Curriculum Vitae

Angelo TROINA

Personal Details

Gender: Male
Date of birth: 9th of August, 1979
Place of birth: Wolfsburg, Germany
Present Citizenship: Italian

Contact Details

Dipartimento di Informatica		Tel.:	+39 011 6706847
Corso Svizzera 185		Fax:	+39 011 751603
10149 - Torino		Email:	troina@di.unito.it
Italia		URL:	www.di.unito.it/∼troina

Actual Position

Since Oct 2007 Assistant Professor at Università di Torino

Language Knowledge

Italian:	native	**German**:	fair
English:	good	**Spanish**:	fair
French:	fair		

Education

11 Jul 1998	High School Diploma at Liceo Scientifico E. Ferrari, Cesenatico (FC) Mark: 60/60
10 Oct 2002	Master Degree in Computer Science at Università di Bologna Thesis: *Un Approccio Algebrico Probabilistico all'Analisi di Proprietà di Sicurezza di Sistemi Crittografici* (*A probabilistic Algebraic Approach for the Analysis of Security Properties of Cryptographic Systems*)

	Advisor: Prof. Roberto Gorrieri
	Mark: 110/110 cum laude
26 Jun 2006	Ph.D. in Computer Science at Università di Pisa
	Thesis: *Probabilistic Timed Automata for Security Analysis and Design*
	Advisor: Prof. Andrea Maggiolo Schettini
Sep'06– Sep'07	Postdoc at Laboratoire d'Informatique (LIX) of the Ecole Polytechnique and Laboratoire Specification et Verification (LSV) of the Ecole Normale Superieure de Cachan.

Ph.D. Schools Attended:

Mar 2003	*Bertinoro International Spring School (BISS'03)*, Bertinoro, Italy
Sep 2003	*Advanced School on Mobile Computing*, Pisa, Italy
Sep 2004	*Foundations of Security Analysis and Design (FOSAD'04)*, Bertinoro, Italy
Apr 2005	*Spring School on Security*, Marseille, France

Research Visits:

Oct/Nov 2005	Visiting student at Laboratoire PPS (Paris VII, Jussieu)
Jun 2008	Research visit at LIX (Ecole Polytechnique)

Professional Experiences

Oct'98–Oct'02	ARSTUD fellowship for undergraduate students
Gen'03–Dec'05	MIUR Ph.D. fellowship
Gen'06–Feb'06	Research contract founded by Dipartimento di Informatica, Università di Pisa. Title of the research project: *Specification and Verification of Distributed Systems*
Mar'06–Apr'06	Research contract founded by Dipartimento di Informatica, Università di Pisa in the context of the AIDA project. Title of the research project: *Integrazione tra strumenti di interpretazione astratta e model checking per la verifica di proprietà di sicurezza di codice mobile*
Apr'06–Dec'06	Research contract founded by Museo storico della fisica e Centro di studi e ricerche "Enrico Fermi". Title of the research project: *Matematica e Diagnosi Medica*
Sep'06–Sep'07	Postdoc fellowship founded by INRIA
Since Oct'07	Assistant professor at Università di Torino

Research Fields of Interest

- Formal Description Techniques of Concurrent Systems
- Formal Modeling and Verification of Real-Time and Probabilistic Systems
- Foundations of Security Analysis and Design
- Systems Biology

Research Activity

While some system properties can be studied in a non-timed and non-probabilistic setting, others, such as quantitative security properties, system performance and reliability properties, require a timed and probabilistic description of the system. My research activity focused on methods for formal modeling and specification of probabilistic timed systems, and on algorithms for the automated verification of their properties. The models considered describe the behavior of a system in terms of time and probability, and the formal specification languages used are based on extensions of timed automata, Markov decision processes and probabilistic replacement rules.

These techniques are applied in two main fields: (1) Security Analysis and (2) Systems Biology.

Security Analysis:

In multilevel systems it is important to avoid unwanted indirect information flow from higher levels to lower levels, namely the so called covert channels. Initial studies of information flow analysis were performed by abstracting away from time and probability. It is already known that systems that are considered to be secure may turn out to be insecure when time or probability are considered. Recently, work has been done in order to consider also aspects either of time or of probability, but not both.

In [C2, T2] a concept of weak bisimulation for Probabilistic Timed Automata is given, together with an algorithm to decide it. This model is used for describing and analyzing a probabilistic nonrepudiation protocol in a timed setting.

In [C6, C12] a general framework is proposed, which is based on Probabilistic Timed Automata, where both probabilistic and timing covert channels can be studied. A Non-Interference security property and a Non Deducibility on Composition security property are defined. They allow expressing information flow in a timed and probabilistic setting, and they can be compared with analogous properties defined in settings where either time or probability or none of them are taken into account. This permits a classification of the properties depending on their discerning power.

In [C1, C3, C11, T1] the assumption of perfect cryptography is relaxed and a new probabilistic equivalence of messages exchanged in a communication protocol is introduced. The methodology takes to the definition of a probabilistic notion of secrecy.

In [C5] a probabilistic model is defined for the analysis of a Non-Repudiation protocol which guarantees fairness without resorting to a trusted third party, by means of a probabilistic algorithm. The PRISM model checker is used for estimating the probability for a malicious user to break the non-repudiation property.

The NRL Pump protocol defines a multilevel secure component whose goal is to minimize leaks of information from high level systems to lower level systems, without degrading average time performances. In [C4, C10] a probabilistic model for the NRL Pump is defined and the FHP-murf probabilistic model checker is used to estimate the capacity of a probabilistic covert channel in the NRL Pump.

In [J3, C7] a model of Parametric Probabilistic Transition Systems is developed, where probabilities associated with transitions may be parameters. Techniques are proposed to find instances of parameters that satisfy a given property and instances that either maximize or minimize the probability of reaching a certain state.

Systems of Data Management Timed Automata (SDMTAs) are networks of communicating timed automata with structures to store messages and functions to manipulate them. In [C14] the decidability of reachability for SDMTAs is proved. As an application, the Yahalom protocol is modeled and analyzed.

In [C19] a probabilistic extension of the Applied Pi-calculus is proposed. Such an extension, whose semantics is defined via Segala's Probabilistic Automata, allows to deal with probabilistic and nondeterministic choice operators, and to model cryptographic primitives through equational teories. Applications to the analysis of security protcols are immediate.

Systems Biology:

In the last few years people became aware that biological processes can be described using means originally developed by computer scientists to model systems of interacting components. This permits simulation of system behaviour and verification of properties. Among the many formalisms that have been applied to biology there are, for instance, Petri Nets, Hybrid Systems, the Pi–calculus and other process algebras (BioAmbients, Brane Calculi, BioPEPA, etc.) and rewriting techniques (κ–calculus, P-Systems, CLS, etc.). Some of these new formalisms have been proposed to describe biomolecular and membrane interactions and some models based on probabilities have been successfully used to develop simulators for biochemical systems.

In [J1, C9, C13] a probabilistic calculus for biomolecular interaction (in particular for enzymatic activity) is introduced. The calculus is based on a set of rewrite rules whose application depends on a probability. As an alternative to GillespieŠs one, an interpretation algorithm and a formal semantics are given for the calculus, and their compatibility is proven. A prototype implementation of the interpreter for the calculus is developed, which permits to follow the evolution of a biomolecular system. The formal semantics, given as a transition system, permits to verify properties of a system by model checking.

In [J2, C15] a new calculus (CLS) is introduced, which is suitable to describe microbiological systems and their evolution. The calculus is used to model interactions among bacteria and bacteriophage viruses, and to reason on their properties.

In [J4, C17] a labelled semantics for CLS is introduced in order to define notions of strong and weak bisimulations for CLS. It is proved that this kind of bisimulations are congruences.

In [J5] a stochastic extension of CLS is defined and used to perform quantitative simulations of cellular pathways.

List of Publications

[**Journals**]

[J1] R. Barbuti, S. Cataudella, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *A Probabilistic Model for Molecular Systems*. Fundamenta Informaticae, vol. 67, pp. 13-27, 2005.

[J2] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *A Calculus of Looping Sequences for Modelling Microbiological Systems*. Fundamenta Informaticae, vol. 72, pp. 21-35, 2006.

[J3] R. Lanotte, A. Maggiolo-Schettini, A. Troina. *Parametric Probabilistic Transition Systems for System Design and Analysis*. Formal Aspects of Computing, vol. 19, pp. 93-109, 2007.

[J4] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *Bisimulations in Calculi Modelling Membranes*. Formal Aspects of Computing, vol 20, pp. 351-378, 2008.

[J5] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, P. Tiberi, A. Troina. *Stochastic Calculus of Looping Sequences for the Modelling and Simulation of Cellular Pathways*. Transactions on Computational Systems Biology, to appear.

[J6] R. Lanotte, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *Design and Verification of Long-Running Transactions in a Timed Framework*. Science of Computer Programming, vol. 73, pp. 76-94.

[**Conferences and Workshops Proceedings**]

[C1] A. Troina, A. Aldini, R. Gorrieri. *A Probabilistic Formulation of Imperfect Cryptography*. 1st IFIP WG 1.7 Int. Workshop on Issues in Security and Petri Nets (WISP'03), Eindhoven, the Netherlands, 2003, Eindhoven University of Technology, pp. 41-55.

[C2] R. Lanotte, A. Maggiolo-Schettini, A. Troina. *Weak Bisimulation for Probabilistic Timed Automata and Applications to Security*. 1st Int. Conference on Software Engineering and Formal Methods (SEFM'03), Brisbane, Australia, 2003, IEEE Computer Society Press, pp. 34-43.

[C3] A. Troina, A. Aldini, R. Gorrieri. *Approximating Imperfect Cryptography in a Formal Model*. Proceedings of the MEFISTO Project 2003 (Formal Methods for Security and Time), Elsevier ENTCS 99, pp. 183-203.

[C4] R. Lanotte, A. Maggiolo-Schettini, S. Tini, A. Troina, E. Tronci. *Automatic Analysis of the NRL Pump*. Proceedings of the MEFISTO Project 2003 (Formal Methods for Security and Time), Elsevier ENTCS 99, pp. 245-266.

[C5] R. Lanotte, A. Maggiolo-Schettini, A. Troina. *Automatic Analysis of a Non-Repudiation Protocol*. 2nd Int. Workshop on Quantitative Aspects of Programming Languages (QAPL'04), Barcelona, Spain, 2004, Elsevier ENTCS 112, pp. 113- 129.

[C6] R. Lanotte, A. Maggiolo-Schettini, A. Troina. *Information Flow Analysis for Probabilistic Timed Automata*. 2nd Int. Workshop on Formal Aspects in Security and Trust (FAST'04), Toulouse, France, 2004, Springer IFIP 173, pp. 13-26.

[C7] R. Lanotte, A. Maggiolo-Schettini, A. Troina. *Decidability Results for Parametric Probabilistic Transition Systems with an Application to Security*. 2nd Int. Conference on Software Engineering and Formal Methods (SEFM'04), Beijing, China, 2004, IEEE Computer Society Press, pp. 114-121.

[C8] R. Lanotte, A. Maggiolo-Schettini, S. Tini, A. Troina. *Verification of Hybrid Automata by Synthesis and Refinement*. 13th Workshop on Concurrency Specification and Programming (CS&P'04), Caputh, Germany, 2004, Humboldt-Universitaet, Informatik-Berichte 170, pp. 69-80.

[C9] R. Barbuti, S. Cataudella, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *A Probabilistic Calculus for Molecular Systems*. 13th Workshop on Concurrency Specification and Programming (CS&P'04), Caputh, Germany, 2004, Humboldt-Universitaet, Informatik- Berichte 170, pp. 202-216.

[C10] R. Lanotte, A. Maggiolo-Schettini, S. Tini, A. Troina, E. Tronci. *Automatic Covert Channel Analysis of a Multilevel Secure Component*. 6th International Conference on Information and Communications Security (ICICS'04), Malaga, Spain, 2004, Springer LNCS 3269, pp. 249-261.

[C11] A. Troina, A. Aldini, R. Gorrieri. *Towards a Formal Treatment of Secrecy against Computational Adversaries*. 2nd IST/FET Int. Workshop on Global Computing (GC'04), Rovereto, Italy, 2004, Springer LNCS 3267, pp. 77-92.

[C12] R. Lanotte, A. Maggiolo-Schettini, A. Troina. *A Classification of Time and/or Probability Dependent Security Properties*. 3rd Int. Workshop on Quantitative Aspects of Programming Languages (QAPL'05), Edinburgh, Scotland, 2005, Elsevier ENTCS 153(2), pp. 177-193.

[C13] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *An Alternative to Gillespie's Algorithm for Simulating Chemical Reactions*. 3rd Int. Workshop on Computational Methods in Systems Biology (CMSB'05), Edinburgh, Scotland, 2005, pp. 167- 178.

[C14] R. Lanotte, A. Maggiolo-Schettini, A. Troina. *Timed Automata with Data Structures for Distributed Systems Design and Analysis.* 3nd Int. Conference on Software Engineering and Formal Methods (SEFM'05), Koblenz, Germany, 2005, IEEE Computer Society Press, pp. 44-53.

[C15] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *A Calculus of Looping Sequences for Modelling Microbiological Systems.* 14th Int. Workshop on Concurrency Specification and Programming (CS&P'05), Ruciane-Nida, Poland, 2006, pp. 29-40.

[C16] R. Lanotte, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *Modeling Long-Running Transactions with Communicating Hierarchical Timed Automata.* 8th IFIP Int. Conference on Formal Methods for Open Object-Based Distributed Systems (FMOODS'06), Bologna, Italy, 2006, Springer LNCS 4037, pp. 108-122.

[C17] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *Bisimulation Congruences in the Calculus of Looping Sequences.* 3rd Int. Colloquium on Theoretical Aspects of Computing (ICTAC'06), Tunis, Tunisia, 2006, Springer LNCS 4281, pp. 93-107.

[C18] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, A. Troina. *The Calculus of Looping Sequences for Modeling Biological Membranes.* 8th Workshop on Membrane Computing (WMC8), invited paper, Thessaloniki, Greece, 2007, Springer LNCS 4860, pp. 54-76.

[C19] J. Goubault-Larrecq, C. Palamidessi, A. Troina. *A Probabilistic Applied Pi-Calculus.* 5th Asian Symposium on Programming Languages and Systems (APLAS'07), Singapore, 2007, Springer LNCS 4807, pp. 175-190.

[C20] J. Krivine, R. Milner, A. Troina. *Stochastic Bigraphs.* 24th Conference on the Mathematical Foundations of Programming Semantics (MFPS'08), invited paper, ENTCS, Philadelphia (PA), USA, May 2008.

[C21] B. Aman, M. Dezani-Ciancaglini, A. Troina. Type Disciplines for Analysing Biologically Relevant Properties. 2nd International Meeting on Membrane Computing and Biologically Inspired Process Calculi (MeCBIC'08), Iasi, Romania, September 2008.

[**Theses**]

[T1] A. Troina. *Un Approccio Algebrico Probabilistico all'Analisi di Proprietà di Sicurezza di Sistemi Crittografici.* Master Thesis, Università di Bologna, 2002.

[T2] A. Troina. *Probabilistic Timed Automata for Security Analysis and Design.* Ph.D. Thesis, Università di Pisa, 2006.

Research Projects

2003	*MEFISTO: Metodi formali per la sicurezza e il tempo.* MIUR
2005-2006	*AIDA: Abstract Interpretation Design and Applications.* MIUR
2005–2009	*Automata: from Mathematics to Applications (AutoMathA).* ESF/PESC
2006	*Matematica e Diagnosi Medica.* Centro Fermi
2006–2007	*ProNoBiS: Probability and Nondeterminism Bisimulations and Security.* INRIA/ARC

Teaching Activity

2004/2005	Teaching assistant of the course *Metodologie di Programmazione.* Corso di Laurea in Informatica, Facoltà di S.M.F.N., Università di Pisa
2007/2008	Teacher of the course *Informatica II.* Corso di Laurea in Ottica ed Optometria, Facoltà di S.M.F.N., Università di Torino
2008/2009	Teacher of the course *Informatica.* Corso di Laurea in Scienze Strategiche e delle Comunicazioni, Interfacoltà in Scienze Strategiche, Università di Torino. Teacher of the course *Laboratorio di Programmazione II.* Corso di Laurea in Informatica, Facoltà di S.M.F.N., Università di Torino. Teacher of the course *Informatica II.* Corso di Laurea in Ottica ed Optometria, Facoltà di S.M.F.N., Università di Torino

Reviewing Activity

Workshops and Conferences
European Symposium on Programming (ESOP), IEEE Computer Security Foundations Symposium (CSF), International Workshop on Constructive Methods for Parallel Programming (CMPP), IEEE International Computer Software and Applications Conference (COMPSAC), IEEE Symposium on Logic in Computer Science (LICS), International Workshop on Practical Applications of Stochastic Modelling (PASM), International Workshop on Views On Designing Complex Architectures (VODCA), International Workshop on Security Issues with Petri Nets and other Computational Models (WISP), International Static Analysis Symposium (SAS), International ACM Conference on Computer and Communications Security (CCS), International IEEE Computer Security Foundations Workshop (CSFW), International Colloquium on Automata, Languages and

Programming (ICALP), International Symposium on Fundamentals of Computation Theory (FCT), International Conference on Foundations of Software Science and Computation Structures (FOSSACS), ACM Symposium on Applied Computing (SAC), International Conference on Software Engineering Research, Management and Applications (SERA), International Workshop on Web Services and Formal Methods (WS-FM), International Conference on Concurrency Theory (CONCUR), International Workshop on Quantitative Aspects of Programming Languages (QAPL), International Conference on Quantitative Evaluation of SysTems (QEST), International Symposium on Ubiquitous Computing Systems (UCS), International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI), Workshop on Issues in the Theory of Security (WITS), Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA), International Symposium on Mathematical Foundations of Computer Science (MFCS), From Biology To Concurrency and back (FBTC)

Journals
Information Processing Letters, Fundamenta Informaticae, Mathematical Structures in Computer Science, Theoretical Computer Science, Journal of Universal Computer Science, Journal of Systems and Software

Torino - October 1, 2008 Angelo TROINA[1]

.....

[1]Consapevole degli effetti penali per dichiarazioni mendaci, falsità in atti ed uso di atti falsi ai sensi dell'art. 76 del DPR 445/2000, sotto la propria responsabilità dichiara la veridicità di quanto riportato nel presente curriculum.

References

These persons are familiar with my professional qualifications and my character:

Prof. Roberto Barbuti
Dip. di Informatica
Università di Pisa
Largo B. Pontecorvo 3
56127 - Pisa
Italia
Tel.: +39 050 2212747
Fax: +39 050 2212726
barbuti@di.unipi.it

Prof. Roberto Gorrieri
Dip. di Scienze dell'Infromazione
Università di Bologna
Mura Anteo Zamboni 7
40127 - Bologna
Italia
Tel.: +39 051 2094509
Fax: +39 051 2094510
gorrieri@cs.unibo.it

Prof. Mariangiola Dezani-Ciancaglini
Dip. di Informatica
Università di Torino
Corso Svizzera 285
10149 - Torino
Italia
Fax: +39 011 751603
dezani@di.unito.it

Prof. Andrea Maggiolo Schettini
Dip. di Informatica
Università di Pisa
Largo B. Pontecorvo 3
56127 - Pisa
Italia
Tel.: +39 050 2212759
Fax: +39 050 2212726
maggiolo@di.unipi.it

Prof. Catuscia Palamidessi
LIX, Ecole Polytechnique
Rue de Saclay
91128 - Palaiseau Cedex
France
Tel.: +33 (0)1 69334117
Fax: +33 (0)1 69334049
catuscia@lix.polytechnique.fr