INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team comete

Concurrency, Mobility and Transactions

Saclay - Île-de-France

Theme : Programs, Verification and Proofs

Table of contents

1. Team

Research Scientists

Catuscia Palamidessi [Team Leader, Senior Researcher, HdR]
Frank Valencia [Junior Researcher]

External Collaborator

Konstantinos Chatzikokolakis [Univ. of Eindhoven, NL. He will join Comète as Junior Researcher in February 2012.]

PhD Students

Andrés Aristizábal [Grant DGA/CNRS. Since 1/10/2009]
Christelle Braun [Grant École Polytechnique. 1/10/2007–30/9/2010]
Mário Sergio Ferreira Alvim Junior [Grant DGA/CNRS. Since 1/10/2008]
Ivan Gazeau [Grant ANR. Co-supervised by Dale Miller, INRIA. Since 1/10/2009]
Sophia Knight [Grant INRIA-CORDIS. Since 15/9/2010]
Marie-Aude Steineur [Grant ANR. Co-supervised by Sami Abbes, Paris VII. Since 1/10/2009]

Post-Doctoral Fellows

Miguel Andrés [Grant QUALCOMM. Since 27/11/2010]
Filippo Bonchi [Grant ERCIM. 1/11/2009–30/6/2010]
Jérémy Dubreil [Grant INRIA. Since 1/12/2009]

Administrative Assistant

Marie-Jeanne Gaffard [SAR]

Other

Luis Fernando Pino Duque [Master's student. Grant Ecole Polytechnique, Since 1/10/2010]

2. Overall Objectives

2.1. Introduction

Our times are characterized by the massive presence of highly distributed and mobile systems consisting of diverse and specialized devices, forming heterogeneous networks, and providing different services and applications. The resulting computational systems are usually referred to as *Ubiquitous Computing*, (see, e.g., the UK Grand Challenge initiative under the name *Sciences for Global Ubiquitous Computing* [42]). *Security* is one of the fundamental concerns that arises in this setting. The problem of *privacy*, in particular, is exacerbated by orders of magnitude: The frequent interaction between users and electronic devices, and the continuous connection between these devices and the internet, offer to malicious agents the opportunity to gather and store huge amount of information, often without the individual being even aware of it. Mobility is also an additional source of vulnerability, since tracing may reveal significant information. To avoid these hazards, honest agents should use special protocols, called *security protocols*.

The systems above are usually very complex and based on impressive engineering technologies, but they do not always exhibit a satisfactory level of robustness and reliability. The same holds for security protocols: they usually look simple, but the properties that they are supposed to ensure are extremely subtle, and it is also difficult to capture the capabilities of the attacker. As a consequence, even protocols that seem at first "obviously correct" are later (often years later) found to be prone to attacks.

In order to overcome these drawbacks, we need to develop formalisms, reasoning techniques, and tools, to specify systems and protocols, their intended properties, and to guarantee that these intended properties are indeed satisfied. The challenges that we envisage are (a) to find suitably expressive formalisms which capture essential new features such as mobility, probabilistic behavior, presence of uncertain information, and potentially hostile environment, (b) to build suitably representative models in which to interpret these formalisms, and (c) to design efficient tools to perform the verification in presence of these new features.

2.2. Highlights of the year

+ Catuscia Palamidessi has been invited to serve as PC co-chair of the 2011 edition of the conference QEST (The International Conference on Quantitative Evaluation of SysTems, http://www.qest.org/).
+ Catuscia Palamidessi has been invited to serve as PC co-chair of the 2011 edition of TOSCA (Theory Of SeCurity and Applications. Associated with the ETAPS conferences, http://www.etaps.org/).
+ Catuscia Palamidessi has been invited speaker at the 2010 edition of the conference LICS (Twenty-Fifth Annual IEEE Symposium on Logic in Computer Science, http://www2.informatik.hu-berlin.de/lics/lics10/).

3. Scientific Foundations

3.1. Probabilistic aspects

Participants: Miguel Andrés, Filippo Bonchi, Christelle Braun, Jérémy Dubreil, Mário Sergio Ferreira Alvim Junior, Ivan Gazeau, Sophia Knight, Catuscia Palamidessi, Marie-Aude Steineur.

Most of our approaches to formal reasoning and verification are characterized by the presence of probabilistic aspects. The need to take these aspects into account can arise for various reasons: First, algorithms for distributed systems and security protocols often use randomization. Second, the modeling of the physical world frequently requires coping with uncertain and approximate information (for example, the number of the requests that are received by a web server during various times of the day), which we may be able to refine by statistical measurements, and then naturally represent using a probabilistic formalism. Third, reality can sometimes be too complicated to be represented and analyzed in detail; probabilistic models offer then a convenient abstraction mechanism.

3.2. Expressiveness issues

Participants: Andrés Aristizábal, Filippo Bonchi, Catuscia Palamidessi, Luis Fernando Pino Duque, Frank Valencia.

We intend to study models and languages for concurrent, probabilistic and mobile systems, with a particular attention to expressiveness issues. We aim at developing criteria to assess the expressive power of a model or formalism in a distributed setting, to compare existing models and formalisms, and to define new ones according to an intended level of expressiveness, taking also into account the issue of (efficient) implementability.

3.3. The probabilistic asynchronous π-calculus

Participants: Miguel Andrés, Filippo Bonchi, Christelle Braun, Sophia Knight, Catuscia Palamidessi, Frank Valencia.

We will focus our efforts on a probabilistic variant of the asynchronous π-calculus, which is a formalism designed for mobile and distributed computation. A characteristic of our calculus is the presence of both probabilistic and nondeterministic aspects. This combination is essential to represent probabilistic algorithms and protocols, and express their properties in presence of unpredictable (nondeterministic) users and adversaries.

4. Application Domains

4.1. Security

Participants: Miguel Andrés, Christelle Braun, Jérémy Dubreil, Mário Sergio Ferreira Alvim Junior, Catuscia Palamidessi.

The aim of our research is the specification and verification of protocols used in mobile distributed systems, in particular security protocols. We are especially interested in protocols for *privacy*, because they exhibit features that require the kind of concepts and approach in which we feel most competent. It is likely, however, that the instruments and tools developed having privacy in mind can later be useful and adaptable also to other domains of security, like *Secure Information flow*. Privacy is a generic term which denotes the issue of preventing certain information to become known to an agent, except in the case that the agent is explicitly allowed to be informed. It may refer to the protection of *private data* (credit card number, personal info etc.), of the agent's identity (*anonymity*), of the link between information and user (*unlinkability*), of its activities (*unobservability*), and of its *mobility* (*untraceability)*.

The common denominator of this class of problems is that an adversary can try to infer the private information (*secrets*) from the information that he can access (*observables*). The purpose of privacy protocols is then to obfuscate the link between secrets and observables as much as possible, and they often use randomization to achieve this purpose, i.e. to introduce *noise*. The protocol can therefore be seen as a *noisy channel*, in the Information-Theoretic sense, between the secrets and the observables.

We intend to explore the rich set of concepts and techniques in the fields of Information Theory and Hypothesis Testing to establish the foundations of privacy, and to develop heuristics and methods to improve protocols for privacy. Our approach will be based on the specification of protocols in the probabilistic asynchronous π-calculus, and the application of model-checking to compute the matrices associated to the corresponding channels.

4.2. Model checking

Participants: Miguel Andrés, Catuscia Palamidessi.

We plan to develop model-checking techniques and tools for verifying properties of systems and protocols specified in the above formalisms. Model checking addresses the problem of establishing whether the model (for instance, a finite-state machine) of a certain specification satisfies a certain logical formula. We intend to concentrate our efforts on aspects that are fundamental for the verification of security protocols, and that are not properly considered in existing tools. Namely, we will focus on: (a) the combination of probability and mobility, which is not provided by any of the current model checkers, (b) the interplay between nondeterminism and probability, which in security present subtleties that cannot be handled with the traditional notion of scheduler, (c) the development of a logic for expressing security (in particular privacy) properties. We should capture both probabilistic and epistemological aspects, the latter being necessary for treating the knowledge of the adversary. Logics of this kind have been already developed, but the investigation of the relation with the models coming from process calculi, and their utilization in model checking, is still in its infancy.

5. Software

5.1. A model checker for the probabilistic asynchronous π-calculus

Participants: Miguel Andrés [correspondant], Catuscia Palamidessi.

In collaborations with Dave Parker and Marta Kwiatkowska, we are developing a model checker for the probabilistic asynchronous π-calculus. Case studies with Fair Exchange and MUTE, an anonymous peer-to-peer file sharing system, are in progress.

Technically we use MMC as a compiler to encode the probabilistic π-calculus into certain PRISM representation, which will then be verified against PCTL using PRISM. The transitional semantics defined in MMC can be reused to derive the symbolic transition graphs of a probabilistic process. The code for derivation will work as an add-on to MMC under XSB and invoke a graph traversal to enumerate all reachable nodes and transitions of the probabilistic process.

In the meanwhile we are also attempting a direct and more flexible approach to the development of a model checker for the probabilistic π-calculus, using OCaml. This should allow to extend the language more easily, to include cryptographic primitives and other features useful for the specification of security protocols. As the result of our preliminary steps in this direction we have developed a rudimentary model checker, available at the following URL: http://vamp.gforge.inria.fr/.

5.2. PRISM model generator

Participants: Konstantinos Chatzikokolakis [correspondant], Catuscia Palamidessi.

This software generates PRISM models for the Dining Cryptographers and Crowds protocols. It can also use PRISM to calculate the capacity of the corresponding channels. More information can be found in [39] and in the file README file width instructions at the URL http://www.lix.polytechnique.fr/comete/software/README-anonmodels.html.

The software can be download at http://www.lix.polytechnique.fr/comete/software/anonmodels.tar.gz. These scripts require Perl to run and have been tested in Linux. The GUI of the corners tool also requires the Perl/TK library. Finally some parts of the model generator tool require PRISM and gnuplot to be installed.

5.3. Calculating the set of corner points of a channel

Participants: Konstantinos Chatzikokolakis [correspondant], Catuscia Palamidessi.

The corner points can be used to compute the maximum probability of error and to improve the Hellman-Raviv and Santhi-Vardy bounds. More information can be found in [40] and in the file README file width instructions at the URL http://www.lix.polytechnique.fr/comete/software/README-corners.html.

The software can be download at http://www.lix.polytechnique.fr/comete/software/corners.tar.gz. These scripts require Perl to run and have been tested in Linux. The GUI of the corners tool also requires the Perl/TK library. Finally some parts of the model generator tool require PRISM and gnuplot to be installed.

5.4. MMCsp, a compiler for the π-calculus

Participants: Peng Wu [correspondant], Catuscia Palamidessi.

MMCsp is a compiler from a simple probabilistic π-calculus to PRISM (http://www.prismmodelchecker.org/manual/Main/Introduction). models. It is built on XSB (http://xsb.sourceforge.net/), a tabled logic programming system, and generates the symbolic semantic representation of a probabilistic pi-calculus term in text. A separate Java program then translates this semantic representation into a probabilistic model for PRISM.

The tool was developed by Peng Wu during his postdoc period in Comète in the context of the collaboration between the teams Comète and PRISM under the INRIA/ARC Project ProNoBib (http://www.lsv.ens-cachan.fr/~goubault/ProNobis/index.html). It is based on the papers [48] and [45].

The source code is free and can be download from http://www.cs.ucl.ac.uk/staff/p.wu/mmc_sp_manual.html.

6. New Results

6.1. Foundations of information hiding

Information hiding refers to the problem of protecting private information while performing certain tasks or interactions, and trying to avoid that an adversary can infer such information. Particular cases of this property are anonymity and privacy.

This topic is one of the main lines of research in Comète. We are investigating various aspects of it, as described below. An overview of the main results we have obtained so far is contained in [15].

6.1.1. The problem of information hiding in presence of concurrency

It is well known that the raising of nondeterminism, due to the possible interleavings and interactions of the parallel components, can cause unintended information leaks. One way to solve this problem, already explored in literature, is to fix the strategy of the scheduler beforehand [38]. However this solution is considered too rigid and unrealistic. In [12] we develop a linguistic (process-calculus) approach to this problem, and we show how to apply it to control the behavior of the scheduler in various anonymity examples. In [22] we propose a milder restriction on the schedulers, and we define the notion of strong (probabilistic) information hiding under various notions of observables. Furthermore, we propose a method, based on the notion of automorphism, to verify that a system satisfies the property of strong information hiding, namely strong anonymity or no-interference, depending on the context.

6.1.2. Safe Equivalences for Security Properties

In the field of Security, process equivalences have been used to characterize various information-hiding properties (for instance secrecy, anonymity and non-interference) based on the principle that a protocol P with a variable x satisfies such property if and only if, for every pair of secrets s_1 and s_2, $P[^{s_1}/_x]$ is equivalent to $P[^{s_2}/_x]$. In [20] we argue that, in the presence of nondeterminism, the above principle relies on the assumption that the scheduler "works for the benefit of the protocol", and this is usually not a safe assumption. Non-safe equivalences, in this sense, include complete-trace equivalence and bisimulation. We present a formalism in which we can specify admissible schedulers and, correspondingly, safe versions of these equivalences. We prove that safe bisimulation is still a congruence. Finally, we show that safe equivalences can be used to establish information-hiding properties.

6.1.3. Interactive systems

In [19] we consider systems where secrets and observables can alternate during the computation. We show that the information-theoretic approach which interprets such systems as (simple) noisy channels is not valid anymore. However, the principle can be recovered if we consider more complicated types of channels, that in Information Theory are known as channels with memory and feedback. We show that there is a complete correspondence between interactive systems and such kind of channels. Furthermore, we show that the capacity of the channels associated to such systems is a continuous function of the Kantorovich metric.

6.1.4. Knowledge, belief and vulnerability

In real life situations it is often the case that the attacker has some extra knowledge, independent from the protocol. For instance, in the case of anonymity protocols, the attacker may have some expectations about the behavioural patterns of individual users. This extra knowledge is called *belief* in case it may be inaccurate. We want to sty how the exit knowledge evolves, and what is its impact on the vulnerability of the system. The case of accurate knowledge is investigated in [26], and the case of belief in [27]. In [26] we also reformulate and extend Reiter and Rubin's notion of probable innocence, and provide a new formalisation for it based on the concept of protocol vulnerability. Accordingly, we establish new formal relationships between protocol parameters and attackers' knowledge expressing necessary and sufficient conditions to ensure probable innocence.

6.1.5. Computing the leakage

In [21] we address the problem of computing the information leakage of a system in an efficient way. We propose two methods: one based on reducing the problem to reachability, and the other based on techniques from quantitative counterexample generation. The second approach can be used either for exact or approximate computation, and provides feedback for debugging. These methods can be applied also in the case in which the input distribution is unknown. We then consider the interactive case and we point out that the definition of associated channel proposed in literature is not sound. We show however that the leakage can still be defined consistently, and that our methods extend smoothly.

6.2. Process Calculi

6.2.1. Concurrent Constraint Programming

Bisimilarity is one of the main representative equivalences for concurrent behaviour. It captures our intuitive notion of process equivalence; two processes are equivalent if they can match each other's moves. Furthermore, it provides an elegant co-inductive proof technique based on the notion of bisimulation. Nevertheless, there have been few attempts to define a notion of bisimilarity for *concurrent constraint programming* (ccp). The ones we were aware of are those in [47] and [44] but they are not completely satisfactory: The first one may tell apart processes with identical observable behaviour, while the second quantifies over all possible inputs from the environment, and hence it is not clear whether it can lead to a feasible proof technique.

Bisimilarity relies on *labelled transitions*: each evolution step of a system is tagged by some information aimed at capturing the possible interactions of a process with the environment. In [23] we provide a labelled transition system for ccp and put forward a notion of ccp bisimilarity. Intuitively, labels represent the minimal information that processes require from the environment to execute. In [33] we show that, unlike previous approaches, our notion of bisimilarity coincides with the standard notion of equivalence for (deterministic) ccp. This way we provide ccp with an alternative co-inductive proof technique, coherent with previous equivalences, for process behaviour.

In [28] we give an account of some of the most representative *concurrent constraint programming* formalisms for the specification and verification of reactive and timed systems. We focus on the semantic and logical aspects of these frameworks. We also discuss probabilistic, stochastic and mobile extensions of ccp as well as several existing working ccp systems.

6.2.2. Expressiveness of Process Calculi

The interaction between the means to specify local and infinite behaviour is fundamental for the expressiveness of process calculi. In [35] we study the expressive power local names in CCS!, the variant of CCS where infinite behaviour is expressed by a replication operation. In particular we prove that if an action is to be performed by a process in CCS!, that action should be reachable in a number of labelled transitions bounded by an exponential function that depends only in the maximal depth of nesting of local names of that process. By determining this function, and given the image-finiteness of corresponding transition system, we prove the decidability of the reachability problem for CCS!. The decidability of reachability for CCS! can alternatively be derived from the results in [37] using a process construction, and the theory of well-structure transition systems. However, while the complexity issue is not addressed in [37], the results in [35] provide a decision procedure for reachability whose complexity is determined by the maximal depth of nesting of local names.

6.3. Randomness

Unpredictable phenomena are omnipresent in natural and artificial processes. In classical physical systems (and by this we mean also relativistic ones) randomness may be defined as 'deterministic unpredictability'. That is, since Poincaré's results (on the Three Body Problem) and his invention of the geometry of dynamical systems, deterministic systems include various forms of chaotic ones, from weak (mixing) systems to ones highly sensitive to border conditions, where random behaviors are part of the deterministic evolutions. Randomness got a new status with the birth of quantum mechanics: access to information on a given systems passes through a nondeterministic process (measurement). In computer sciences, randomness is at the core of algorithmic information theory, all the while nondeterministic algorithms and networks present crucial random aspects. Finally, an extensive use of randomness is made also in biology.

In [29] we discuss the concept of randomness in these different fiels, and we try to distill the common features. The purpose is to get a better understanding of the randomn phaenomena, and lay the ground for a general theory of randomness.

6.4. Web services

One of the objective of component based architectures is to automate the design of reliable system by assembling components chosen from a poll. This approach is for example particularly interesting in the context of web services. To reach such an objective, we need to formally define the service that the synthesized system is expected to provide. In [25], we propose a notion of modal specification of services. This notion extends the notion of modal specification introduced in [41] by adding concepts of partial observation and service termination. We provide an algorithm to compute a controller, an extra component, that enforce a service specification on a given finite state system. In the context of security, this work can also be seen as a contribution to the enforcement of availability properties by supervisory control, complementing the line of work on control for safety [13] and for confidentiality [36], [46], [43].

6.5. Compositional Modeling of Signaling Pathways

The biological data regarding the signaling pathways often consider single pathways or a small number of them. In [24] we propose a methodology for composing this kind of data in a coherent framework, in order to be able to investigate a bigger number of signaling pathways. We specify a biological system by means of a set of stoichiometric-like equations resembling the essential features of molecular interactions. We represent these equations by a timed concurrent constraint (ntcc) language, which can deal with partial information and the time for a reaction to occur. We describe a freely available prototypical implementation of our framework.

7. Other Grants and Activities

7.1. National Initiatives

7.1.1. ANR project PANDA: "Analyse du Parallélisme et de la Distribution"

This project is financed by the ANR, for the years 2009-2011. The partners involved are:

- EPIs Comète and Parsifal at INRIA Saclay. Responsible: Catuscia Palamidessi
- CEA Saclay. Responsible: Emmanuel Haucourt
- Pôle Parisien. Responsible: Damiano Mazza
- Pôle Méditerranéen. Responsible: Emmanuel Godard
- Airbus. Responsible: Jean Souyris.

7.1.2. ANR project CPP: Confidence, Proofs and Probabilities

This project is financed by the ANR, for the years 2009-2011. The partners involved are:

- LSV. Responsible: Jean Goubault-Larrecq
- EPIs Comète and Parsifal at INRIA Saclay. Responsible: Catuscia Palamidessi
- CEA LIST. Responsible: Olivier Bouissou
- Supelec SSE. Responsible: Gilles Fleury
- Supelec L2S. Responsible: Michel Kieffer

7.2. International Initiatives

7.2.1. DRI Equipe Associée PRINTEMPS

PRINTEMPS (PRobability and INformation Theory for Modeling Privacy and Secrecy) focuses on the applications of Information Theory to security. We are particularly interested in studying the interactions between Concurrency and Information Theory.

This project has started in January 2006 and includes the following sites:

- INRIA Futurs. Responsible: C. Palamidessi
- McGill University, Canada. Responsible: P. Panangaden

Home page: http://www.lix.polytechnique.fr/comete/Projects/Printemps/.

7.2.2. DRI Equipe Associée FORCES

FORCES (FORmalisms from Concurrency for Emergent Systems) aims at providing more robust formalisms for analyzing the emergent systems our teams have been modeling during recent years, namely: Security Protocols, Biological Systems and Multimedia Semantic Interaction.

This project has started in January 2007 and includes the following sites:

- Pontificia Universidad Javeriana, Colombia. Responsible: C. Rueda
- INRIA Futurs. Responsible: F. Valencia
- IRCAM, France.

Home page: http://www.lix.polytechnique.fr/comete/Forces/.

8. Dissemination

8.1. Animation of the scientific community

Note: In this section we include only the activities of the permanent internal members of Comète.

8.1.1. Editorial activity

Catuscia Palamidessi is:

- Member of the Editorial Board of the journal on Mathematical Structures in Computer Science, published by the Cambridge University Press.
- Member of the Editorial Board of the journal on Theory and Practice of Logic Programming, published by the Cambridge University Press.
- Member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, Elsevier Science.
- Co-editor of the special issue of the Journal of Computer Security dedicated to a selection of the best papers presented at SECCO'07 [30].

Frank D. Valencia is:

- Area editor (for the area of Concurrency) of the ALP Newsletter.
- Co-editor of the proceedings of the 17th International Workshop on Expressiveness in Concurrency [31].

8.1.2. Steering Committees

Catuscia Palamidessi is member of:

- The Council of EATCS, the European Association for Theoretical Computer Science. Since 2005.
- The Steering Committee of ETAPS, the European Joint Conferences on Theory and Practice of Software. Since 2006.
- The IFIP Technical Committee 1 – Foundations of Computer Science. Since 2007.
- The IFIP Working Group 2.2 – Formal Description of Programming Concepts. Since 2001.
- The IFIP Working Group 1.7 – Theoretical Foundations of Security Analysis and Design. Since 2010.

8.1.3. Invited Talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

- BCTCS 2010. The British Colloquium for Theoretical Computer Science. Edinburgh, UK. April 2010. http://www.bctcs.ac.uk/BCTCS2010/.
- ARSPA-WITS'10. The Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security. Paphos, Cyprus, March 2010. http://www.avantssar.eu/arspa-wits10/. Affiliated with ETAPS 2010. http://www.etaps10.cs.ucy.ac.cy/.
- The Amir Pnueli Memorial Symposium. New York, USA, May 2010. http://www.cs.nyu.edu/acsys/pnueli/.
- (Joint invited speaker) MPC 2010, the 10th International Conference on Mathematics of Program Construction, and AMAST 2010, the 13th International Conference on Algebraic Methodology And Software Technology. Manoir St-Castin, Québec, Canada, June 2010. http://mpc-amast2010.fsg.ulaval.ca/.
- LICS 2010. The Twenty-Fifth Annual IEEE Symposium on Logic in Computer Science, Edinburgh, UK, July 2010. http://www2.informatik.hu-berlin.de/lics/lics10/.
- (Joint invited speaker) SOS 2010, the workshop on Structural Operational Semantics (http://www.ru.is/faculty/luca/SOS2010/), and EXPRESS 2010, the workshop on Expressiveness in Concurrency Theory (http://csd.informatik.uni-oldenburg.de/~sib/EXPRESS10/). Affiliated to CONCUR 2010, the 21st International Conference in Concurrency Theory (http://concur2010.inria.fr/). Paris, August 2010.
- Dagstuhl seminar on Quantitative and Qualitative Analysis of Network Protocols (http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=10051). Schloss Dagstuhl, Germany, 31 Jan - 5 Feb 2010.

8.1.4. Organization of workshops and conferences

- Catuscia Palamidessi is serving as PC co-chair of the 2011 edition of QEST (The International Conference on Quantitative Evaluation of SysTems, http://www.qest.org/qest2011/).
- Catuscia Palamidessi is serving as PC chairs of the first edition of TOSCA (Theory Of SeCurity and Applications). To be held in 2011. Associated with the ETAPS conferences, http://www.etaps.org/.
- Frank Valencia has co-chaired EXPRESS 2010, the workshop on Expressiveness in Concurrency Theory (http://csd.informatik.uni-oldenburg.de/~sib/EXPRESS10/. Affiliated to CONCUR 2010, the 21st International Conference in Concurrency Theory (http://concur2010.inria.fr/). Paris, August 2010.

8.1.5. Participation in program committees

Catuscia Palamidessi has been/is a member of the program committees of the following conferences:

- MFPS XXVI. The 26th Conference on the Mathematical Foundations of Programming Semantics. Ottawa, Canada, May 2010. http://www.math.tulane.edu/~mfps/mfps26/MFPS_XXVI.html
- CONCUR 2010. The 21st International Conference on Concurrency Theory. Paris, France, September 2010. http://concur2010.inria.fr/
- MFPS XXVII. The 27th Conference on the Mathematical Foundations of Programming Semantics, Carnegie Mellon University, Pittsburgh, May 2011. http://129.81.170.14/~mfps/MFPS27/MFPS27/MFPS_XXVII.html
- CSF 2011. The 24th IEEE Computer Security Foundations Symposium. Abbaye des Vaux de Cernay, France, June 2011. http://csf2011.inria.fr/
- CALCO 2011. Fourth International Conference on Algebra and Coalgebra in Computer Science. Winchester, UK, August 2011. http://calco2011.ecs.soton.ac.uk/

Frank D. Valencia has been a member of the program committee of ICLP 2010, the 26th International Conference in Logic Programming. Edinburgh, UK, July 2010. http://www.floc-conference.org/ICLP-home.html.

Catuscia Palamidessi has been/is a member of the program committees of the following workshops:

- FCS-PrivMod 2010. Workshop on Foundations of Security and Privacy. Edinburgh, UK, July 2010. http://www.loria.fr/~cortier/FCS-PrivMod10/
- LIS 2010. Workshop on Logics in Security. Copenhagen, Denmark, August 2010. http://lis.gforge.uni.lu
- SVT 2011. Software Verification and Testing track of the 26th Annual ACM Symposium On Applied Computing. Tunghai University, TaiChung, Taiwan, March 2011. http://www.acm.org/conferences/sac/sac2011/.

8.1.6. Participation in other committees

Catuscia Palamidessi has served in the following committees:

- The LICS 2011 Test Of Time Award Committee.
- The EAPLS PhD Award (http://eapls.org/pages/phd_award/). Since 2010.

8.1.7. Organization of seminars

- Frank D. Valencia and Andrés Aristizábal are the organizer of the Comète-Parsifal Seminar. This seminar takes place weekly at LIX, and it is meant as a forum where the members of Comète and Parsifal present their current works and exchange ideas. See http://www.lix.polytechnique.fr/comete/seminar/.

8.2. Visitors

- Miguel Andrés, PhD student, University of Nijmegen, NL. He has visited Comète for several months (January, April, September and November) in 2010.
- Linda Brodo, Assistant Professor, University of Sassari, Italy. She has visited Comète for one month in June 2010.
- Pierpaolo Degano, Professor, University of Pisa, Italy. He has visited Comète for three months from June till September 2010.
- Moreno Falaschi, Professor, University of Siena, Italy. He has visited Comète for one month in June 2010.
- Vladimiro Sassone, Professor, University of Southampton, UK. He has visited Comète for three weeks from August 15 till September 8, 2010.

8.3. Service

Catuscia Palamidessi has served as:

- Member of the Commission Scientifique du Centre de Recherche INRIA Saclay, From February 2008 till March 2010.
- Reviewer for the projects proposal for the program PRIN, sponsored by the Italian MIUR ("Ministero dell'Istruzione, dell'Università e della Ricerca"). Since 2004.
- Member of the Comité d'Orientation Scientifique et Technique, Groupe de travail Relation Internationales (COST-GTRI). Since November 2007.
- Member of the Comité de These for Mathematics and Computer Science at the École Polytechnique. Since October 2007.
- Directrice adjointe du LIX, le Laboratoire d'Informatique de l'Ecole Polytechnique. Since April 2010.
- Member of the Evaluation Committee for the LIX/CNRS chair, 2010-11.
- Member of the Comité Academique de l'Ecole Polytechnique. Since November 2010.

Frank Valencia has served as:

- Member of the Evaluation Committee of the LIX/Qualcomm postdoc grants for the year 2010.
- Member of the Evaluation Committee for the LIX/CNRS chair, 2010-11.

8.4. Teaching

8.4.1. Postgraduate

- Frank Valencia is teaching (together with Francesco Zappa Nardelli, James Leifer and Emmanuel Haucourt) the course "Concurrence" at the "Master Parisien de Recherche en Informatique" (MPRI) in Paris. Total 12 hours. Winter semester 2010-11.

8.4.2. Undergraduate

- Frank D. Valencia has been a lecturer on Process Modelling at the Masters Program in Computer Science of the Pontificia Universidad Javeriana de Cali. January 2010 and Fall 2010. Total 60 hours.

8.5. Advising

8.5.1. PhD students

Catuscia Palamidessi has supervised the following PhD students:

- Christelle Braun. Allocataire École Polytechnique - Ministère. 1/10/2007 – 17/5/2010.
- Sophia Knight. Allocataire INRIA/CORDIS. Since 15/9/2010.
- Mário Sergio Ferreira Alvim Junior. Allocataire CNRS/DGA. Since 1/10/2008.
- Ivan Gazeau. Allocataire ANR. Co-supervised by Dale Miller, Ecole Polytechnique, Paris. Since 1/10/2009.
- Marie-Aude Steineur. Allocataire ANR. Co-supervised by Sami Abbes, University of Paris VII, France. Since 1/10/2009.

Catuscia Palamidessi and Frank Valencia have co-supervised the following PhD students

- Andrés Aristizábal. Allocataire DGA/CNRS. Since 1/10/2009.

8.5.2. Internships

The team Comète has supervised the following internship students during 2010:

- Luis Fernando Pino Duque. Master student at the University of Cali, Colombia. 5/11/2009 – 5/12/2009

8.5.3. PhD defenses

Catuscia Palamidessi has been "rapporteur" for the thesis of the following PhD students:

- Antonio Vitale (University of Bologna, Italy). PhD thesis on *Expressiveness in biologically inspired languages*. Advised by Cosimo Laneve. Defended in Spring 2010.
- Andrea Turrini (University of Verona, Italy). PhD thesis on *Hierarchical and compositional verification of cryptographic protocols*. Advised by Roberto Segala. Defended in Spring 2010.

Catuscia Palamidessi has also been opponent for the PhD thesis of Magnus Johansson (Dept. of Information Technology, Uppsala University). Title of the thesis: *Psi-calculi: a framework for mobile process calculi: Cook your own correct process calculus - just add data and logic*. Advidsed by Björn Victor and Joachim Parrow. Defended on 31 May 2010.

9. Bibliography

Major publications by the team in recent years

[1] D. CACCIAGRANO, F. CORRADINI, C. PALAMIDESSI. *Separation of synchronous and asynchronous communication via testing*, in "Theoretical Computer Science", 2007, vol. 386, n° 3, p. 218-235, http://hal.inria.fr/inria-00200916/en/.

[2] K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Making Random Choices Invisible to the Scheduler*, in "Information and Computation", 2010, vol. 208, n° 6, p. 694-715 [*DOI :* 10.1016/J.IC.2009.06.006], http://hal.inria.fr/inria-00424860/en.

[3] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, P. PANANGADEN. *Anonymity Protocols as Noisy Channels*, in "Information and Computation", 2008, vol. 206, n° 2–4, p. 378–401 [*DOI :* 10.1016/J.IC.2007.07.003], http://hal.inria.fr/inria-00349225/en/.

[4] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, P. PANANGADEN. *On the Bayes risk in information-hiding protocols*, in "Journal of Computer Security", 2008, vol. 16, n° 5, p. 531–571 [*DOI :* 10.3233/JCS-2008-0333], http://hal.inria.fr/inria-00349224/en/.

[5] Y. DENG, C. PALAMIDESSI. *Axiomatizations for probabilistic finite-state behaviors*, in "Theoretical Computer Science", 2007, vol. 373, n° 1-2, p. 92–114, http://hal.inria.fr/inria-00200928/en/.

[6] P. GIAMBIAGI, G. SCHNEIDER, F. D. VALENCIA. *On the Expressiveness of Infinite Behavior and Name Scoping in Process Calculi.*, in "Proceedings of FoSSaCS", Lecture Notes in Computer Science, Springer, 2004, vol. 2987, p. 226-240, http://www.brics.dk/~fvalenci/papers/fossacs04.pdf.

[7] C. PALAMIDESSI, O. M. HERESCU. *A randomized encoding of the π-calculus with mixed choice*, in "Theoretical Computer Science", 2005, vol. 335, n° 2-3, p. 73-404, http://hal.inria.fr/inria-00201105/en/.

[8] C. PALAMIDESSI. *Comparing the Expressive Power of the Synchronous and the Asynchronous pi-calculus*, in "Mathematical Structures in Computer Science", 2003, vol. 13, n° 5, p. 685–719, http://hal.inria.fr/inria-00201104/en/.

[9] C. PALAMIDESSI, V. A. SARASWAT, F. D. VALENCIA, B. VICTOR. *On the Expressiveness of Linearity vs Persistence in the Asynchronous pi-calculus*, in "Proceedings of the Twenty First Annual IEEE Symposium on Logic in Computer Science (LICS)", IEEE Computer Society, 2006, p. 59–68, http://hal.inria.fr/inria-00201096/en/.

[10] F. D. VALENCIA. *Decidability of infinite-state timed CCP processes and first-order LTL*, in "Theoretical Computer Science", 2005, vol. 330, n° 3, p. 577–607, http://www.brics.dk/~fvalenci/papers/tcs.pdf.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] C. BRAUN. *Quantitative Approaches to Information Hiding*, Ecole Polytechnique X, May 2010, http://hal.inria.fr/tel-00527367/en.

Articles in International Peer-Reviewed Journal

[12] K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Making Random Choices Invisible to the Scheduler*, in "Information and Computation", 2010, vol. 208, n° 6, p. 694-715 [*DOI :* 10.1016/J.IC.2009.06.006], http://hal.inria.fr/inria-00424860/en.

[13] J. DUBREIL, P. DARONDEAU, H. MARCHAND. *Supervisory Control for Opacity*, in "IEEE Transactions on Automatic Control", May 2010, http://hal.archives-ouvertes.fr/inria-00483891/en.

[14] S. KRAMER, J. C. BRADFIELD. *A general definition of malware*, in "Journal in Computer Virology", 2010, vol. 6, n° 2, p. 105-114, http://www.springerlink.com/content/x537315445477225/.

Invited Conferences

[15] M. S. ALVIM, M. E. ANDRÉS, C. PALAMIDESSI. *Probabilistic Information Flow*, in "25th Annual IEEE Symposium on Logic in Computer Science (LICS 2010)", Edinburgh, United Kingdom, IEEE Computer Society, 2010, p. 314-321 [*DOI :* 10.1109/LICS.2010.53], http://hal.inria.fr/hal-00548200/en.

[16] M. S. ALVIM, M. E. ANDRÉS, C. PALAMIDESSI. *Entropy and Attack Models in Information Flow*, in "6th IFIP International Conference on Theoretical Computer Science (TCS 2010)", Brisbane, Australia, C. S. CALUDE, V. SASSONE (editors), IFIP Advances in Information and Communication Technology, Springer, 2010, vol. 323, p. 53-54 [*DOI :* 10.1007/978-3-642-15240-5_4], http://hal.archives-ouvertes.fr/hal-00548212/en/.

[17] C. PALAMIDESSI. *Compositionality of Secure Information Flow*, in "Joint Conference: 10th International Conference on the Mathematics of Program Construction (MPC 2010), and 13th International Conference on Algebraic Methodology And Software Technology (AMAST 2010)", Lac Beaufort, Québec City, Canada, C. BOLDUC, J. DESHARNAIS, B. KTARI (editors), Lecture Notes in Computer Science, Springer, 2010, vol. 6120, p. 19-19 [*DOI :* 10.1007/978-3-642-13321-3_2], http://hal.archives-ouvertes.fr/hal-00548210/en/.

[18] C. PALAMIDESSI, M. S. ALVIM, M. E. ANDRÉS. *Interactive Information Flow*, in "Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS 2010)", Paphos, Cyprus, A. ARMANDO, G. LOWE (editors), Lecture Notes in Computer Science, Springer, 2010, vol. 6186, p. 111-111 [*DOI :* 10.1007/978-3-642-16074-5_8], http://hal.archives-ouvertes.fr/hal-00548211/en/.

International Peer-Reviewed Conference/Proceedings

[19] M. S. ALVIM, M. E. ANDRÉS, C. PALAMIDESSI. *Information Flow in Interactive Systems*, in "21th International Conference on Concurrency Theory (CONCUR 2010)", Paris, France, P. GASTIN, F. LAROUSSINIE (editors), Lecture Notes in Computer Science, Springer, 2010, vol. 6269, p. 102-116 [*DOI :* 10.1007/978-3-642-15375-4_8], http://hal.inria.fr/inria-00479672/en.

[20] M. S. ALVIM, M. E. ANDRÉS, C. PALAMIDESSI, P. VAN ROSSUM. *Safe Equivalences for Security Properties*, in "6th IFIP International Conference on Theoretical Computer Science (TCS 2010)", Brisbane, Australia, C. S. CALUDE, V. SASSONE (editors), IFIP Advances in Information and Communication Technology, Springer, 2010, vol. 323, p. 55-70 [*DOI :* 10.1007/978-3-642-15240-5_5], http://hal.inria.fr/inria-00479674/en.

[21] M. E. ANDRÉS, C. PALAMIDESSI, P. VAN ROSSUM, G. SMITH. *Computing the Leakage of Information-Hiding Systems*, in "16th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2010)", Cyprus, J. ESPARZA, R. MAJUMDAR (editors), Lecture Notes in Computer Science, Springer, 2010, vol. 6015, p. 373-389 [*DOI :* 10.1007/978-3-642-12002-2_32], http://hal.inria.fr/hal-00445445/en.

[22] M. E. ANDRÉS, C. PALAMIDESSI, P. VAN ROSSUM, A. SOKOLOVA. *Information Hiding in Probabilistic Concurrent Systems*, in "7th IEEE International Conference on Quantitative Evaluation of SysTems (QEST 2010)", Williamsburg, VA, USA, IEEE Computer Society, 2010, p. 17-26 [*DOI :* 10.1109/QEST.2010.11], http://hal.inria.fr/hal-00548187/en.

[23] A. A. ARISTIZÁBAL P.. *Bisimilarity in Concurrent Constraint Programming*, in "Technical Communications of the 26th International Conference on Logic Programming (ICLP 2010)", Edinburgh, United Kingdom, M. V. HERMENEGILDO, T. SCHAUB (editors), Leibniz International Proceedings in Informatics, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, July 2010, vol. 7, p. 236-240, Short paper accepted at the Doctoral Programme of ICLP'2010 [*DOI :* 10.4230/LIPICS.ICLP.2010.236], http://hal.inria.fr/hal-00546857/en.

[24] D. CHIARUGI, M. FALASCHI, C. OLARTE, C. PALAMIDESSI. *Compositional modelling of signalling pathways in timed concurrent constraint programming*, in "First ACM International Conference on Bioinformatics and Computational Biology (BCB 2010)", Niagara Falls, New York, USA, ACM Digital Libraries, 2010, p. 414-417 [*DOI :* 10.1145/1854776.1854843], http://hal.inria.fr/hal-00548213/en.

[25] P. DARONDEAU, J. DUBREIL, H. MARCHAND. *Supervisory Control for Modal Specifications of Services*, in "Workshop on Discrete Event Systems (WODES 2010)", Berlin, Germany, August 2010, p. 428-435, http://hal.inria.fr/inria-00510013/en.

[26] S. HAMADOU, C. PALAMIDESSI, V. SASSONE, E. EL SALAMOUNY. *Probable Innocence and Independent Knowledge*, in "Postproceedings of the 6th International Workshop on Formal Aspects in Security and Trust", Eindhoven, The Netherlands, P. DEGANO, J. D. GUTTMAN (editors), Lecture Notes in Computer Science, Springer, 2010, vol. 5983, p. 141-156 [*DOI :* 10.1007/978-3-642-12459-4_11], http://hal.inria.fr/inria-00424853/en.

[27] S. HAMADOU, V. SASSONE, C. PALAMIDESSI. *Reconciling Belief and Vulnerability in Information Flow*, in "31st IEEE Symposium on Security and Privacy", Berleley/Oakland, California, USA, IEEE Computer Society, 2010, p. 79-92 [*DOI :* 10.1109/SP.2010.13], http://hal.inria.fr/inria-00548007/en.

Scientific Books (or Scientific Book chapters)

[28] M. GABBRIELLI, C. PALAMIDESSI, F. D. VALENCIA. *Concurrent and Reactive Constraint Programming*, in "A 25-Year Perspective on Logic Programming", A. DOVIER, E. PONTELLI (editors), Springer, June 2010, p. 231-253 [*DOI :* 10.1007/978-3-642-14309-0_11], http://hal.inria.fr/hal-00545256/en.

[29] G. LONGO, C. PALAMIDESSI, P. THIERRY. *Some Bridging Results and Challenges in Classical, Quantum and Computational Randomness*, in "Randomness Through Computation", H. ZENIL (editor), World Scientific, 2011, ISBN: 978-981-4327-74-9, http://hal.inria.fr/hal-00445553/en.

Books or Proceedings Editing

[30] D. GORLA, C. PALAMIDESSI (editors). *Journal of Computer Security 18(2). Special Issue dedicated to a selection of the best papers presented at SECCO'07*, IOS Press, 2010 [*DOI :* 10.3233/JCS-2010-0359], http://hal.inria.fr/hal-00548217/en.

[31] F. D. VALENCIA, S. FRÖSCHLE (editors). *Proceedings of the 17th International Workshop on Expressiveness in Concurrency*, Electronic Proceedings in Theoretical Computer Science, November 2010 [*DOI :* 10.4204/EPTCS.41], http://hal.inria.fr/hal-00547314/en.

Research Reports

[32] M. S. ALVIM, K. CHATZIKOKOLAKIS, P. DEGANO, C. PALAMIDESSI. *Differential Privacy versus Quantitative Information Flow*, INRIA, 2010, http://hal.inria.fr/hal-00548214/en.

[33] A. A. ARISTIZÁBAL P., F. BONCHI, C. PALAMIDESSI, L. PINO, F. D. VALENCIA. *Deriving Labels and Bisimilarity for Concurrent Constraint Programming*, INRIA, 2010, Accepted at FoSSaCS 2011, the 14th International Conference on Foundations of Software Science an Computation Structures (FOSSACS 2011). To be published by Springer in the Lecture Notes in Computer Science series, http://hal.inria.fr/hal-00546722/en.

[34] P. DARONDEAU, J. DUBREIL, H. MARCHAND. *Supervisory Control for Modal Specifications of Services*, INRIA, April 2010, n^{o} RR-7247, http://hal.inria.fr/inria-00472736/en.

[35] L. PINO. *Analysis of the reachability problem in fragments of the Pi-calculus*, Universidad del Valle, Colombia, 2010, BSc Thesis from Universidad del Valle, Colombia, http://hal.inria.fr/hal-00546849/en.

References in notes

[36] E. BADOUEL, M. A. BEDNARCZYK, A. M. BORZYSZKOWSKI, B. CAILLAUD, P. DARONDEAU. *Concurrent Secrets*, in "8th Workshop on Discrete Event Systems, WODES'06", Ann Arbor, Michigan, USA, S. LAFORTUNE, F. LIN, D. TILBURY (editors), July 2006.

[37] N. BUSI, M. GABBRIELLI, G. ZAVATTARO. *Comparing Recursion, Replication, and Iteration in Process Calculi*, in "Proc. of ICALP 04", LNCS, Springer-Verlag, 2004.

[38] R. CANETTI, L. CHEUNG, N. LYNCH, O. PEREIRA. *On the Role of Scheduling in Simulation-Based Security*, 2007, Cryptology ePrint Archive, Report 2007/102.

[39] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, P. PANANGADEN. *Anonymity Protocols as Noisy Channels*, in "Inf. and Comp.", 2008, vol. 206, n^{o} 2–4, p. 378–401 [*DOI :* 10.1016/J.IC.2007.07.003], http://hal.inria.fr/inria-00349225/en/.

[40] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, P. PANANGADEN. *On the Bayes risk in information-hiding protocols*, in "Journal of Computer Security", 2008, vol. 16, n^{o} 5, p. 531–571 [*DOI :* 10.3233/JCS-2008-0333], http://hal.inria.fr/inria-00349224/en/.

[41] J. DUBREIL, P. DARONDEAU, H. MARCHAND. *Opacity Enforcing Control Synthesis*, in "Proceedings of the 9th International Workshop on Discrete Event Systems (WODES'08)", Göteborg, Sweden, IEEE, May 2008, p. 28-35, http://www.lix.polytechnique.fr/~dubreil/publications/2008-Wodes-Opacity.pdf.

[42] T. HOARE, R. MILNER. *Grand Challenges for Computing Research*, in "Computer Journal", 2005, vol. 48, n^{o} 1, p. 49-52.

[43] K. LARSEN. *Modal specifications*, in "Automatic Verification Methods for Finite State Systems", J. SIFAKIS (editor), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 1990, vol. 407, p. 232-246.

[44] N. P. MENDLER, P. PANANGADEN, P. J. SCOTT, R. A. G. SEELY. *A Logical View of Concurrent Constraint Programming*, in "Nord. J. Comput.", 1995, vol. 2, n^{o} 2, p. 181-220.

[45] G. NORMAN, C. PALAMIDESSI, D. PARKER, P. WU. *Model checking probabilistic and stochastic extensions of the π-calculus*, in "IEEE Transactions of Software Engineering", 2009, vol. 35, n^{o} 2, p. 209–223, http://hal.archives-ouvertes.fr/inria-00424856/en/.

[46] P. J. RAMADGE, W. M. WONHAM. *The Control of Discrete Event Systems*, in "Proceedings of the IEEE; Special issue on Dynamics of Discrete Event Systems", 1989, vol. 77, n^{o} 1, p. 81-98.

[47] V. A. SARASWAT, M. C. RINARD. *Concurrent Constraint Programming*, in "POPL", ACM Press, 1990, p. 232-245.

[48] P. WU, C. PALAMIDESSI, H. LIN. *Symbolic Bisimulation for Probabilistic Systems*, in "Proceedings of 4th International Conference on the Quantitative Evaluation of SysTems (QEST)", IEEE Computer Society, 2007, p. 179-188, http://www.lix.polytechnique.fr/~catuscia/papers/Wu/qest2.pdf.