), Lacanau, France, pages 111-125, July 1999.

[54] "Automatic Verification of Real-Time Systems With Discrete Probability Distributions", M. Kwiatkowska, G. Normann, R. Segala, and J. Sproston, in Proceedings di 5^{th} international AMAST Workshop on Real-Time and Probabilistic Systems (ARTS '99), LNCS 1601, pages 79–95, May 1999.

[55] "Hybrid I/O Automata for the Compositional Analysis of Hybrid Systems", *International Symposium on Mathematical Tehory of Networks and Systems* (MTNS98), Padova, July 1998.

[56] "System Support for Partition-Aware Network Applications", O. Babaoglu, R. Davoli, A. Montresor and R. Segala, in Proceedings of the 18th International Conference on Distributed Computing Systems (ICDCS '98), pagine 184–191, Amsterdam, The Netherlands, May 1998.

[57] "Testing Probabilistic Automata", R. Segala, in Proceedings of CONCUR96, Pisa, Italy, LNCS 1119, pages 299–314, 1996.

[58] "Hybrid I/O Automata", N. Lynch, R. Segala, F. Vaandrager, H.B. Weinberg, in *Hynrid Systems III*, LNCS 1066, pages 496–510, October 1996.

[59] "A Compositional Trace-Based Semantics for Probabilistic Automata", in proceedings of CONCUR95, Philadelphia, PA, USA, LNCS 962, pages 234-248, 1995.

[60] "Formal Verification of Timed Properties of Randomized Distributed Algorithms", A. Pogosyants, R. Segala, in proceedings of PODC95, Ottawa, Ontario, Canada, pages 174–183, 1995.

[61] "Probabilistic Simulations for Probabilistic Processes", R. Segala and N. Lynch, Proceedings of CONCUR94, Uppsala, Sweden, LNCS 836, 1994.

[62] "Proving Time Bounds for Randomized Distributed Algorithms", N. Lynch, I. Saias, and R. Segala, Proceedings of PODC94, Los Angeles, CA, 1994.

[63] "Liveness in Timed and Untimed Systems", R. Gawlick, R. Segala, J. Søgaard Andersen, and N. Lynch, Proceedings of ICALP94, Jerusalem, Israel, LNCS 820, 1994. A full version appears as technical report number MIT/LCS/TR-587.

[64] "A Comparison of Simulation Techniques and Algebraic Techniques for Verifying Concurrent Systems", N. Lynch and R. Segala, Proceedings del Second North American Process Algebra Workshop, Cornell University, NY, 1993

[65] "Quiescence, Fairness, Testing and the notion of Implementation", R. Segala, Proceedings of CONCUR93, Hildesheim, Germany, LNCS 715, 1993.

2 Invitations

Invited Lecturer at International Schools

- *10th International School on Formal Methods for the Design of Computer, Communication and Software Systems: Quantitative Aspects of Programming Languages*, Bertinoro, Italia, Giugno 2010.
- *International School on Foundations of Security Analysis and Design*, Bertinoro, Italy, September 2007. Title of lecture: "Quantitative Analysis in Security".
- *Spring School on Security*, Marseille, France, April 2005. Title of lecture: "Analysis of randomized protocols and applications to security."
- *International School on Foundations of Security Analysis and Design*, Bertinoro, Italy, September 2001. Title of lecture: "Applied Cryptography".
- *International School on Foundations of Security Analysis and Design*, Bertinoro, Italy, September 2000. Title of lecture: "Applied Cryptography".
- *EEF summerschool on Formal Methods and Performance Analysis*, Nijmegen, The Netherlands, July 2000. Title of lecture: "Verification of Probabilistic Distributed Algorithms".

Invited Tutorials

- *17th International Conference on Concurrency Theory (CONCUR 2006)*, Bonn, Germany. Title of tutorial: "Probability and Nondeterminism in Operational Models of Concurrency".
- *Workshop on Probabilistic Methods in Verification, Achen, Germany, September 2001.* Title of tutorial: "Nondeterminism in probabilistic verification".

Invited Talks

- *Workshop on Computational and Symbolic Proofs of Security*, Atagawa, Japan, April 2009. Title of talk: "On the use of Probabilistic Automata for Security Proofs".
- *Workshop on Automata and Verification*, Mons, Belgium, August 2008. Title of talk: "Verification with Probabilistic Automata".
- *Nancy Lynch Celebration*, Toronto, August 2008. Title of talk: "The power of Simulation Relations".
- *VERAP - Approximate Verification of Probabilistic Systems*, project workshop, Paris, November 2007. Title of talk: "Computationally Bounded Approximated Simulation Relations".
- *5th Workshop on Quantitative Aspects of Programming Languages(QAPL 2007)*, Braga, Portugal, April 2007. Title of talk: "Nondeterminism in Quantitative Analysis of Probabilistic Systems".
- *Alpine Verification Meeting*, Lausanne, October 2005. Title of talk: "Modelling Stochastic Nondeterministic Systems: the challenge of continuous measures".
- *Probabilities and Artificial Intelligence Workshop*, Barbados, April 2004. Title of talk: Axiomatizations for Probabilistic Automata.

- *Workshop on Mathematical Models of Systems, Montreal, Canada, October 2002.* Title of talk: "Models for Discrete Nondeterministic Stochastic Systems".
- *Workshop on Probabilistic Methods in Verification, Indianapolis, USA, June 1998.* Title of talk: "The Essence of Coin Lemmas".
- *Compositionality - The Significant Difference, Malente/Holstein, Germany, September 1997.* Title of talk: "Compositional Verification of Randomized Distributed Systems".
- *Workshop on Distributed Algorithms (WDAG), Saarbrücken, Germany, September 1997.* Title of talk: "Verification of the Randomized Consensus Algorithm of Aspnes and Herlihy: a Case Study".

Invitations to Panel Sessions

- *19th IEEE Computer Security Foundations Workshop (CSFW 2006)*, Venice, Italy, July 2006. Argument: "Nondeterminism in Security Modeling".

Other Invitations

- Invited to *Dagstuhl meeting on Quantitative Models: Expressiveness and Analysis*, Germany, January 2010.
- Invited Observer to *IFIP WG 2.2 meeting*, Torino, September 2008. Declined due to conflicting events.
- Invitato to DIMACS, Rutger University, NJ, USA, April 2008.
- Visiting Professor *École Normale Supérieure Cachan*, France, May 2008.
- Invited to the workshop *Two Decades of Probabilistic Verification: Reflections and Perspectives*, Lorentz Center, Leiden, The Netherlands, November 2007.
- Invited Observer to *IFIP WG 2.2 meeting*, Nancy, France, September 2007. Declined due to conflicting events.
- Visiting Professor, *Ecole Normale Superieure Cachan*, France, June 2007.
- Visiting Professor, *NTT Labs, Yokosuka*, Japan, May 2007.
- Invited to *LIX Colloquium on Emerging Trends in Concurrency Theory*, Paris, November 2006.
- Invited Observer to *IFIP WG 2.2 meeting*, Skagen, Denmark, September 2005. Declined due to conflicting events.
- Invited to the workshop on 25 years of Process Algebras, Bertinoro, Italy, August 2005.
- Invited Observer to *IFIP WG 2.2 meeting*, Bertinoro, Italy, September 2004.
- Invited to *Dagstuhl meeting on Probabilistic Methods in Verification and Planning*, Germany, May 2003.
- Invited Observer to *IFIP WG 2.2 meeting*, Amsterdam, The Netherlands, May 2003. Declined due to conflicting events.
- Invited Observer to *IFIP WG 2.2 meeting*, Oldenburg, Germany, September 2002.

- Invited to *Dagstuhl meeting on Probabilistic Methods in Verification*, Germany, May 2000.
- Invited to several research institutes for seminars about the research activity.

3 Professional Scientific Activities

Steering Committees

- Elected member of the steering committee of QEST from 2003 to 2007.
- Member of the steering committee of PROBMIV from 1999 to 2004.

Program Committees

- *Tenth International Conference on Quantitative Evaluation of SysTems (QEST)*, Cordoba, Argentina, 2013.
- *Int. Coll. on Automata, Languages, Programming (ICALP)*, Zürich, Switzerland, 2011.
- *Seventh International Conference on Quantitative Evaluation of SysTems (QEST)*, USA, 2010. (PC co-chair).
- *Formal Methods for Aerospace*, Eindhoven, The Netherlands, November 2009.
- 16th workshop Expressiveness in Concurrency (EXPRESS), Bologna, Italy, September 2009.
- *Sixth International Conference on Quantitative Evaluation of SysTems (QEST)*, Budapest, Hungary, 2009.
- *Fifth International Conference on Quantitative Evaluation of SysTems (QEST)*, Saint Malo, France, 2008.
- *14th International Workshop on Expressiveness in Concurrency (EXPRESS)*, Lisbon, Portugal, 2007.
- *Fourth International Conference on Quantitative Evaluation of SysTems (QEST)*, (tutorial chair), Edinburgh, UK, 2007.
- *International Conference on Quantitative Evaluation of SysTems (QEST 2006)*, Riverside, CA, USA.
- *22nd Conference on the Mathematical Foundations of Programming Semantics (MFPS 2006)*, Genova, Italy.
- *Workshop on Quantitative Aspects of Programming Languages (QAPL 2006)*, Vienna, Austria.
- *Int. Conf. on Quantitative Evaluation of SysTems (QEST)*, Torino, 2005.
- *21st Conference on the Mathematical Foundations of Programming Semantics (MFPS)*, Birmingham, 2005.
- *Int. Coll. on Automata, Languages, Programming (ICALP)*, Lisboa, 2005.
- *Work. on Quant. Aspects of Programming Languages (QAPL)*, Edinburgh, 2005.
- *Work. on Foundations of Global Ubiquitous Computing*, London, 2004.
- *Int. Conf. on Quantitative Evaluation of SysTems (QEST)*, Twente, 2004.
- *Work. on Quant. Aspects of Programming Languages (QAPL)*, Barcelona, 2004.
- *Int. Conf. on Principles of Distributed Computing (PODC)*, Boston, 2003.

- *Int. Conf. on Concurrency Theory (CONCUR)*, Marseille, 2003.
- *Workshop on Process Algebra and Performance Modelling, Probabilistic Methods in Verification (PAPM/PROBMIV)*, 2002 (chair).
- *International Conference on Distributed Computing Systems*, 2002.
- *Workshop on Process Algebra and Performance Modelling, Probabilistic Methods in Verification (PAPM/PROBMIV)*, 2001.
- *International Workshop on Expressiveness in Concurrency (Express)*, 2001.
- *Hybrid Systems: Computation and Control*, Rome, 2001.
- *Third Workshop on Probabilistic Methods in Verification (PROBMIV)*, 2001.
- *Hybrid Systems: Computation and Control*, 2000.
- *Second Workshop on Probabilistic Methods in Verification (PROBMIV)*, 1999.
- 5^{th} *International AMAST Workshop on Real-Time and Probabilistic Systems*, 1999.
- *Workshop on Probabilistic Methods in Verification (PROBMIV)*, 1998.
- *Hybrid Systems: Computation and Control*, 1998.
- *Workshop on Distributed Algorithms (WDAG)*, 1996.

Editorial Boards

- Member of the editorial board of *Information and Computation* since 2011.
- Member of the editorial board of *Int. Journal of Hybrid Systems* from 2001 to 2011.

External Member in PhD Thesis Committees

- Martin Neuhäusser: "Model Checking Nondeterministic and Randomly Timed Systems", Advisor Joost/Pieter Katoen, University of Twente, The Netherlands, January 2010.
- Daniele Magazzeni: "Explicit Model Checking Techniques Applied to Control and Planning Problems", Advisor Giuseppe Della Penna, Università degli Studi dell'Aquila, December 2008.
- Lijun Zhang: "Decision Algorithms for Probabilistic Simulations", Advisor Holger Hermanns, Universität des Saarlandes, Germany, December 2008.
- Elie Bursztein: "Anticipation games. Game theory applied to network security", Advisor Jean Goubault-Larrecq, Ecole Normale Superieure, Cachan, France, November 2008.
- Yuxin Deng: "Axiomatisations and Types for Probabilistic and Mobile Processes", Advisor Catuscia Palamidessi, INRIA, Paris, July 2005.
- Marielle Stoelinga: "Verification of Probabilistic Real-Time and Parametric Systems", Advisor Frits Vaandrager, University of Nijmegen, April 2002.
- Sue-Hwey Wu: "Compositional Behaviors of Probabilistic I/O Automata", Advisors S. Smolka e E. Stark, Stony Brook, NY, April 1996.

Reviews of Scientific Papers

Reviewer several international conferences and journals, including Acta Informatica, ACM Transactions on Programming Languages and Systems, Distributed Computing, IEEE Transactions on Software Engineering, Information and Computation, Journal of the Association of Computing Machinery, Journal of Parallel and Distributed Computing, Theoretical Computer Science.

4 Teaching Activity

Courses

University of Verona

- *Algorithms and Data Structures* (96 hours), since 2009.
- *Security and Cryptography* (48 hours), since 2009.
- *Model Checking* (20 hours, PhD level), 2004, 2008.
- *Algorithms and Data Structures* (64 hours), from 2001 to 2009.
- *Security and Cryptography* (40 hours), from 2001 to 2009.
- *Basic Computer Science* (62 hours), from 2003 to 2007.
- *Laboratory of Algorithms and Data Structures* (24 hours), from 2002 to 2005.
- *Operating Systems* (108 hours), 2000/01.

University of Bologna

- *Algorithms and Data Structures* (80 hours), from 1995 to 2001.
- *Cryptography* (40 hours), from 1998 to 2001.

Massachussetts Institute of Technology

- *Theory of Computation*, assistant, 1993.

Thesis Supervision

Advisor for several laurea and laurea magistralis theses. Advisor for the following Master and PhD students.

- "Measures on Probabilistic Automata", Federica Panarotto, PhD thesis, Department of Computer Science, University of Verona, (advisor R. Segala), 2017.
- "Hierarchical and Compositional Verification of Cryptographic Protocols", Andrea Turrini, PhD thesis, Department of Computer Science, University of Verona, (advisor R. Segala), 2008.
- "Axiomatic and Logical Characterizations of Probabilistic Preorders and Trace Semantics", Augusto Parma, PhD thesis, Department of Computer Science, University of Verona, (advisor R. Segala), 2008.
- "The Complexity of Randomized Distributed Algorithms", A. Pogosyants, PhD thesis, Massachusetts Institute of Technology, (advisors: N. Lynch e R. Segala).
- "Time Optimal Self-Stabilizing Spanning Tree Algorithms", S. Aggarwal, Master thesis, Massachusetts Institute of Technology, (advisors: N. Lynch, S. Kutten, R. Segala), June 1994.

5 Professional Administrative Activities

Administrative Activities for the University

- Chair of the Computer Engineering Degrees from 2009 to 2013 and from 2018 to 2021, University of Verona. Duties include keeping contacts with external industries and organizations to ensure consistency between the study programme and the needs of the surrounding environment.
- Delegate of the Rector for student advisory (2006-2013), e-learning since (2007-2013), life-long learning since (2010-2013). Duties include coordination of the office for advising students on their plans of study and their subsequent career after graduation, keeping contacts with external institutions (public regional offices, industries, labor organizations, professional register organizations) to facilitate continuity between study and work, and to enhance collaboration aimed at the creation of advanced study and continuous professional education programs.
- Chair of the PhD program in Computer Science from 2006 to 2009, University of Verona.
- Vice-chair of the Department of Computer Science since 2007, University of Verona.
- Member of the Administrative Council of UNIONLINE (Consorzio delle università del triveneto per la formazione a distanza) from 2008 to 2011.
- Member of the Administrative Council of COSP (Comitato Provinciale Orientamento Scolastico Professionale) since 2006.
- Chair of the project of the University of Verona for teaching basic computer science to students from other disciplines since 2001.
- Vice-chair for Computer Science courses and chair of the teaching committee from 2002 to 2006, University of Verona.

Organization of Events

- Co-organizer of the PAPM-ProbMIV workshop, Copenhagen, Denmark, 2002.
- Vice-chair of the organizing committee of ICALP '96, Bologna, Italy.

6 Research Projects

- *Security Horizons* (2013-2016), PRIN project on verification of network system security coordinated by Pisa.
- *Modelli e tecniche di analisi formale per la sicurezza dei sistemi software* (2008-2009), PRIN project on network system security coordinated by Venice.
- *C4C* (2007-2009), EU project on coordination for control coordinated by CWI, The Netherlands.
- *ProNoBiS: Probability and Nondeterminism, Bisimulations and Security* (2006-2007), INRIA project involving ENS Cachan, INRIA Futurs, Queen Mary University, Universit Paris 7, Universit di Verona, University of Birmingham.
- *AIDA Abstract Interpretation Design and Applications* (2005-2007), MIUR COFIN project involving Bologna, Padova, Parma, Pisa, Udine, Venezia, Verona (coordinator).

- *Automated Verification of Probabilistic Protocols with PRISM* (2003-2006), visiting fellow, EPSRC project, University of Birmingham.
- *(SPY-Mod) Abstract interpretation and model checking for the verification of embedded systems* (2003-2005) Basic Research project involving the Universities of Padova (coordinator), Venezia, Verona.
- *CoVer: Constraint-based Verification of Reactive systems* (2002-2004) MURST involving the Universities of Bologna (coordinator), Genova, Padova, Parma, Udine, Verona, CNR-IEI-CNUCE Pisa.
- *Mefisto* - MURST (2001 - 2003).
- *Tosca* - MURST project (1999 - 2001). Task leader for hybrid systems.
- *Automatic Verification of Randomized Distributed Algorithms* (1998-2001), visiting fellow, EPSRC project, University of Birmingham.