CURRICULUM VITAE

Name and Surname: Daniele Gorla
Birth Date: October 12th, 1976
Web Page: `http://www.dsi.uniroma1.it/~gorla`
E-mail: `gorla@di.uniroma1.it`
Degrees:

- *Conservatorium Diploma in violin* (with the highest marks, Music Conservatorium of Perugia, July 1999);
- *Laurea (MSc) in Informatics* (summa cum laude, University of Rome "La Sapienza", December 2000);
- *PhD in "Informatics and Applications"* (University of Florence, February 2005, supervisors: Prof. Rocco De Nicola and Prof. Rosario Pugliese).

Current Position: *Assistant Professor (ricercatore)* at the Department of Informatics of the University of Rome "La Sapienza".

Research Interests: semantics of concurrent programming; process calculi with distribution, mobility and/or cryptography; formal methods for security; categorial semantics of concurrency.

Education:

- *Microsoft DotNet Crash Course* held in Cambridge (UK), March 2002;
- *Bertinoro International Summer School for Graduate Studies in Computer Science,* May 2002;
- *Marktoberdorf International Summer School* on "Models, Algebras, and Logic of Engineering Software", August 2002;
- *Summer School on Software Security*, held in Eugene (Oregon, USA), June 2004.

Professional Activities:

- Contracts:
  - *Research grant* at the University of Florence (Dip. Sistemi e Informatica) from April to October 2001. Research title: "Calculi for the specification and the verification of cryptographic protocols ";
  - *Research grant* at the University of Bologna (Dip. di Elettronica, Informatica e Sistemistica) from July to October 2002. Research title: "Using logical theories to analyse fault-tolerance problems in distribuited systems";
  - *Research grant* at the University of Roma "La Sapienza" (Dip. di Informatica) from October 2003 to February 2006;
- Research periods in international institutions:
  - *Marie Curie Fellow* at COGS (Centre for Research in Cognitive Science), University of Sussex (Brighton, UK), from July to September 2003;
  - *Research fellowship* at the University of Sussex (Dep. of Informatics) from January to April 2005;
  - *Visiting professor* at the laboratory "Preuves, Programmes et Systèmes" (PPS) of the university "Paris Diderot" (Paris VII) in February 2008;
  - *Visiting Fellow* at the Faculty of Engineering and Information Technology, University of Technology Sydney (Australia) September – October 2010;
- Invited contributions:
  - *Invited speaker* of the ICALP'03 satellite workshop **SecCo'03**;
  - *Invited lecturer* in the international school **BASICS'09**, organized by the University of Shanghai in October 2009;
  - *Invited tutorial* at the workshop **"Qualitative and Quantitative Network Protocol Analysis"**, organized at Dagstuhl, February 2010;

- Member of Program Committes:
  - *PC co-chair* and *organizer* of the workshop **SecCo'07: Security Issues in Concurrency**, co-located with CONCUR'07;
  - *PC member* and *panelist* of the workshop **EXPRESS'07: Expressiveness in Concurrency**, co-located with CONCUR'07;
  - *PC member* of the workshop **PLID'08: Programming Language Interference and Dependence**, co-located with SAS'08;
  - *PC co-chair* e *organizer* of the workshops **EXPRESS'08** and **EXPRESS'09**, co-located with CONCUR'08 and CONCUR'09;
  - *PC member* of **MFPS XXV: the 25th Conference on Mathematical Foundations of Programming Semantics**, 2009;
  - *PC member* of **CONCUR 2010: the 21st Conference on Concurrency Theory**, 2010;
- Editorial activity:
  - *Guest editor* for the **Electronic Notes in Theoretical Computer Science** (proceedings of SecCo'07 and EXPRESS'08)
  - *Guest editor* for the **Journal of Computer Security** (special issue of SecCo'07)
  - *Guest editor* for the **Journal of Mathematical Structures in Computer Science** (special issues of EXPRESS'08 and EXPRESS'09);
  - *Guest editor* for the **Electronic Proceedings in Theoretical Computer Science** (proceedings of EXPRESS'09).
- Reviewing activity:
  - *international journals:* ACM TOPLAS, Information and Computation (2 papers), Acta Informatica (2 papers), Bullettin EATCS, Theoretical Informatics and Applications, Journal of Logic and Algebraic Programming (2 papers), International Journal of Foundations of Computer Science (2 papers), Journal of Computer Security, Mathematical Structures in Computer Science, Nordic Journal of Computing, Journal of Computer Science and Technology, ACM Computing Surveys;
  - *international conferences and workshop:* FST&TCS 2002, ACM SAC 2003, Foundations of Global Computing Workshop 2003, COORDINATION'04, FoSSaCS'05, COORDINATION'05, CSFW'05, CONCUR'05, EXPRESS'05, SECCO'05, ESOP'06, CSFW'06, COORDINATION'06, LICS'06, COORDINATION'07, CONCUR'07, EXPRESS'07 (3 papers), SECCO'07 (2 papers), FoSSaCS'08, COORDINATION'08, ICALP'08, ICLP'08, PerCom'09, ESOP'09, CONCUR'09 (2 papers), ESOP'10, FoSSaCS'10, CIAC'10, IFIP-TCS'10, CONCUR'10 (3 articoli), EXPRESS'10.

Teaching activity (at the university of Rome "La Sapienza")**:**

- *Teaching assistant* for the course "Computer Architectures", Autumn 2001;
- *Teaching assistant* for the courses "Computer Architectures" and " Laboratory of Programming Languages", Autumn 2002;
- *Teaching assistant* for the course "Mathematical Logics", Autumn 2003;
- *Teaching assistant* for the courses "Programming in C" and "Concurrency theory", Spring 2004;
- *Teaching assistant* for the courses "Mathematical Logics", Autumn 2005;
- *Teaching assistant* for the courses "Assembly languages", "Concurrency theory" and "Language-based security", Spring 2006;
- *Teaching assistant* for the course "Mathematical Logics", Autumn 2006;
- *Lecturer* for the courses "Concurrency theory" and "Language-based security", Spring 2006;
- *Teaching assistant* for the course "Mathematical Logics", Autumn 2007;
- *Teaching assistant* for the course "Assembly languages", Spring 2008;
- *Lecturer* for the courses "Concurrency theory" and "Language-based security", Spring 2008.
- *Lecturer* for the courses "Concurrency theory" and "Language-based security", Spring 2009;
- *Teaching assistant* for the course "Mathematical Logics", Autumn 2009;
- *Lecturer* for the course "Concurrency theory", Autumn 2009;
- *Lecturer* for the course "Programming Methodologies", Spring 2010.

International conferences and workshops attended:

- *ETAPS'02*, and presentation of a paper at *FoSSaCS;*
- *Types for Global Computing Workshop*, and presentation of a paper;
- *1st International Conference on Security in Pervasive Computing (SPC'03)*, and presentation of a paper;
- *2nd EATCS Workshop on Foundations of Global Computing (FGC'03)* affiliated to ICALP'03;
- *1st International Workshop on Security Issues in Coordination Models, Languages, and Systems (SecCo'03)*, affiliated to ICALP'03, as invited speaker;
- *ICALP'03*, and presentation of a paper;
- *6th Int. Conf. on Coordination Models and Languages (COORDINATION'04);*
- *19th Annual ACM Symposium on Applied Computing (SAC 2004)*, and presentation of a paper;
- *17th IEEE Computer Security Foundations Workshop (CSFW'04)*, and presentation of a paper;
- *3rd EATCS and 2nd UK Grand Challenge joint workshop on Foundations of Global Ubiquitous Computing (FGUC'04)*, and presentation of a paper;
- *Dagstuhl Seminar on "Foundations of Global Computing",* and presentation of a paper;
- *7th Int. Conf. on Coordination Models and Languages (COORDINATION'05) ,* and presentation of a paper;
- *ICALP'05*, and presentation of a paper;
- *ETAPS'06*, and presentation of a paper at *FoSSaCS;*
- *EXPRESS'06*, and presentation of a paper;
- *Symposium on "Emerging Trends in Concurrency";*
- *SecCo'07*, as organizer e co-chair;
- *EXPRESS'07*, as panellist;
- *CONCUR'08*, and presentation of a paper;
- *EXPRESS'08*, as organizer e co-chair;
- *TGC'08*, and presentation of a paper;
- *MFPS XXV*, and presentation of a paper;
- *EXPRESS'09*, as organizer e co-chair;
- *BASICS'09*, and invited lecture;
- *Dagstuhl Workshop on "Qualitative and Quantitative Network Protocol Analysis"*, and invited tutorial.

Seminars in (national ed foreign) Universities and Research Institutes:

- *"Access Control in a Language with Distribution and Code Mobility"* at the University of Milan, November 2002;
- *"A Distributed Calculus for Role-Based Access Control"* at the Dept. of Informatics, Univ. of Sussex (UK), May 2004;
- *"Comparing communication primitives via their relative expressive power*" at the Ecole Polytechnique (Parigi), March 2006;
- *"Comparing calculi for mobility via their relative expressive power*" at the Imperial college (London), Ecole Polytechnique (Parigi) and PPS-ParisVII, March 2007;
- *"Towards a unified approach to encodability and separation results for process calculi*" at Ecole Polytechnique (Parigi) and PPS-ParigiVII, February 2008.

National and international research projects working in:

- *Models, Calculi and Languages for Network Aware Programming (NAPOLI),* MURST national research program;
- *Network Aware Programming and Interoperability (NAPI),* Microsoft Research grant;
- *Mobile Calculi based on Domains (MIKADO),* EU proactive initiative FET-Global Computing (Contract IST-2001-32222);
- *Architectures for Mobility (AGILE),* EU proactive initiative FET-Global Computing (Contract IST-2001-32222).
- *Software Engineering for Service-Oriented Overlay Computers (SENSORIA),* EU Sixth Framework Programme, Priority 2 – Information Society Technologies (Contract number 016004);

- *Quantified Information Flow for Process Algebras*, Royal Society, for bilateral exchanges between "La Sapienza" and "Kings College" of London.

Papers in international conferences and workshops:

[C1] *"On Compositional Reasoning in the Spi–Calculus"*, together with Michele Boreale. Proceedings of **FoSSaCS 2002** (5th International Conference on Foundations of Software Science and Computation Structures), LNCS 2303, pages 67 – 81. Springer, 2002.

[C2] *"Resource Access and Mobility Control with Dynamic Privileges Acquisition"*, together with Rosario Pugliese. Proceedings of **ICALP 2003** (30th International Colloquium on Automata, Languages and Programming), LNCS 2719, pages 119 – 132. Springer, 2003.

[C3] *"Enforcing Security Policies via Types"*, together with Rosario Pugliese. Proceedings of **SPC 2003** (1st International Conference on Security in Pervasive Computing), LNCS 2802, pages 88 – 103. Springer, 2003.

[C4] *"Controlling Data Movement in Global Computing Applications"*, together with Rosario Pugliese. Proceedings of **SAC 2004** (19th Annual ACM-SIGAPP Symposium on Applied Computing), pages 1462 – 1467. ACM Press, 2004.

[C5] *"A Distributed Calculus for Role-Based Access Control"*, together with Chiara Braghin and Vladimiro Sassone. Proceedings of **CSFW 2004** (17th Computer Security Foundations Workshop), pages 48 – 60. IEEE Computer Society, 2004.

[C6] *"On the expressive power of KLAIM-based Calculi"*, together with Rocco De Nicola and Rosario Pugliese. Proceedings of **EXPRESS 2004** (11th Workshop on Expressiveness in Concurrency), ENTCS 128(2): 117 – 130. Elsevier, 2004.

[C7] *"Security Policies as Membranes in Systems for Global Computing"*, together with Matthew Hennessy and Vladimiro Sassone. Proceedings of **FGUC 2004** (3rd EATCS Workshop on Fondations of Global Ubiquitous Computing), ENTCS 138(1):23 – 42. Elsevier, 2004.

[C8] *"Global Computing in a Dynamic Network of Tuple Spaces"*, together with Rocco De Nicola and Rosario Pugliese. Proceedings of **COORDINATION 2005** (7th Intern. Conf. on Coordination Models and Languages), LNCS 3454, pages 157 – 172. Springer, 2005.

[C9] *"Pattern Matching over a Dynamic Network of Tuple Spaces"*, together with Rocco De Nicola and Rosario Pugliese. Proceedings of **FMOODS 2005** (7th IFIP Intern. Conf. on Formal Methods for Open Object-based Distributed Systems), LNCS 3535, pages 1 – 14. Springer, 2005.

[C10] *"Basic Observables for a Calculus for Global Computing"*, together with Rocco De Nicola and Rosario Pugliese. Proceedings of **ICALP 2005** (32nd International Colloquium on Automata, Languages and Programming), LNCS 3580, pages 1226 – 1238. Springer, 2005.

[C11] *"On the Relative Expressive Power of Asynchronous Communication Primitives"*. Proceedings of **FoSSaCS 2006** (9th International Conference on Foundations of Software Science and Computation Structures), LNCS 3921, pages 47 – 62. Springer, 2006.

[C12] *"Inferring Dynamic Credentials for Role-based Trust Management"*, together with M. Hennessy and V. Sassone. Proceedings of **PPDP 2006** (8th ACM-SIGPLAN International Symposium on Principles and Practice of Declarative Programming), pages 213 – 224. ACM Press, 2006.

[C13] *"Synchrony vs Asynchrony in Communication Primitives"*. Proceedings of **EXPRESS 2006** (13th Workshop on Expressiveness in Concurrency), ENTCS 175(3): 87 – 108. Elsevier, 2007.

[C14] *"From Flow Logic to Static Type Systems for Coordination Languages"*, together with R.De Nicola, R.R.Hansen, F.Nielson, H.Riis Nielson, C.W.Probst and R.Pugliese. Proceedings of **COORDINATION 2008** (10th Intern. Conf. on Coordination Models and Languages), LNCS 5052, pages 100 – 116. Springer, 2008.

[C15] *"Network Applications of Graph Bisimulation"*, together with Pietro Cenciarelli and Emilio Tuosto. Proceedings of **IGCT 2008** (4th Intern. Conf. On Graph Transformation), LNCS 5214, pages 131 – 146. Springer, 2008.

[C16] *"Towards a Unified Approach to Encodability and Separation Results for Process Calculi"*. Proceedings of **CONCUR 2008** (19th Intern. Conf. on Concurrency Theory), LNCS 5201, pages 492–507. Springer, 2008.

[C17] *"On the Relative Expressive Power of Ambient-based Calculi"*. Proceedings of **TGC 2008** (4th Intern. Symp. on Trustworthy Global Computing), LNCS 5474, pages 141 – 156. Springer, 2009.

[C18] *"On the Relative Expressive Power of Calculi for Mobility"*. Proceedings of **MFPS XXV** (25th Intern. Conf. on Mathematical Foundations of Programming Semantics), ENTCS 249, pages 269 – 286. Elsevier, 2009.

[C19] *"Depletable Channels: Dynamics and Behaviour"*, together with Pietro Cenciarelli and Ivano Salvo. Proceedings of **FCT 2009** (17th Intern. Symp. on Fundamentals of Computation Theory), LNCS 5966, pages 50 – 61. Springer, 2009.

[C20] *"Concurrent Pattern Calculus"*, together with Thomas Given-Wilson e Barry Jay. Proceedings of **IFIP-TCS 2010** (6th Intern. IFIP Conference on Theoretical Computer Science), IFIP AICT 323, pagg. 244 – 258. IFIP, 2010.

[C21] *"A semiring-based trace semantics for processes with applications to information leakage analysis"*, together with Michele Boreale e David Clark. Proceedings of **IFIP-TCS 2010** (6th Intern. IFIP Conference on Theoretical Computer Science), IFIP AICT 323, pagg. 340 – 354. IFIP, 2010.

Papers in books and collections:

[B1] *"The KLAIM Project: Theory and Practice"*, together with L.Bettini, V.Bono, R.De Nicola, G.Ferrari, M.Loreti, E.Moggi, R.Pugliese, E.Tuosto, B.Venneri. In **Global Computing: Programming Environments, Languages, Security and Analysis of Systems**, LNCS 2874, pages 88-150. Springer, 2003. Partially based on [C2] and [C3].

Papers in international journals:

[J1] *"Process Calculi and the Verification of Security Protocols"*, together with Michele Boreale. Partially based on [C1]. **International Journal of Telecommunication and Information Technology**, special issue on Cryptographic Protocol Verification, pages 28 – 40. National Institute of Telecommunications – Warsaw, 2002.

[J2] *"Security Policies as Membranes in Systems for Global Computing"*, together with Matthew Hennessy and Vladimiro Sassone. Extended version of [C7]. **Logical Methods in Computer Science**, 1(3:2), 1 – 23, 2005. Previously appeared as Research Report 02/2004, Dept. of Informatics, Univ. of Sussex at Brighton (UK), 2004.

[J3] *"Role-Based Access Control for a Distributed Calculus"*, together with Chiara Braghin and Vladimiro Sassone. Extended version of [C5]. **Journal of Computer Security**, 14(2):113 – 155, IOS Press, 2006. Previously appeared as Tech.Rep. 08/2004, Dip. Informatica, Univ. "La Sapienza".

[J4] *"On the expressive power of KLAIM-based Calculi "*, together with Rocco De Nicola and Rosario Pugliese. Extended version of [C6]. **Theoretical Computer Science,** 356(3):387 – 421, Elsevier, 2006. Previously appeared as Tech.Rep. 09/2004, Dip. Informatica, Univ. di Roma "La Sapienza".

[J5] *"Confining Data and Processes in Global Computing Applications"*, together with Rocco De Nicola and Rosario Pugliese. Extended version of [C4]. **Science of Computer Programming**, 63(1):57 – 87, Elsevier Science, 2006.

[J6] *"Global Computing in a Dynamic Network of Tuple Spaces"*, together with Rocco De Nicola and Rosario Pugliese. Extended version of [C8]. **Science of Computer Programming**, 64(2):187 – 204, Elsevier Science, 2007. Previously appeared as Tech.Rep. 05/2005, Dip. Informatica, Univ. di Roma "La Sapienza".

[J7] *"Basic Observables for a Calculus for Global Computing"*, together with Rocco De Nicola and Rosario Pugliese. Extended version of [C10]. **Information and Computation**, 205(10):1491 – 1525, Elsevier 2007. Previously appeared as Tech.Rep. 07/2004, Dip.Informatica, Univ. di Roma "La Sapienza".

[J8] *"Comparing Communication Primitives via their Relative Expressive Power"*. Extended and revised version of [C11] and [C13]. **Information and Computation**, 206(8):931 – 952, Elsevier 2008.

[J9] *"Dynamic management of capabilities in a network aware coordination language"*, together with Rosario Pugliese. Extended version of [C2]. **Journal of Logic and Algebraic Programming**, 78:665 – 689, Elsevier 2009. Previously appeared as Tech.Rep. 06/2004, Dip. Informatica, Univ. "La Sapienza".

[J10] *"Tree-functors, Determinacy and Bisimulations"*, together with Rocco De Nicola and Anna Labella. **Mathematical Structures in Computer Science**, 20(3):319 – 358, CUP 2010. Previously appeared as Tech. Rep. 02/2006, Dip. Informatica, Univ. "La Sapienza" with title "Characterising Bisimulations Functorially".

[J11] *"From Flow Logic to Static Type Systems for Coordination Languages"*, together with R.De Nicola, R.R.Hansen, F.Nielson, H.Riis Nielson, C.W. Probst e R.Pugliese. Extended version of [C14]. **Science of Computer Programming**, 75(6): 376 – 397. Elsevier, 2010.

[J12] *"Towards a Unified Approach to Encodability and Separation Results for Process Calculi"*. Extended and revised version of [C16]. **Information and Computation**, 208(9):1031 – 1053. Elsevier 2010.

[J13] *"A Taxonomy of Calculi for Distribution and Mobility"*. Extended and revised version of [C17] and [C18]. To appear in **Distributed Computing**, Springer 2010. Previously appeared as Tech. Rep. 09/2006, Dip. Informatica, Univ. "La Sapienza" with title "Comparing Calculi for Mobility via their Relative Expressive Power".

Edited:

[E1] *"Security Issues in Concurrency (SecCo'07): Proceedings"*, together with Catuscia Palamidessi. **Electronic Notes in Theoretical Computer Science**, 194(1), Elsevier, 2008.

[E2] *"Expressiveness Issues in Concurrency (EXPRESS'08): Proceedings"*, together with Thomas Hildebrandt. **Electronic Notes in Theoretical Computer Science**, 242(1). Elsevier, 2009.

[E3] *"Expressiveness Issues in Concurrency (EXPRESS'09): Proceedings"*, together with Sybille Froeschle. **Electronic Notes in Theoretical Computer Science**, 8, 2009.

[E4] *"Security Issues in Concurrency (SecCo'07): Special issue"*, together with Catuscia Palamidessi. **Journal of Computer Security**, volume 18(2). IOS Press, 2010.

[E5] *"Expressiveness Issues in Concurrency (EXPRESS'08): Special issue"*, together with Thomas Hildebrandt. **Mathematical Structures in Computer Science**, volume 20(1). CUP, 2010.

[E6] *"Expressiveness Issues in Concurrency (EXPRESS'09): Special issue"*, together with Sybille Froeschle. **Mathematical Structures in Computer Science**, in preparation.

Text Books:

[L1] *"Introduzione alla logica e al linguaggio matematico"* (in italian), together with Giorgio T. Bagni and Anna Labella. McGraw-Hill, 2008. ISBN 978-88-386-6505-9.

Research Reports:

[R1] *"Enforcing Security Policies via Types"*, together with Rosario Pugliese. Tech.Rep. 05/2004, Dip. Informatica, Univ. di Roma "La Sapienza". Extended version of [C3].

[R2] *"Inferring Dynamic Credentials for Role-based Trust Management"*, together with M. Hennessy and V. Sassone. Tech. Rep. 04/2006, Dip. di Informatica, Univ. di Roma "La Sapienza" (Italy). Extended version of [C12].

[T1] **MS Thesis:** *Grammatiche di sincronizzazione per generare l'esposizione di una fuga*. Dip. Informatica, Univ. di Roma "La Sapienza", December 2000.

[T2] **PhD Thesis:** *Semantic Approaches to Global Computing Systems*. PhD thesis XVII-04-I, Dip. di Sistemi ed Informatica, Univ. di Firenze, February 2005. Awarded by the **Italian Council of the EATCS** as the second best italian thesis on theoretical computer science (area "Programming Languages and Semantics") in the years 2004/05.

***h*-index:**

- Done through *publish-or-perish*: **11**
- Manually done via *google-scholar*, by excluding self-citations: **10**
  - [B1] cited by 77
  - [C2] cited by 29
  - [C7] cited by 25
  - [C5] cited by 22
  - [J12] cited by 20
  - [J7] cited by 18
  - [C11] cited by 13
  - [C1] cited by 13
  - [J5] cited by 10
  - [C3] cited by 10

***g*-index:**

- Done through *publish-or-perish*: **18**
- Manually done via *google-scholar*, by excluding self-citations: **16**
  Indeed, apart from the 10 papers mentioned for the *h*-index, there are the following papers:
  - [C8] cited by 10
  - [C4] cited by 7
  - [J5] cited by 5
  - [C9] cited by 5
  - [J8] cited by 5
  - [C13] cited by 4

Last update: July 8th, 2010

Overal Comment on my Research

The research is finalized to the development and use of formal methods for concurrent programming. Three main research lines can be identified: approaches that describe and guarantee security properties of concurrent programs; development and use of behavioural equivalences, to describe and verify the behavior of concurrent programs; comparison between various formalisms, based on their expressive power. Such studies have been lead on minimal languages (also known as 'process calculi') with advanced features, like sophisticated communication primitives, distribution and mobility of code, cryptographic primitives.

Below, you can find detailed comments on each research line; [T2] collects most of the research carried out until the beginning of 2005 in a cross-sectional way, that is collecting together results from the three research lines [C2,C3,C4,C6,C8,C9,C10,C14,B1,J4,J5,J6,J7,J9,J11,R1]. The unifying criterion has been the particular language on which the several theories they have been adapted; in particular, in all these works it has been used the language KLAIM [DFP98] (acronym of "Kernel Language for Agents Interaction and Mobility"). The fundamental features of such language are: processes distributed on a net of nodes, local and remote communication based on tuple spaces and pattern matching [Gel85], possibility to program the movement of code between different nodes of the net.

1. Formal methods for the security of concurrent programs (language-based security)

The study of concurrent formalisms and languages is focused on the possible interactions between various users (represented by programs in concurrent execution on the same machine or distributed on different but interconnected machines). In this scenario, it is fundamental to specify and force proper security properties. In literature a huge variety of such properties is present; some of them have been studied in the introduced research.

A typical security property is *data secrecy*. To this aim, we introduce in [C4] a framework where the programmer labels the sensitive data with a region expressing the nodes of the net (that is, which users) can access the data. We then develop a type system that guarantees that this property is respected in every execution of a well-typed system. The work in [C4] is adapted in [J5] to three distributed calculi: KLAIM, the distributed pi-calculus by Hennessy and Riely [HR02] and the Ambient calculus by Cardelli and Gordon [CG00]. This fact shows that different theoretical and programming choices can however support the same typing approach. An alternative approach to data secrecy in concurrent and distributed systems relies on cryptography. In this way, reserved data are cyphred and the decryption key is only given to the users entitled to access the data. Also in this setting, the use of process calculi has been a fruitful reasoning tool: in particular, a deep impact has obtained by the Spi-calculus [AG98], a cryptographic variant of the pi-calculus [MPW92]. For this language, we have developed in [C1] a sound (and complete, for finite processes) axiomatization for the bisimulation that allows the derivation of equational laws easying the proof of simple property of cryptographic protocols. [J1] shows an actual case-study: proving confidentiality and authentication in the framework of the protocol KERBEROS [KN93].

An orthogonal issue in the security of concurrent systems is the possibility of *controlling the activity of the processes* that it contains. To this aim, in [C2,C3,C7,C14,B1,J2,J9,J11,R1] we define type systems that aim at controlling the executions of the processes in a node. Every node is associated to a type describing the legal operations that a process running at the node can perform. In some sense, the type of a node is the interface of the node, since it is an upper bound to the actions that can be executed from that node. [C14,B1,J11] introduce a basic type system that is then enriched in with more sophisticated features. In [C3,R1] types contain fine-grained information: access rights to incoming code are granted according to the origin of a process. Moreover, a fine-grained classification on the operations is introduced: we keep in consideration not only the kind of operations but also their arguments. Therefore, operations that forbid reading a secret datum are not handled like operations of reading public data. In [C2,J9] we evolve the base model in an other direction, orthogonal to the previous one: the type of a node can vary during a computation, according the interactions happened between that node and the rest of the net. Therefore, some privileges can be acquired or lost by the node. This scenario describes well the scenario that processes in execution on a WAN meet and models in simple and elegant way applications of electronic commerce.

Finally, in [C7,J2] we better examine the type of a node and the properties that can guarantee. In particular, by smoothly varying the definition of the type (set of actions, multiset of actions, finite-state automaton whose input are actions), we can easy express more and more refined policies via type systems. Clearly, to verify that a process respects the policies specified by a highly expressive type is very expensive in computational terms; for this reason, we use notions of trust and subtype to make type-checking as efficient as possible.

In systems distributed on a geographic scale, the use of *trust* between users is a simple, robust and scalable way to assure security properties. The basic idea is to grant authorizations based on the possession of certificates that, opportunely combined, supply an unforgeable evidence to the authorization. Typical concepts of programming languages (like logics or type systems) have been successfully used to specify and use trust-based systems [LMW03]. In [C12,R2] we have extended mechanisms for certificate management to base certificate validity on the moment and on the context in which they are used. In practice, we have considered the framework based on logical programming introduced in [LMW03] and we have added the notion of temporal duration and of validity conditions. Both these characteristics have been already used for a long time in the trust-based commerical systems; however, their formal study has revealed several technical complications and has evidenced possible evolutions of the systems used in practice.

[C2,C3,C7,C14,B1,J2,J9,J11,R1] are base on the accesses control mechanism known in literature as *discretionary model*. In such a model, the system administrator assigns to users access rights relying on their identity. In [SCFY96] it has been introduced another mechanism to assign rights: *role-based access control (RBAC)*. In such a model, privileges are assigned to roles; during the life of the system, several users play different roles and their actions must be authorised from the privileges associated to their activated roles. In [C5,J3] we study the impact of such mechanism in a distributed version of the pi-calculus [MPW92]: we provide a type system (that dealing with security policies) and a bisimulation (to reason on the functionalities of the systems under consideration). As revealed by the case-studies, the theory simplifies the definition of systems and policies, once fixed some behavioural properties to meet.

2. Development and use of behavioural equivalences

Traditionally, a programming language is a 'calculus' if it is possible to develop on it behavioural theories. Such theories allow to equationally reason on the functionalities of a program written in such language, without considering implementation details. The main scope of [C10,J7] is therefore the definition of behavioural equivalences for a core calculus derived from KLAIM. The developed theory can be smoothly tailored to handle failures and connectivity of the net, some key features in a WAN scenario. The theory is then used in [C8,J6,J7,T2] to prove the correctness of some typical protocols for distributed and fault-tolerant systems ('the dining philosophers', 'the k-set agreement', two protocols for message delivering), by using exclusively an equational approach.

To better estimate and comprise the notions of equivalence used, we have also studied such equivalences 'more abstractly', i.e. by studying them not in a particular language but rather by considering a more 'denotational' model of concurrent programming based on trees. In such a model, we have studied [J10] the categorial properties that characterize three fundamental equivalences in concurrency theory: the strong, branching and weak versions of the bisimulation. It turned out that such equivalences can be expressed in a very natural way by simple adaptations of the very famous notion of 'functor fullness'; this fact supplies a further evidence on the key role that such equivalences play in concurrency.

3. Comparison between different formalisms: expressive power

An evident fact in the programming language field is the enormous variety of proposals present in literature or used in practice. Concurrent programming, and above all the formalisms with mobile code developed in the last years, is a typical example of this fact: many languages differ only for small details and often the difference between several formalisms, if any, is not very clear. For this reason, several ways to compare

different languages have been developed so far; however, no unified methodology has been developed yet to face this problem, known as 'expressiveness' (or 'expressive power') of the languages.

An empiric way to test expressiveness is via examples: it consists in showing applications that can be well modelled in a language but not in other ones. Although this approach does not have a solid theoretical base, it is a lot used in practice, also because it has the advantage of being close to the programmer (that will use the language in practice) by showing him the typical applications in which he should prefer a language respect to another. We have followed this approach in [C9], where we have studied the expressive power of several alternatives (always easy to distributedly implement) to the standard pattern matching [Gel85].

A more rigorous method is to encode a language in another, or to prove that this is impossible. This approach enhances the previous one, in the sense that it rigorously shows how as constructs of a language can be implemented in another one or, viceversa, which features of a language cannot be implemented in the other. Clearly, in order to develop such results, it is crucial to fix the properties that the encoding function must enjoy; intuitively, the encoding must translate terms without modifying their behaviors. Again, this fact can be formalized in several ways and no common agreement on the right way to formalize it has been reached yet. In this direction, we can locate [C6,C11,C13,C16,C17,C18,J4,J8,J12,R3]. In [C6,J4] we study 'fully abstract' encodings between different dialect of the KLAIM language; the several dialects progressively simplify the original language and culminate in an extremely simple calculus. In [C11,C13,J8] we study the expressive power of various communication primitives; the primitives are obtained by combining in every possible way four typical features of communication: synchrony (synchronous vs asynchronous communications), arity (delivery of a single message or more messages at once), communication medium (channels or tuple spaces) and absence/presence of pattern matching. Finally, in [C17,C18,R3] we compare different calculi for mobility: the pi-calculus, one of its distributed versions, KLAIM, Ambient and its variants (Boxed Ambient and its variants, Safe Ambient and its variants, Seal).

References:

[AG98] M. Abadi, A.D. Gordon. *A Calculus for Cryptographic Protocols: the Spi-calculus*. **Information and Computation**, 148(1):1-70, 1999.

[CG00] L. Cardelli, A.D. Gordon. *Mobile Ambients*. **Theoretical Computer Science**, 240(1):177-213, 2000.

[DFP98] R. De Nicola, G. Ferrari, R. Pugliese. *KLAIM: a Kernel Language for Agents Interaction and Mobility*. **IEEE Transactions on Software Engineering**, 24(5):315-330, 1998.

[HR02] M. Hennessy, J. Riely. *Resource Access Control in Systems of Mobile Agents*. **Information and Computation**, 173:82-120. 2002.

[KN93] J. Kohl, B. Neuman. *The Kerberos Network Authentication Service (version 5)*. Internet Request for Comment RFC-1510, 1993.

[LMW03] N. Li, J.C. Mitchell, W.H. Winsborough. *Beyond Proof-of-compliance: Security Analysis in Trust Management*. **Journal of the ACM**, 52(3):474--514, 2005.

[MPW92] R. Milner, J. Parrow, D. Walker. *A Calculus of Mobile Processes (part I and II)*. **Information and Computation**, 100(1):1-77, 1992.

[SCFY96] R. Sandhu, E. Coyne, H. Feinstein, C. Youmann. *Role-Based Access Control Models*. **IEEE Computer**, 29(2):38-47, 1996.

[SBM99] R. Sandhu, V. Bhamidipati, Q. Munawer. *The ARBAC97 Model for Role-Based Administration of Roles*. **ACM Trans. on Information and System Security**, 2(1):105-135, 1999.