

CURRICULUM SCIENTIFICO E DIDATTICO

ROBERTO SEGALA

Gennaio 2025

Dati Personali:

Nome: Roberto Segala.

Data di nascita: 24 Gennaio 1968, in Legnago (VR).

Recapito: Dipartimento di Informatica, Università di Verona, Strada Le Grazie 15,
37134 Verona.

Telefono: 045 8027997 - 328 8606224.

Fax: 045 8027982.

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

Residenza: Via Oberdan 4, 37040 Vangadizza di Legnago (VR) (tel. 0442-26170).

Titoli:

Mag. 95 PhD in Electrical Engineering and Computer Science, presso il Massachusetts Institute of Technology, Cambridge, MA, USA. Titolo della tesi: Modeling and Verification of Randomized Distributed Real-Time Systems (relatore Prof. Nancy Lynch, controrelatori Proff. Butler Lampson e Albert Meyer).

Giu. 92 Master in Electrical Engineering and Computer Science, presso il Massachusetts Institute of Technology, Cambridge, MA, USA. Titolo della tesi: A Process Algebraic view of I/O Automata (relatore Prof. Nancy Lynch).

Lug. 91 Diploma ordinario in Scienze dell'Informazione presso la Scuola Normale Superiore di Pisa.

Lug. 91 Laurea in Scienze dell'Informazione, presso l'Università degli Studi di Pisa. Voto di Laurea: 110/110 e lode. Titolo della Tesi: Algebre di Processi come Automi con Input e Output (relatore Prof. Rocco De Nicola, controrelatore Prof. Maggiolo A. Schettini).

Posizioni di lavoro:**Università di Verona - Dip. di Informatica**

Professore Ordinario dal 01/11/2005. Titolare del corso di Algoritmi (laurea in Informatica) e del corso di Crittografia (laurea magistrale in Ingegneria e Scienze Informatiche).

Università di Verona - Dip. di Informatica

Professore Associato dal 01/10/2001 al 31/10/2005. Titolare del corso di Algoritmi e Strutture Dati e del corso di Sicurezza e Crittografia.

Università di Bologna - Dip. di Scienze dell'Informazione

Ricercatore dal 01/07/1995 al 30/09/2001. Assistente del corso di Algoritmi e Strutture Dati negli anni 1995/96/97/98. Titolare del corso di Algoritmi e Strutture Dati e del corso di Crittografia negli anni 1998/99/00/01.

Massachusetts Institute of Technology, Boston, MA - USA

Research assistant dal 01/09/1991 al 30/06/1995; Teaching assistant dal 15/01/1993 al 31/05/1993; visiting scholar dal 12/09/1990 al 13/12/1990.

Hewlett Packard Laboratories, Bristol - UK dal 28/08/1989 al 28/10/1989.

Stage estivo. Il lavoro é consistito nel dare una semantica al linguaggio di specifica ASN.1 in termini del linguaggio algebrico ACT ONE.

Centro Scientifico IBM, Roma 10/1988 - 11/1988.

Stage estivo. Sviluppo in C di un editor di spettro vocale.

Aree di Ricerca:

Semantica dei linguaggi per la programmazione concorrente: Modelli matematici per descrivere il comportamento di sistemi concorrenti e distribuiti: sistemi di transizione, reti di Petri, strutture di eventi. Linguaggi per la descrizione di processi e loro semantica: approccio *interleaving* e *truly concurrent*.

Modelli per la specifica e verifica di sistemi concorrenti: Relazioni di preordine, simulazioni e bisimulazioni, state charts, Input/Output automata, trace structures, temporal logic of actions, process algebra. Studio di safety e liveness.

Modelli per la descrizione di sistemi real-time: Process algebra con nozione di tempo, timed automata, sistemi ibridi, nozioni di regolarità in timed automata. Studio ed analisi di fenomeni quali time deadlock e Zeno behavior.

Modelli per la descrizione di algoritmi concorrenti probabilistici: Studio del nondeterminismo in ambienti probabilistici, proprietà di algoritmi probabilistici, metodi di simulazione, metodi basati su tracce e testing.

Modelli per la descrizione di sistemi ibridi: integrazione di comportamenti continui e discreti, semantiche a tracce, tecniche di simulazione, gestione della liveness, recettività, composizionalità. Integrazione con la teoria dei controlli.

Verifica di algoritmi concorrenti probabilistici: verifica di correttezza, studio della complessità temporale di un algoritmo concorrente probabilistico. Tecniche basate su invarianti, simulazione, astrazione. Tecniche modulari.

Sicurezza: algoritmi crittografici, pagamenti elettronici, protocolli di autenticazione, multilevel security. Verifica di protocolli. Modelli simbolici e computazionali.

Model checking: algoritmi e tecniche di model checking per sistemi real-time, ibridi, e probabilistici. Studio di tecniche basate su BDD, OBDD, MTBDD. Studio di tecniche basate su riduzione a mathematical programming. Integrazione tra theorem proving e model checking.

Pubblicazioni

Lavori di Tesi

- [1] “Modeling and Verification of Randomized Distributed Real-Time Systems” di R. Segala, tesi di Ph.D., Massachusetts Institute of Technology, Maggio 1995. Disponibile come technical report numero MIT/LCS/TR-676.
- [2] “A Process Algebraic view of I/O Automata”, di R. Segala, tesi di Master, Massachusetts Institute of Technology, Giugno 1992. Disponibile come technical report numero MIT/LCS/TR-557.
- [3] “Algebre di Processi come Automi con Input e Output”, di R. Segala, tesi di laurea, Dipartimento di Informatica, Università di Pisa, Luglio 1991.

Libri

- [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 pagine, 2010.
- [5] “The Theory of Timed Automata”, D. Kaynar, N. Lynch, R. Segala, F. Vaandrager, Synthesis Lecture on Computer Science, Morgan & Claypool Publishers, 123 pagine, Aprile 2006. ISBN 159829010X.

Articoli su Riviste Internazionali

- [6] “A computable and compositional semantics for hybrid systems”, di D. Bresolin, P. Collins, L. Geretti, R. Segala, T. Villa, S. Gonzalez, *Information and Computation*, 300, pagine 105–189, 2024.
- [7] “Task-structured probabilistic I/O automata”, di R. Canetti, L. Cheung, D. Kaynar, M. Liskov, N. Lynch, O. Pereira, R. Segala, *Journal of Computer and System Sciences*, 94, pagine 63–97, 2018
- [8] “Probabilistic Logical Characterization”, di H. Hermanns, A. Parma, R. Segala, B. Wachter, L. Zhang, *Information and Computation*, 209(2), pagine 154–172, 2011.
- [9] “A quantitative doxastic logic for probabilistic processes and applications to information-hiding”, di S. Kramer, C. Palamidessi, R. Segala, A. Turrini, C. Braun, *Journal of Applied Non-classical Logics*, 19(4), pagine 489–516, 2009.
- [10] “Analyzing Security Protocols Using Time-Bounded Task-PIOAs”, di Ran Canetti, Ling Cheung, Dilsun Kirli Kaynar, Moses Liskov, Nancy A. Lynch, Olivier Pereira, Roberto Segala, *Discrete Event Dynamic Systems* 18(1), pagine 111–159, 2008.
- [11] “Observing Branching Structure through Probabilistic Contexts”, N. Lynch, R. Segala, F. Vaandrager, *SIAM Journal on Computing* 37(4), pagine 977–1013, 2007.
- [12] “Dynamic Load Balancing with Group Communication”, di S. Dolev, R. Segala, e A. Shvartsman, *Theoretical Computer Science* 369, pagine 348–360, 2006. Versione estesa per rivista di [55].

- [13] Switched PIOA: Parallel Composition via Distributed Scheduling, L. Cheung, N. Lynch, R. Segala, F. Vaandrager, *Theoretical Computer Science* 365, pagine 83–108, 2006.
- [14] “Hybrid I/O Automata”, di N. Lynch, R. Segala, F. Vaandrager, *Information and Computation*, 185, pagine 105–157, 2003. Versione estesa per rivista di [50].
- [15] “Automatic Verification of Real-Time Systems With Discrete Probability Distributions”, di M. Kwiatkowska, G. Normann, R. Segala, e J. Sproston, *Theoretical Computer Science* 282, pagine 101–150, 2002. Versione estesa per rivista di [56].
- [16] “Verification of the Randomized Consensus Algorithm of Aspnes and Herlihy: a Case Study”, di A. Pogosyants, R. Segala, e N. Lynch, *Distributed Computing* 13(3):155–186, Luglio 2000.
- [17] “Liveness in Timed and Untimed Systems”, di R. Gawlick, R. Segala, J. Søgard Andersen, e N. Lynch, *Information and Computation*, 141(2):119–171, 1998. Versione estesa per rivista di [64].
- [18] “Quiescence, Fairness, Testing, and the Notion of Implementation”, di R. Segala, in *Information and Computation*, 138(2):194–210, Novembre 1997. Versione estesa per rivista di [66].
- [19] “Probabilistic Simulations for Probabilistic Processes”, di R. Segala e N. Lynch, in *Nordic Journal of Computing*, 2(2):250–273, 1995. Versione per rivista di [62] su invito degli organizzatori di CONCUR94.
- [20] “A Comparison of Simulation Techniques and Algebraic Techniques for Verifying Concurrent Systems”, di N. Lynch e R. Segala, in *Formal Aspects of Computing*, 7(3):231–265, 1995. Versione estesa per rivista di [65].
- [21] “A Process Algebraic View of I/O Automata”, di R. De Nicola e R. Segala, in *Theoretical Computer Science*, 138:391–423, 1995.

Articoli Invitati

- [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, pagine 238–253, Settembre 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, pagine 64–78, Agosto 2006.
- [24] “Verification of Probabilistic Distributed Algorithms”, di R. Segala, articolo invitato relativo ai corsi di FMFA 2000 (Formal Methods and Performance Analysis, Euro Summer School on Trends in Computer Science), LNCS 2090, pagine 232–260, 2001.
- [25] “The Essence of Coin Lemmas”, di R. Segala, articolo invitato al *Workshop on Probabilistic Methods in Verification* (PROBMIV), Indianapolis, USA, Giugno 1998. Una revisione dell’articolo appare sul volume 22 di ENTCS, articoli selezionati da PROBMIV.
- [26] “Hybrid I/O Automata for the Compositional Analysis of Hybrid Systems”, di R. Segala, articolo invitato ad una sessione speciale su Hybrid Systems del *International Symposium on Mathematical Theory of Networks and Systems* (MTNS98), Padova, Luglio 1998.

- [27] “Compositional Verification of Randomized Distributed Algorithms”, di R. Segala, in *Proceedings of Compositionality: The Significant Difference*, Malente/Holstein, Germania, LNCS 1536, pagine 515–540, Settembre 1997.
- [28] “Verification of the Randomized Consensus Algorithm of Aspnes and Herlihy: a Case Study”, di A. Pogosyants, R. Segala, e N. Lynch, in *Proceedings of the Workshop on Distributed Algorithms (WDAG)*, Saarbrücken, Germania, LNCS 1320, pagine 22–36, Settembre 1997.

Articoli su Atti di Conferenze Internazionali – con revisione

- [29] “Recent Results on Computable and Compositional Semantics for Hybrid Systems”, di D. Bresolin, P. Collins, L. Geretti, R. Segala, T. Villa, *OVERLAY 2024*, pagine 23–29, 2024.
- [30] “A computable and compositional semantics for hybrid automata”, di D. Bresolin, P. Collins, L. Geretti, R. Segala, T. Villa, S. Zivanovic Gonzalez, *Proceedings of Hybrid Systems, Computation and Control*, pagine 1–11, 2020.
- [31] “Random Measurable Selections”, di 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*, pagine 343–362 2014.
- [32] “World Automata: a compositional approach to model implicit communication in hierarchical Hybrid Systems”, di M. Capiluppi, R. Segala, *Proceedings of HAS*, pagine 58–72, 2013.
- [33] “Modelling Implicit Communication in Multi-Agent Systems with Hybrid Input/Output Automata”, di M. Capiluppi, R. Segala, *Proceedings of GandALF*, pagine 1–14, 2112.
- [34] “Reasoning about Probabilistic Security Using Task-PIOAs”, di A. Jaggar, C. Meadows, M. Mislove, R. Segala, *Proceedings of ARSPA-WITS*, pagine 2-22, 2010.
- [35] “Conditional Automata: A Tool for Safe Removal of Negligible Events”, di R. Segala, A. Turrini, *Proceedings of CONCUR 2010*, pages 539-553, 2010.
- [36] “Approximated Computationally Bounded Simulation Relations for Probabilistic Automata”, R. Segala, A. Turrini, *Proceedings of the 20th IEEE Computer Security Foundations Symposium*, Venezia, pagine 140-156, Luglio 2007.
- [37] “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, Portogallo, LNCS 4423, ine 287-301, Aprile 2007.
- [38] “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, Luglio 2006.
- [39] “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)*, pagine 34–39, Luglio 2006.

- [40] “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, pagine 44–53, Settembre 2005.
- [41] “Stochastic Transition Systems for Continuous State Spaces and Non-determinism” di 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, pagine 125–139, Aprile 2005.
- [42] “Axiomatization of Trace Semantics for Stochastic Nondeterministic Processes” di A. Parma e R. Segala, in *Proceedings of the First International Conference on Quantitative Evaluation of SysTems (QEST)*, Twente, The Netherlands, pagine 294–303, Settembre 2004.
- [43] “Switched Probabilistic Automata”, di L. Cheung, N. Lynch, R. Segala, F. Vaandrager, in *Proceedings of the First International Colloquium on Theoretical Aspects of Computing (ICTAC)*, Guiyang, China, Settembre 2004.
- [44] “A Framework for Modeling Timed Systems with Restricted Hybrid Automata”, di D. K. Kaynar, N. Lynch, R. Segala, e F. Vaandrager, in *RTSS 2003: The 24th IEEE International Real-Time Systems Symposium*, Cancun, Messico, pagine 166–177, Dicembre, 2003.
- [45] “Compositionality for Probabilistic Automata”, di N. Lynch, R. Segala e F. Vaandrager, in *Proceedings of CONCUR 03*, LNCS 2761, pagine 208–221, Settembre 2003.
- [46] “Decision Algorithms for Probabilistic Bisimulation”, di S. Cattani e R. Segala, in *Proceedings of CONCUR02*, LNCS 2421, pagine 371–385, Agosto 2002.
- [47] “Coin Lemmas with Random Variables”, di K. Folegati e R. Segala, in *Proceedings of PAPM/PROBMIV 2001*, Aachen, Germania, LNCS2165, pagine 71–86, Settembre 2001.
- [48] “Automated Verification of a Randomized Distributed Consensus Protocol Using Cadence SMV and PRISM”, di M. Kwiatkowska, G. Norman, e R. Segala, in *Proceedings of CAV 2001*, Parigi, Francia, LNCS 2102, pagine 194–206, Luglio 2001.
- [49] “Axiomatizations for Probabilistic Bisimulation”, di E. Bandini e R. Segala, in *Proceedings of ICALP 2001*, Creta, Grecia, LNCS 2076, pagine 370–381, Luglio 2001.
- [50] “Hybrid I/O Automata Revisited”, di N. Lynch, R. Segala, F. Vaandrager, in *Proceedings of Hybrid Systems: Computation and Control*, Roma, LNCS 2034, pagine 403–417, Marzo 2001.
- [51] “Verifying Quantitative Properties of Continuous Probabilistic Real-Time Graphs”, di M. Kwiatkowska, G. Normann, R. Segala, e J. Sproston, in *Proceedings di CONCUR00*, LNCS 1877, pagine 123–137, Agosto 2000.
- [52] “Verifying Soft Deadlines with Probabilistic Timed Automata” di M. Kwiatkowska, G. Normann, R. Segala, e J. Sproston, in *Proceedings di WAVE00*, Giugno 2000.

- [53] “Symbolic Model Checking of Concurrent Probabilistic Processes Using MTBDDs and the Kronecker Representation”, di L. de Alfaro, M. Kwiatkowska, G. Norman, D. Parker e R. Segala, in Proceedings di TACAS 2000, Berlino, LNCS 1785, Aprile 2000.
- [54] “A New Definition of Multilevel Security”, di R. Focardi, R. Gorrieri, R. Segala, in *Proceedings of the Workshop on Issues in the Theory of Security (WITS)*, Ginevra, Svizzera, Luglio 2000.
- [55] , “Dynamic Load Balancing with Group Communication”, di S. Dolev, R. Segala, e A. Shvartsman, in Proceedings di International Colloquium on Structural Information and Communication Complexity (SIROCCO), Lacanau, Francia, pagine 111-125, Luglio 1999.
- [56] “Automatic Verification of Real-Time Systems With Discrete Probability Distributions”, di M. Kwiatkowska, G. Normann, R. Segala, e J. Sproston, in Proceedings di 5th international AMAST Workshop on Real-Time and Probabilistic Systems (ARTS '99), LNCS 1601, pagine 79–95, Maggio 1999.
- [57] “System Support for Partition-Aware Network Applications”, di O. Babaoglu, R. Davoli, A. Montresor e R. Segala, in Proceedings of the 18th International Conference on Distributed Computing Systems (ICDCS '98), pagine 184–191, Amsterdam, Olanda, Maggio 1998.
- [58] “Testing Probabilistic Automata”, di R. Segala, in Proceedings di CONCUR96, Pisa, Italia, Agosto, LNCS 1119, pagine 299–314, 1996.
- [59] “Hybrid I/O Automata”, di N. Lynch, R. Segala, F. Vaandrager e H.B. Weinberg, in *Hybrid Systems III*, LNCS 1066, pages 496–510. Articoli selezionati da DIMACS Workshop on Verification and Control of Hybrid Systems, Ottobre 1995.
- [60] “A Compositional Trace-Based Semantics for Probabilistic Automata”, di R. Segala, Proceedings di CONCUR95, Philadelphia, PA, USA, pagine 234–248, LNCS 962, Agosto 1995.
- [61] “Formal Verification of Timed Properties of Randomized Distributed Algorithms” di A. Pogoyants e R. Segala, Proceedings di PODC95, Ottawa, Ontario, Canada, pagine 174–183, 1995.
- [62] “Probabilistic Simulations for Probabilistic Processes”, di R. Segala e N. Lynch, Proceedings di CONCUR94, Uppsala, Svezia, LNCS 836, pagine 481–496, Agosto 1994.
- [63] “Proving Time Bounds for Randomized Distributed Algorithms”, di N. Lynch, I. Saia, e R. Segala, Proceedings di PODC94, Los Angeles, CA, pagine 314–323, Agosto 1994.
- [64] “Liveness in Timed and Untimed Systems”, di R. Gawlick, R. Segala, J. Sogaard Andersen, e N. Lynch, Proceedings di ICALP94, Gerusalemme, Israele, LNCS 820, pagine 166–177, Luglio 1994.
- [65] “A Comparison of Simulation Techniques and Algebraic Techniques for Verifying Concurrent Systems”, di N. Lynch e R. Segala, Proceedings del Second North American Process Algebra Workshop, Cornell University, NY, 1993
- [66] “Quiescence, Fairness, Testing and the notion of Implementation”, di R. Segala, Proceedings di CONCUR93, Hildesheim, Germania, pagine 324–338, LNCS 715, Agosto 1993.

1 Inviti Presso Scuole, Convegni, Istituti

Invited Lecturer a Scuole Internazionali

- *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, Italia, Settembre 2007. Titolo della relazione: “Quantitative Analysis in Security”.
- *Spring School on Security*, Marsiglia, Francia, Aprile 2005. Titolo della relazione: “Analysis of randomized protocols and applications to security.”
- *International School on Foundations of Security Analysis and Design*, Bertinoro, Italia, Settembre 2001. Titolo della relazione: “Applied Cryptography”.
- *International School on Foundations of Security Analysis and Design*, Bertinoro, Italia, Settembre 2000. Titolo della relazione: “Applied Cryptography”.
- *EEF summerschool on Formal Methods and Performance Analysis*, Nijmegen, Olanda, Luglio 2000. Titolo della relazione: “Verification of Probabilistic Distributed Algorithms”.

Invited Tutorial a Convegni

- *17th International Conference on Concurrency Theory (CONCUR 2006)*, Bonn, Germania. Titolo della relazione: “Probability and Nondeterminism in Operational Models of Concurrency”.
- *Workshop on Probabilistic Methods in Verification, Aachen, Germania, Settembre 2001*. Titolo della relazione: “Nondeterminism in probabilistic verification”.

Invited Speaker a Convegni

- *Workshop on Computational and Symbolic Proofs of Security*, Atagawa, Giappone, Aprile 2009. Titolo della presentazione: “On the use of Probabilistic Automata for Security Proofs”.
- *Workshop on Automata and Verification*, Mons, Belgio, Agosto 2008. Titolo della relazione: “Verification with Probabilistic Automata”.
- *Nancy Lynch Celebration*, Toronto, Agosto 2008. Titolo della relazione: “The power of Simulation Relations”.
- *VERAP - Approximate Verification of Probabilistic Systems*, project workshop, Parigi, Novembre 2007. Titolo della relazione: “Computationally Bounded Approximated Simulation Relations”.
- *5th Workshop on Quantitative Aspects of Programming Languages (QAPL 2007)*, Braga, Portogallo, Aprile 2007. Titolo della relazione: “Nondeterminism in Quantitative Analysis of Probabilistic Systems”.
- *Alpine Verification Meeting*, Lausanne, Ottobre 2005. Titolo della relazione: “Modelling Stochastic Nondeterministic Systems: the challenge of continuous measures”.

- *Probabilities and Artificial Intelligence Workshop*, Barbados, Aprile 2004. Titolo della relazione: “Axiomatizations for Probabilistic Automata”.
- *Workshop on Mathematical Models of Systems, Montreal, Canada, Ottobre 2002*. Titolo della relazione: “Models for Discrete Nondeterministic Stochastic Systems”.
- *Workshop on Probabilistic Methods in Verification, Indianapolis, USA, Giugno 1998*. Titolo della relazione: “The Essence of Coin Lemmas”.
- *Compositionality - The Significant Difference, Malente/Holstein, Germania, Settembre 1997*. Titolo della relazione: “Compositional Verification of Randomized Distributed Systems”.
- *Workshop on Distributed Algorithms (WDAG), Saarbrücken, Germania, Settembre 1997*. Titolo della relazione: “Verification of the Randomized Consensus Algorithm of Aspnes and Herlihy: a Case Study”.

Inviti a Tavole Rotonde

- *19th IEEE Computer Security Foundations Workshop (CSFW 2006)*, Venezia, Luglio 2006. Tema: “Nondeterminism in Security Modeling”.

Inviti presso Istituti di Ricerca

- Invitato presso il DIMACS, Rutger University, NJ, USA, per una settimana per attività di collaborazione nella ricerca, Aprile 2008.
- Visiting Professor per un mese alla *École Normale Supérieure* di Cachan, Francia, Maggio 2008.
- Visiting Professor per un mese alla *École Normale Supérieure* di Cachan, Francia, Giugno 2007.
- Invitato agli NTT Labs, Yokosuka, Giappone, per collaborazione in attività di ricerca e per un ciclo di seminari sull’analisi della sicurezza basata su automi, Maggio 2007.
- Invitato presso vari istituti di ricerca dove ha tenuto seminari sulla propria attività di ricerca. Lista parziale: LIAFA, CWI, AT&T Bell Labs, Stanford University, Berkeley, New York State University, MIT, University of Pennsylvania, University of Nijmegen, University of Birmingham, University of Augsburg.

Inviti Speciali

- Invitato al *Dagstuhl meeting on Quantitative Models: Expressiveness and Analysis*, Germania, Gennaio 2010.
- Invited Observer a *IFIP WG 2.2 meeting*, Torino, Settembre 2008. Declinato per altri eventi in conflitto.
- Invitato al workshop *Two Decades of Probabilistic Verification: Reflections and Perspectives*, Lorentz Center, Leiden, Olanda, Novembre 2007.
- Invited Observer a *IFIP WG 2.2 meeting*, Nancy, Francia, Settembre 2007. Declinato per altri eventi in conflitto.
- Invitato al *LIX Colloquium on Emerging Trends in Concurrency Theory*, Parigi, Novembre 2006.

- Invited Observer a *IFIP WG 2.2 meeting*, Skagen, Danimarca, Settembre 2005.
Declinato per altri eventi in conflitto.
- Invitato al workshop di celebrazione dei 25 anni di Process Algebra, Bertinoro, Agosto 2005.
- Invited Observer a *IFIP WG 2.2 meeting*, Bertinoro, Italia, Settembre 2004.
- Invitato al *Dagstuhl meeting on Probabilistic Methods in Verification and Planning*, Germania, Maggio 2003.
- Invited Observer a *IFIP WG 2.2 meeting*, Amsterdam, Olanda, Maggio 2003.
Declinato per altri eventi in conflitto.
- Invited Observer a *IFIP WG 2.2 meeting*, Oldenburg, Germania, Settembre 2002.
- Invitato al *Dagstuhl meeting on Probabilistic Methods in Verification*, Germania, Maggio 2000.

2 Attività Professionale Scientifica

Partecipazione a Steering Committee

- Membro eletto della steering committee di QEST dal 2003 al 2007.
- Membro della steering committee di PROBMIV dal 1999 al 2004.

Partecipazione a Comitati di Programma

- *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)
- *21st Int. Conf. on Concurrency Theory (CONCUR)*, Parigi, 2010.
- *Formal Methods for Aerospace*, Eindhoven, Olanda, Novembre 2009.
- *16th workshop Expressiveness in Concurrency (EXPRESS)*, Bologna, Italia, Settembre 2009.
- *Sixth International Conference on Quantitative Evaluation of SysTems (QEST)*, Budapest, Ungheria, 2009.
- *Fifth International Conference on Quantitative Evaluation of SysTems (QEST)*, Saint Malo, Francia, 2008.
- *14th International Workshop on Expressiveness in Concurrency (EXPRESS)*, Lisbona, Portogallo, 2007.
- *Fourth International Conference on Quantitative Evaluation of SysTems (QEST)*, (tutorial chair), Edinburgo, UK, 2007.
- *International Conference on Quantitative Evaluation of SysTems (QEST)*, Riverside, CA, USA, 2006.
- *22nd Conference on the Mathematical Foundations of Programming Semantics (MFPS)*, Genova, 2006.
- *Workshop on Quantitative Aspects of Programming Languages (QAPL)*, Vienna, Austria, 2006.
- *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.
- *14th Int. Conf. on Concurrency Theory (CONCUR)*, Marseille, 2003.
- *Work. on Process Algebra and Performance Modelling, Probabilistic Methods in Verification (PAPM/PROBMIV)*, Copenhagen, 2002 (chair).
- *Int. Conf. on Distributed Computing Systems*, Toulouse, 2002.
- *Work. on Process Algebra and Performance Modelling, Probabilistic Methods in Verification (PAPM/PROBMIV)*, Aachen, 2001.
- *Int. Work. on Expressiveness in Concurrency (Express)*, Aalborg, 2001.
- *Hybrid Systems: Computation and Control*, Roma, 2001.
- *Hybrid Systems: Computation and Control*, Pittsburgh, 2000.
- *Work. on Probabilistic Methods in Verification (PROBMIV)*, Eindhoven, 1999.
- *Int. AMAST Work. on Real-Time and Probabilistic Systems*, Bamberg, 1999.
- *Work. on Probabilistic Methods in Verification (PROBMIV)*, Indianapolis, 1998.
- *Hybrid Systems: Computation and Control*, Berkeley, 1998.
- *Work. on Distributed Algorithms (WDAG)*, Bologna, 1996.

Partecipazione a comitati editoriali

- Membro dell'editorial board di *Information and Computation* dal 2011.
- Membro dell'editorial board del *Int. Journal of Hybrid Systems* dal 2001 al 2011.

Membro esterno/revisore in commissioni di dottorato

- Martin Neuhäusser: “Model Checking Nondeterministic and Randomly Timed Systems”, Relatore Joost/Pieter Katoen, University of Twente, Olanda, Gennaio 2010.
- Daniele Magazzeni: “Explicit Model Checking Techniques Applied to Control and Planning Problems”, Relatore Giuseppe Della Penna, Università degli Studi dell'Aquila, Dicembre 2008.
- Lijun Zhang: “Decision Algorithms for Probabilistic Simulations”, Relatore Holger Hermanns, Universität des Saarlandes, Germania, Dicembre 2008.
- Elie Bursztein: “Anticipation games. Game theory applied to network security”, Relatore Jean Goubault-Larrecq, Ecole Normale Supérieure, Cachan, Francia, Novembre 2008.
- Yuxin Deng: “Axiomatisations and Types for Probabilistic and Mobile Processes”, Relatore Catuscia Palamidessi, INRIA, Parigi, Luglio 2005.
- Marielle Stoelinga: “Verification of Probabilistic Real-Time and Parametric Systems”, Relatore Frits Vaandrager, University of Nijmegen, Aprile 2002.
- Sue-Hwey Wu: “Compositional Behaviors of Probabilistic I/O Automata”, Relatori S. Smolka e E. Stark, Stony Brook, NY, Aprile 1996.

Altre Commissioni di Valutazione

- Membro della commissione di abilitazione di Veronique Cortier, CNRS LORIA, Francia, Novembre 2009.

Revisione di articoli scientifici

Revisore per numerosi convegni internazionali e per numerose riviste tra cui 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.

3 Attività Didattica

Insegnamento di corsi

Università di Verona

- *Algoritmi* (96 ore), corso di laurea in Informatica, AA 2009/25.
- *Crittografia* (48 ore), corso di laurea magistrale in Ingegneria e Scienze Informatiche, dal 2009.
- *Algoritmi e Strutture Dati* (64 ore), corsi di laurea in Informatica, dal 2009.
- *Model Checking* (20 ore), corso di dottorato in Informatica, 2008, 2005.
- *Laboratorio di Algoritmi e Strutture Dati* (24 ore), corsi di laurea in Informatica e Tecnologie dell'Informazione, AA 2002/05.
- *Sicurezza e Crittografia* (40 ore), corsi di laurea in Informatica VO, e laurea specialistica in Informatica e Sistemi Intelligenti e Multimediali, AA 2001/09.
- *Informatica* (62 ore), corso di laurea in Biotecnologie Agroindustriali, AA 2003/07.
- *Sistemi Operativi* (108 ore), corso di laurea in Informatica, AA 2000/01.

Università di Bologna

- *Algoritmi e Strutture Dati* (80 ore), corso di laurea in Informatica, AA 1995/2001.
- *Crittografia* (40 ore), corso di laurea in Informatica, AA 1998/2001.

Massachusetts Institute of Technology

- *Theory of Computation*, assistente del corso, 1993.

Supervisione di Tesi

Supervisore di numerose tesi di laurea e laurea specialistica presso le Università di Verona e Bologna. Supervisore di tesi di dottorato e master come da lista seguente.

- “Measures on Probabilistic Automata”, di Federica Panarotto, tesi di dottorato, Dipartimento di Informatica, Università degli Studi di Verona, (relatore R. Segala), 2017.
- “Hierarchical and Compositional Verification of Cryptographic Protocols”, di Andrea Turrini, tesi di dottorato, Dipartimento di Informatica, Università degli Studi di Verona, (relatore R. Segala), 2008.
- “Axiomatic and Logical Characterizations of Probabilistic Preorders and Trace Semantics”, di Augusto Parma, tesi di dottorato, Dipartimento di Informatica, Università degli Studi di Verona, (relatore R. Segala), 2008.
- “The Complexity of Randomized Distributed Algorithms”, di A. Pogosyants, tesi di PhD, Massachusetts Institute of Technology, (relatori: N. Lynch e R. Segala).
- “Time Optimal Self-Stabilizing Spanning Tree Algorithms”, di S. Aggarwal, tesi di master, Massachusetts Institute of Technology, (relatori: N. Lynch, S. Kutten, e R. Segala), Giugno 1994.

4 Attività Organizzativa

Organizzazione Didattica e Amministrativa

- Presidente del corso di laurea magistrale in Ingegneria e Scienze Informatiche dal 2009 al 2012 e dal 2018 al 2021.
- Membro del Consiglio di Amministrazione di UNIONLINE (Consorzio delle università del triveneto per la formazione a distanza) dal 2008 al 2011.
- Presidente del gruppo di lavoro di Ateneo per i Saperi Minimi dal 2008 al 2011.
- Direttore Vicario del Dipartimento di Informatica dal 2008 al 2010.
- Delegato del Rettore per l'Orientamento e l'e-learning dal 2007 al 2013.
- Membro del Consiglio di Amministrazione del COSP (Comitato Provinciale Orientamento Scolastico Professionale) dal 2006 al 2013.
- Delegato del Rettore per l'Orientamento alla Formazione Universitaria dal 2006 al 2007.
- Coordinatore del corso di Dottorato in Informatica dal 2006 al 2009.
- Vice-presidente del consiglio di corso di studi delle classi 26 e 23/S dell'Università di Verona dal 2002 al 2006.
- Presidente della commissione didattica dei corsi delle classi 26 e 23/S dell'Università di Verona dal 2002 al 2006.
- Responsabile del progetto di Ateneo dell'Università di Verona sulla didattica dell'Informatica di Base per non Informatici dal 2002 al 2013.
- Referente di Ateneo per l'ECDL (European Computer Drivers Licence) e responsabile dei rapporti con AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico) dell'Università di Verona dal 2002 al 2016.
- Rappresentante di sede presso il GRIN (Gruppo Ricercatori Informatica Nazionale) dal 2001 al 2009.
- Responsabile del progetto Campus One per il corso di laurea in Informatica dell'Università di Verona dal 2001 al 2003.
- Presidente della Commissione Tesi e Pratiche Studenti dei corsi delle classi 26 e 23/S dell'Università di Verona dal 2001 al 2003.

Organizzazione di Convegni

- Co-organizzatore del workshop PAPM-ProbMIV 2002, Copenhagen, Danimarca.
- Vice-chair del comitato organizzatore di ICALP '96, Bologna.

5 Partecipazione a Progetti di Ricerca

- *Security Horizons* (2013-2016), progetto PRIN sulla verifica della sicurezza dei sistemi e delle reti coordinato da Pisa.
- *Modelli e tecniche di analisi formale per la sicurezza dei sistemi software* (2008-2009), progetto PRIN sulla sicurezza dei sistemi e delle reti coordinato da Venezia.

- *C4C* (2007-2009), progetto Europeo sul controllo distribuito coordinato da CWI, Olanda.
- *ProNoBiS: Probability and Nondeterminism, Bisimulations and Security* (2006-2007), progetto INRIA con ENS Cachan, INRIA Futurs, Queen Mary University, Universit Paris 7, Universit di Verona, University of Birmingham.
- *AIDA Abstract Interpretation Design and Applications* (2005-2007), progetto MIUR COFIN con Bologna, Padova, Parma, Pisa, Udine, Venezia, Verona (coordinatore).
- *Automated Verification of Probabilistic Protocols with PRISM* (2003-2006), ruolo di visiting fellow, progetto EPSRC della University of Birmingham.
- *(SPY-Mod) Abstract interpretation and model checking for the verification of embedded systems* (2003-2005) Progetto FIRB (Basic Research) coordinato tra le università di Padova (coordinatore), Venezia, Verona.
- *CoVer: Constraint-based Verification of Reactive systems* (2002-2004) Progetto MURST coordinato tra le università di Bologna (coordinatore nazionale), Genova, Padova, Parma, Udine, Verona, CNR-IEI-CNUCE Pisa.
- *Mefisto* - Progetto MURST (Ottobre 2001 - Ottobre 2003).
- *Tosca* - Progetto MURST (Ottobre 1999 - Ottobre 2001). Task leader di “Sistemi ibridi”.
- *Automatic Verification of Randomized Distributed Algorithms* (1998-2001), ruolo di visiting fellow, progetto EPSRC della University of Birmingham.