INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Comète

Concurrence, Mobilité et Transactions

Saclay - Île-de-France

Theme : Programs, Verification and Proofs

Table of contents

Joint team with LIX (Laboratoire d'Informatique de l'École Polytechnique) and CNRS.

1. Team

Research Scientist

Catuscia Palamidessi [Team Leader, Research Director (DR), INRIA, HdR]
Frank Valencia [Research Associate (CR) CNRS]

External Collaborator

Konstantinos Chatzikokolakis [Univ. of Eindhoven, NL. Ex PhD student of Comète. He defended his thesis on 26/10/2007]

PhD Student

Jesus Aranda [Co-supervised by Juan Francisco Diaz, Universidad del Valle, Colombia. 1/10/2006 – 31/11/2009]
Andrés Aristizábal [Allocataire DGA/CNRS. Since 1/10/2009]
Romain Beauxis [Allocataire Region Ile de France. 1/10/2005 – 31/5/2009]
Christelle Braun [Allocataire École Polytechnique - Ministère. Since 1/10/2007]
Mario Sergio Ferreira Alvim Junior [Allocataire DGA/CNRS. Since 1/10/2008]
Ivan Gazeau [Allocataire ANR. Co-supervised by Dale Miller, INRIA. Since 1/10/2009]
Carlos Olarte [Allocataire INRIA/CORDIS. 1/10/2006 – 30/10/2009]
Sylvain Pradalier [Allocataire ENS Cachan. Co-supervised by Cosimo Laneve, University of Bologna, Italy. 1/9/2006 – 30/9/2009]
Marie-Aude Steineur [Allocataire ANR. Co-supervised by Sami Abbes, Paris VII. Since 1/10/2009]

Post-Doctoral Fellow

Filippo Bonchi [Grant ERCIM. Since 1/11/2009]
Jérémy Dubreil [Grant INRIA. Since 1/12/2009]

Visiting Scientist

Miguel Andrés [PhD student, University of Nijmegen, NL. Three months: May, September and October]
Linda Brodo [Assistant Professor, University of Sassari, Italy. One month: January]
Marzia Buscemi [Postdoc, IMT Lucca Institute for Advanced Studies, Italy. Two months: January 15 – March 15]
Ehab El-Salamouny [PhD student, University of Southampton, UK. Two weeks: January 7 – January 21]
Moreno Falaschi [Professor, University of Siena, Italy. Three months: January, July and September]
Sardaouna Hamadou [Postdoc, University of Southampton, UK. Two weeks: August 15 – August 31]
Cosimo Laneve [Professor, University of Bologna, Italy. Two months: May 15 – July 15]
Geoffrey Smith [Associate Professor, Florida University, USA. One month: June 3 – July 3]
Antonio Vitale [PhD student, University of Bologna, Italy. Three months: June, July and September]

Administrative Assistant

Marie-Jeanne Gaffard [Secretary (SAR) INRIA]

Other

Michael Martinez [Stagiare. University of Cali, Colombia. Three months: May 1 – July 31]
Yamil Salim Percy [Stagiare. University of Cali, Colombia. One month: Nov 5 – Dec 5]

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* [46]). *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*.

These systems 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 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, computer scientists 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 and Frank Valencia have served as PC chairs of the 2009 edition of the conference SOFSEM (Current Trends in Theory and Practice of Computer Science, http://www.ksi.mff.cuni.cz/sofsem09/index.php).
- Catuscia Palamidessi has served as PC chairs of the 2009 edition of the conference MFPS (Mathematical Foundations of Programming Semantics XXV, http://www.math.tulane.edu/~mfps/mfps25.htm).
- Catuscia Palamidessi has been invited to serve as PC chairs 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 be a 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/).
- Acceptance of the ANR project proposal PANDA: "Analyse du Parallélisme et de la Distribution". This project is financed by the ANR, for the years 2009-2011. The partners involved are: the EPIs Comète and Parsifal at INRIA Saclay, the CEA Saclay, Airbus, and various universities in France.
- Acceptance of the ANR project proposal CPP: Mobile and Secure Complex Systems This project is financed by the ANR, for the years 2009-2011. The partners involved are: LSV, the EPIs Comète and Parsifal at INRIA Saclay, the CEA LIST, Supelec SSE and Supelec L2S.

3. Scientific Foundations

3.1. Probabilistic aspects

Participants: Miguel Andrés, Romain Beauxis, Filippo Bonchi, Christelle Braun, Jérémy Dubreil, Mario Sergio Ferreira Alvim Junior, Ivan Gazeau, Catuscia Palamidessi, Sylvain Pradalier, Marie-Aude Steineur.

The need to deal with probabilities 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 one can refine by statistical measurements, and which can then be naturally represented 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: Jesus Aranda, Andrés Aristizábal, Romain Beauxis, Filippo Bonchi, Christelle Braun, Catuscia Palamidessi, Carlos Olarte, Frank Valencia, Antonio Vitale.

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: Jesus Aranda, Romain Beauxis, Christelle Braun, Catuscia Palamidessi, Frank Valencia.

We will focus our efforts on a probabilistic variant of the asynchronous π-calculus, that 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, Romain Beauxis, Christelle Braun, Jérémy Dubreil, Mario Sergio Ferreira Alvim Junior, Catuscia Palamidessi, Geoffrey Smith.

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 case that 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, Romain Beauxis, 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. These are (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: Romain Beauxis [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 [42] 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 [43] 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.

6. New Results

6.1. Expressive power of models and formalisms for concurrency

Participants: Jesus Aranda, Romain Beauxis, Catuscia Palamidessi, Frank Valencia.

6.1.1. On the Expressive Power of Restriction in CCS with Replication

Busi et al. [40] showed that $\text{CCS}_!$ (CCS with replication instead of recursion) is Turing powerful by providing an encoding of Random Access Machines (RAMs) which preserves and reflects *convergence* (i.e., the existence of terminating computations). The encoding uses an unbounded number of restrictions arising from having restriction operators under the scope of replication. On the other hand, in [39] they had shown that there is no encoding of RAMs into $\text{CCS}_!$ which preserves and reflects divergence.

In [23] we have studied the expressive power of restriction and its interplay with replication. We have done this by considering several syntactic variants of $\text{CCS}_!$ which differ from each other in the use of restriction with respect to replication. We have considered three syntactic variations which do not allow the use of an unbounded number of restrictions: $\text{CCS}_!^{-!\nu}$ is the fragment of $\text{CCS}_!$ not allowing restrictions under the scope of a replication. $\text{CCS}_!^{-\nu}$ is the restriction-free fragment of $\text{CCS}_!$. The third variant is $\text{CCS}_{!+pr}^{-!\nu}$ which extends $\text{CCS}_!^{-!\nu}$ with PhillipÕs priority guards. We have shown that the use of unboundedly many restrictions in $\text{CCS}_!$ is necessary for obtaining Turing expressiveness in the sense of Busi et al. We have done this by showing that there is no encoding of RAMs into $\text{CCS}_!^{-!\nu}$ which preserves and reflects convergence. We have also proved that up to failures equivalence, there is no encoding from $\text{CCS}_!$ into $\text{CCS}_!^{-!\nu}$ nor from $\text{CCS}_!^{-!\nu}$ into $\text{CCS}_!^{-\nu}$. As lemmata for the above results we have proved that convergence is decidable for $\text{CCS}_!^{-!\nu}$ and that language equivalence is decidable for $\text{CCS}_!^{-\nu}$. As corollary it follows that convergence is decidable for restriction-free CCS. Finally, we have shown the expressive power of priorities by providing an encoding of RAMs in $\text{CCS}_{!+pr}^{-!\nu}$: Not only does the encoding preserve and reflect convergence but it also preserves and reflects divergence (the existence of infinite computations). This is to be contrasted with the result of Busi et al. mentioned above.

6.1.2. Linearity vs persistence

In his PhD thesis [11] Aranda has presented an expressiveness study of linearity vs persistence in the asynchronous π-calculus (Aπ), a representative process calculus, w.r.t. De Nicola and Hennessy's testing scenario which is sensitive to divergence. The work considers Aπ and three sub-languages of it, each capturing one source of persistence: the persistent-input Aπ-calculus (PIπ), the persistent-output Aπ-calculus (POπ) and the persistent Aπ-calculus (Pπ). It is shown that, under some general conditions related to compositionality of the encoding and preservation of the infinite behaviour, there cannot be an encoding from Aπ into a (semi)-persistent calculus preserving the must testing semantics. It also shown that, unlike for Aπ, convergence and divergence are decidable for POπ (and Pπ). As a consequence there is no encoding preserving and reflecting divergence or convergence from Aπ into POπ (and Pπ). This work confirms informal expressiveness claims in the literature of CCP.

6.1.3. Expressiveness of ntcc

In the context of the modeling expressiveness of process calculi, in [31] we have studied the suitability of the ntcc (nondeterministic timed concurrent constraint) calculus for modeling, simulating and analyzing biological systems. In particular, we have explored if it is possible to model membrane systems in ntcc. As the main contribution of this paper, we have proposed a general mechanism for modeling membrane systems in ntcc. The application of this mechanism has been illustrated with a model for the LDL cholesterol degradation pathway using membrane systems defined in ntcc. We have simulated the model of the LDL cholesterol degradation pathway by using ntccSim, a tool to run program specifications in ntcc.

6.1.4. Fairness

In [16] we have defined fair computations in the π-calculus. We have followed Costa and Stirling's approach for CCS-like languages [44], [45] but exploited a more natural labeling method of process actions to filter out unfair process executions. The new labeling has allowed us to prove all the significant properties of the original one, such as unicity, persistence and disappearance of labels. It has also turned out that the labeled π-calculus is a conservative extension of the standard one. We have contrasted the existing fair testing notions [38], [48] with those that naturally arise by imposing weak and strong fairness. This comparison provides the expressiveness of the various fair testing-based semantics and emphasizes the discriminating power of the one already proposed in the literature.

6.1.5. On the asynchronous nature of the asynchronous π-calculus

In [12] and [37] we have addressed the question of what kind of asynchronous communication is exactly modeled by the asynchronous π-calculus (π_a). To this purpose we have defined a calculus $\pi_{\mathfrak{B}}$ where channels are represented explicitly as special buffer processes. The base language for $\pi_{\mathfrak{B}}$ is the (synchronous) π-calculus, except that ordinary processes communicate only via buffers. We have compared this calculus with π_a, and we have shown that there is a strong correspondence between π_a and $\pi_{\mathfrak{B}}$ in the case that buffers are bags: there are indeed encodings which map each π_a process into a strongly asynchronous bisimilar $\pi_{\mathfrak{B}}$ process, and each $\pi_{\mathfrak{B}}$ process into a weakly asynchronous bisimilar π_a process. In case the buffers are queues or stacks, on the contrary, the correspondence does not hold. We have shown indeed that it is not possible to translate a stack or a queue into a weakly asynchronous bisimilar π_a process. Actually, for stacks we have shown an even stronger result, namely that they cannot be encoded into weakly (asynchronous) bisimilar processes in a π-calculus without mixed choice.

6.2. Foundations of information hiding

Participants: Romain Beauxis, Christelle Braun, Konstantinos Chatzikokolakis, Mario Sergio Ferreira Alvim Junior, Catuscia Palamidessi.

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.

The systems for information hiding often use random mechanisms to obfuscate the link between the observables and the information to be protected. The random mechanisms can be described probabilistically, while the value of the secret may be totally unpredictable, irregular, and hence expressible only nondeterministically. Nondeterminism can also be present due to the interaction of the various component of the system.

6.2.1. Information-hiding in presence of probability and nondeterminism

Formal definitions of the concept of anonymity and information flow have been investigated in the past either in a totally nondeterministic framework, or in a purely probabilistic one. In [15], we have investigated a notion of anonymity which combines both probability and nondeterminism, and which is suitable for describing the most general situation in which the protocol and the users can have both probabilistic and nondeterministic behavior. We have also investigated the properties of the definition for the particular cases of purely nondeterministic users and purely probabilistic users. We have formulated the notions of anonymity in terms of probabilistic

automata, and we have described protocols and users as processes in the probabilistic π-calculus, whose semantics is again based on probabilistic automata.

6.2.2. The problem of the scheduler

It has been observed recently that in security the combination of nondeterminism and probability can be harmful, in the sense that the resolution of the nondeterminism can reveal the outcome of the probabilistic choices even though they are supposed to be secret [41]. This is known as the problem of the *information-leaking scheduler*. In [17] we have developed a linguistic (process-calculus) approach to this problem, and we have shown how to apply it to control the behavior of the scheduler in various anonymity examples.

6.2.3. Information theory and Bayes risk

Recent research in quantitative theories for information-hiding tend to converge towards the idea of modeling the system as a noisy channel in the information-theoretic sense. The notion of information leakage, or vulnerability of the system, has been related in some approaches to the concept of mutual information of the channel. A recent work of Smith [51] has shown, however, that if the attack consists in one single try, then the mutual information and other concepts based on Shannon entropy are not suitable, and he has proposed to use Rényi's min-entropy instead. In [25] we have considered and compared two different possibilities of defining the leakage, based on the Bayes risk, a concept related to Rényi min-entropy.

6.2.4.

In [27] we have analyzed the CROWDS anonymity protocol under the novel assumption that the attacker has independent knowledge on behavioural patterns of individual users. Under such conditions we have studied, reformulated and extend Reiter and Rubin's notion of probable innocence, and we have provided a new formalisation for it based on the concept of protocol vulnerability. Accordingly, we have established new formal relationships between protocol parameters and attackers' knowledge expressing necessary and sufficient conditions to ensure probable innocence.

6.2.5. Bounds on the leakage of the input distribution

In information hiding, an adversary that tries to infer the secret information has a higher probability of success if it knows the distribution on the secrets. In [24] we have shown that if the system leaks probabilistically some information about the secrets, (that is, if there is a probabilistic correlation between the secrets and some observables) then the adversary can approximate such distribution by repeating the observations. More precisely, it can approximate the distribution on the observables by computing their frequencies, and then derive the distribution on the secrets by using the correlation in the inverse direction. We have illustrate this method, and then we have studied the bounds on the approximation error associated with it, for various natural notions of error. As a case study, we have applied our results to Crowds, a protocol for anonymous communication.

6.3. Specification and verification of security protocols

Participants: Mario Sergio Ferreira Alvim Junior, Catuscia Palamidessi.

6.3.1. A doxastic logic for security

In [19] we have introduced a novel modal logic, namely the *doxastic μ-calculus with error control* (DμCEC). The distinguishing feature of our logic is to provide a combination of *dynamic* operators for belief (whence the attribute "doxastic") with a *control* on the possible error of apprehension of the perceived reality, and for internalized probability. Both operators are dynamic (non-monotonic) thanks to the possibility of combining them with temporal operators, and are parameterized with a lower and upper probability bound (the error control).

As an application, we have shown how to formalize *probabilistic anonymity* and *oblivious transfer* in the logic, and how to validate these formalizations on implementations specified in probabilistic CCS.

6.3.2. A General definition of malware

In [18] we have proposed a general, formal definition of *malware* in the language of *modal logic*. Our definition is general thanks to its abstract formulation, which, being abstract, is independent of — but nonetheless generally applicable to — the manifold concrete manifestations of malware. From our formulation of malware, we have derived equally general and formal definitions of *benware* (not malware), *anti-malware* ("antibodies" against malware), and *medware* ("medicine" for affected software). We have provided theoretical tools and practical techniques for the *detection*, *comparison*, and *classification* of malware and its derivatives.

6.4. Concurrent Constraint Programming

Participants: Romain Beauxis, Moreno Falaschi, Catuscia Palamidessi, Carlos Olarte, Frank Valencia.

6.4.1. A smooth probabilistic extension of concurrent constraint programming

Concurrent constraint programming (ccp, [50]) is a model of computation based on the notion of store as the information available for the process. Each process has access to a global store, with respect to which it tests and adds constraints. During the execution, the store can only increase. A domain-theoretic denotational semantics has been defined in [49], that maps a process to the supremum store that it can reach. It is then possible to compute this supremum store by a fixed point construction, based on the grammar of the process.

6.4.2. Universal timed concurrent constraint programming

in his PhD thesis [13], Olarte has studied a temporal concurrent constraint calculus as a model of concurrency for mobile, timed reactive systems. The study is conducted by developing a process calculus called utcc, Universal Temporal CCP. The thesis is that utcc is a model for concurrency where behavioral and declarative reasoning techniques coexist coherently, thus allowing for the specification and verification of mobile reactive systems in emergent application areas. The utcc calculus generalizes tcc with the ability to express mobility. Here mobility is understood as communication of private names as typically done for mobile systems and security protocols. The utcc calculus introduces parametric ask operations called abstractions that behave as persistent parametric asks during a time-interval but may disappear afterwards. The applicability of the calculus is shown in several domains of Computer Science. Namely, decidability of Pnueli's First-order Temporal Logic, closure-operator semantic characterization of security protocols, semantics of a Service-Oriented Computing language, and modeling of Dynamic Multimedia-Interaction systems.

6.4.3. Abstract interpretation

In [26] we have extended the semantics of constraint calculus tcc to a "collecting" semantics for the utcc calculus based on closure operators over sequences of constraints. Relying on this semantics, we have formalized the first general framework for data flow analyses of tcc and utcc programs by abstract interpretation techniques. The concrete and abstract semantics we have proposed are compositional, thus allowing us to reduce the complexity of data flow analyses. We have shown that our method is sound and parametric w.r.t. the abstract domain. Thus, different analyses can be performed by instantiating the framework. We have illustrated how it is possible to reuse abstract domains previously defined for logic programming, e.g., to perform a groundness analysis for tcc programs. We have shown the applicability of this analysis in the context of reactive systems. Furthermore, we have made also use of the abstract semantics to exhibit a secrecy flaw in a security protocol.

6.4.4. Declarative analysis of structured communications

In [28] we have described a unified concurrent-constraint framework for the declarative analysis of structured communications. By relying on the utcc constraint calculus, we have showed that in addition to the usual operational techniques from process calculi, the analysis of structured communications can elegantly exploit logic-based reasoning techniques. We have presented a concurrent constraint interpretation of the language for structured communications proposed by Honda, Vasconcelos, and Kubo [47]. Distinguishing features of our approach are: the possibility of including partial information (constraints) in the session model, the use of explicit time for reasoning about session duration and expiration, and a tight correspondence with logic, which formally relates session execution and linear-time temporal logic formulas.

6.4.5. Multimedia Interaction

In [29] we have argued for the utcc calculus as a declarative model for dynamic multimedia interaction systems. Firstly, we have shown that the notion of constraints as partial information allowed us to neatly define temporal relations between interactive agents or events. Secondly, we have shown that mobility in utcc allows for the specification of more flexible and expressive systems. Thirdly, by relying on the underlying temporal logic in utcc, we have shown how non-trivial temporal properties of the model can be verified. As an application we have proposed a model for dynamic interactive scores where interactive points can be defined to adapt the hierarchical structure of the score depending on the information inferred from the environment. Our model broadens the interaction mechanisms available for the composer in previous (more static) models.

6.4.6. Musical applications

In [30] we have illustrated that the constraint calculus ntcc is useful for modeling complex musical processes, in particular for music improvisation. For example, for the vertical dimension one can specify that a given process can nondeterministically choose any note satisfying a given constraint. For the horizontal dimension one can specify that the process can nondeterministically choose the time to play the note subject to a given time upper bound. This nondeterministic view is particularly suitable for processes representing a musician's choices when improvising. Similarly, the horizontal dimension may supply partial information on a rhythmic pattern that leaves room for variation while keeping a basic control. We have also illustrated how implementing a weaker ntcc model of a musical process may greatly simplify the formal verification of its properties. We have argued that this modeling strategy provides a "runnable specification" for music problems that eases the task of formally reasoning about them.

6.4.7. FORCES

In [22] we have provided an overview of of our associated-team FORCES focusing on its motivation, results and future research directions. FORCES (FORmalisms from Concurrency for Emergent Systems) is a Colombian-French project funded by the program of ÒEquipes AssociéesÓ of INRIA. The teams involved in this research collaboration are the Music Representation Research Group (IRCAM), AVISPA (Colciencias) and our team Comète. The main goal of the project is to provide more robust formalisms for analyzing the emergent systems our teams have been modeling during recent years: I.e., Security Protocols, Biological Systems and Multimedia Semantic Interaction. The results described in this sections were indeed obtained in the context of FORCES.

6.5. Model checking

Participants: Romain Beauxis, Catuscia Palamidessi.

Model checking is the main tool that we aim at developing for the verification of security protocols.

6.5.1. Model checking the probabilistic π-calculus

In [20], in collaboration with the PRISM team at Oxford, we have established the basis for an implementation of model checking for the probabilistic π-calculus. Building upon the (non-probabilistic) π-calculus model checker MMC [52], we have developed an automated procedure for constructing a Markov decision process representing a probabilistic π-calculus process. This representation can then be verified using existing probabilistic model checkers such as PRISM. Secondly, we have demonstrated how for a large class of systems an efficient, compositional approach can be applied, which uses our extension of MMC on each parallel component of the system and then translates the results into a higher-level model description for the PRISM tool.

6.5.2. Model checking techniques for computing the information leakage

In [21] we have addressed the problem of computing the information leakage of a system in an efficient way. We have proposed 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 have considered the interactive case and we have pointed out that the definition of associated channel proposed in literature is not sound. However, we have shown that the leakage can still be defined consistently, and that our methods extend smoothly to this case.

6.6. Modeling biological systems: The nanoκ calculus

Participants: Jesus Aranda, Sylvain Pradalier, Frank Valencia.

Nano-devices are molecular machines synthesized from molecular subcomponents whose functions are combined in order to perform the function of the machine. An important and characteristic feature of these devices is their intrinsic compositional nature. Therefore process-algebra formalisms are natural candidate for their modeling. In his PhD thesis [14], Pradalier has introduced a dialect of the κ-calculus, the nanoκ-calculus and has illustrated its relevance for the modeling and simulation of nano-devices with an example stemming from the collaboration with the chemistry department of bologna: the [2]RaH rotaxane. Pradalier has modeled it in nanoκ and has simulated its behaviour under various conditions of concentration. He was then able to show that some classical assumption about kinetic rates were not correct any longer in this setting. The κ-calculus has many advantages for the modelling of biochemical systems. In particular it is compact, easily reusable and modifiable and biological-like and thus easier to learn for biochemists. On the other hand the π-calculus, also often used to model biochemical systems, has a much more developed theory and more available tools. Pradalier has then investigated the possibility of encoding the nano κ-calculus into the stochastic π-calculus, and has found a translation that satisfies strong correctness properties. Furthermore, Pradalier has considered the chemical master equation, which describes probabilistically the possible behaviours of the system over time in terms of a differential equation on the probability to be in a given state at a given instant. Pradalier has introduced a notion of equivalence based on the chemical master equation and has proved that it corresponds exactly to the notion backward stochastic bisimulation. This results establishes a bridge between a chemical semantics and a computer semantics, and it also constitutes a first step towards a metrics for biochemistry. Finally Pradalier has investigated the relative expressive power of the synchronous and asynchronous stochastic π-calculus, for which he has used the encodability of the nanoκ-calculus.

7. Other Grants and Activities

7.1. Actions nationales

7.1.1. ANR project PANDA: "Analyse du Paralllisme 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

7.1.3. LIX project on Distributed, Mobile and Secure Complex Systems

This project is financed by the DGA, for the years 2007-2009. The teams involved are:

- Hipercom. Responsible: Philippe Jacquet
- Comète. Responsible: C. Palamidessi
- Algorithmes et Optimisation. Responsible: Philippe Baptiste
- MAX. Responsible: Michel Fliess.

7.2. Actions internationales

7.2.1. DRI Equipe Associée PRINTEMPS

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

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

PRINTEMPS focuses on the applications of Information Theory to security. We are particularly interested in studying the interactions between Concurrency and Information Theory.

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

7.2.2. DRI Equipe Associée REACT

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.

REACT stands for “Robust theories for Emerging Applications in Concurrency Theory”, which reflects the goals of the project.

Home page: http://cic.puj.edu.co/wiki/doku.php?id=grupos:avispa:react.

8. Dissemination

8.1. Contribution to scientific events and activities

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.
- Catuscia Palamidessi is member of the Editorial Board of the journal on Theory and Practice of Logic Programming, published by the Cambridge University Press.
- Catuscia Palamidessi is member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, Elsevier Science.
- Frank D. Valencia is area editor (for the area of Concurrency) of the ALP Newsletter.

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

8.1.3. Invited Talks

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

- Workshop on "Ubiquitous Computing at a Crossroads". London, UK. January 2009. http://www.nottingham.ac.uk/bridging/ubicomp/workshop.html
- BASICS 2009 International Workshop on Computation and Interaction. Shanghai, China. October 2009. http://basics.sjtu.edu.cn/summer_school/basics09/.
- IFIP 1.8 Workshop on Formal Methods for Embedded Systems. Eindhoven, NL. November 2009. http://www.cse.unsw.edu.au/~rvg/FMES/

8.1.4. Organization of workshops and conferences

- Catuscia Palamidessi has served as PC chairs of the 2009 edition of the conference on Mathematical Foundations of Programming Semantics (MFCS XXV), http://www.math.tulane.edu/~mfps/mfps25.htm.
- Catuscia Palamidessi and Frank Valencia have served as PC chairs of the 2009 edition of the International conference on Current Trends in Theory and Practice of Computer Science (SOFSEM), http://www.ksi.mff.cuni.cz/sofsem09/index.php.

8.1.5. Participation in program committees

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

- CONCUR 2010. The 21st International Conference on Concurrency Theory. Paris, France, September 2010. http://concur2010.inria.fr/
- 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 2009. The 20th International Conference on Concurrency Theory. Bologna, Italy, September 2009. http://concur09.cs.unibo.it/
- PPDP 2009. The 11th International ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming. Coimbra, Portugal. September 2009. http://www.dcc.fc.up.pt/ppdp09/
- FOSSACS 2009. The 12th International Conference on Foundations of Software Science and Computation Structures. (Part of ETAPS 2009.) York, UK. March 2009. http://fossacs09.soe.ucsc.edu/

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
- PLID 2009. The 5th International Workshop on Programming Language Interference and Dependence. London, UK. March 2009 http://www.dcs.qmul.ac.uk/~pm/plid/
- SecCo 09. The 7th International Workshop on Security Issues in Concurrency. Bologna, Italy, September 2009.

Frank D. Valencia has been/is a member of the program committees of the following conferences and workshops:

- ICLP 2009. 25th International Conference on Logic Programming. Pasadena, USA, July 2009.

Carlos A. Olarte has been/is a member of the program committees of the following conferences:

- SAC 2009. 24th Annual ACM Symposium on Applied Computing. Track on Constraint Satisfaction and Programming. Honolulu, USA, March 2009.

8.1.6. Organization of seminars

- Frank D. Valencia and Carlos Olarte 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. Service

Catuscia Palamidessi has served as:

- Member of the Commission Scientifique du Centre de Recherche INRIA Saclay, since February 2008.
- 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 INRIA GTRI (Group de Travail Relations Internationales) from November 2007 till October 2009.
- Member of the Comité de These for Mathematics and Computer Science at the École Polytechnique. Since October 2007.

8.3. Teaching

8.3.1. Postgraduate

- Frank Valencia is teaching (together with Francesco Zappa Nardelli and Roberto Amadio) the course "Concurrence" at the "Master Parisien de Recherche en Informatique" (MPRI) in Paris. Winter semesters 2008-09 and 2009-10.

Catuscia Palamidessi has given the following lectures or intensive courses to PhD and master students:

- Lecture on an Information-Theoretic approach to Confidentiality. PhD program at the University of Pisa, Italy. October 2009.
- Lecture on Anonymity Protocols as Noisy Channels. Master students of ENS Lyon, France. October 2009.
- Lectures on Information-Hiding. Mini-course of 4 hours for the PhD program at the University of Venice, Italy. April 2009.

8.3.2. Undergraduate

- Frank D. Valencia has been a lecturer on "Concurrency Theory" at Universidad Javeriana de Cali. Fall 2009.

8.4. Advising

8.4.1. PhD students

Catuscia Palamidessi has supervised the following PhD students:

- Romain Beauxis. Allocataire Region Ile de France. 1/10/2005 – 31/5/2009.
- Christelle Braun. Allocataire École Polytechnique - Ministère. Since 1/10/2007.
- Mario Sergio Ferreira Alvim Junior. Allocataire CNRS/DGA. Since 1/10/200.
- Ivan Gazeau. Allocataire ANR. Co-supervised by Dale Miller, Ecole Polytechnique, Paris. Since 1/10/2009
- Sylvain Pradalier. Allocataire ENS Cachan. Co-supervised by Cosimo Laneve, University of Bologna, Italy. 1/9/2006 – 30/9/2009.
- 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

- Jesus Aranda. Co-supervised by Juan Francisco Diaz, Universidad del Valle, Colombia. 1/10/2006 – 31/11/2009
- Andrés Aristizábal. Allocataire DGA/CNRS. Since 1/10/2009
- Carlos Olarte. Allocataire INRIA/CORDIS. 1/10/2006 – 30/10/2009

8.4.2. Internships

The team Comète has supervised the following internship students during 2008:

- Michael Matinez. Master student at the University of Cali, Colombia. 1/5/2009 – 31/7/2009
- Yamil Salim Percy. Master student at the University of Cali, Colombia. 5/11/2009 – 5/12/2009

8.4.3. PhD defenses

Catuscia Palamidessi has been “rapporteur” for the thesis, and member of the jury at the thesis defense, of the following PhD students:

- Luca Fossati (University of Turin, Italy). PhD Thesis on *Modeling the Handshaking Protocol for Asynchrony*. Defended on 9 February 2009. Advised by Simona Ronchi Della Rocca and Pierre-Louis Curien.
- Cinzia Di Giusto (University of Bologna, Italy). PhD thesis on *Expressiveness of Concurrent Languages*. Defended on 20 April 2009. Advised by Maurizio Gabbrielli.

Catuscia Palamidessi has also been president of the committee at the “defense day” of all thesis in Computer Science for the year 2009 at the University of Bologna. 20 April 2009.

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", vol. 386, n^{o} 3, 2007, p. 218-235, http://hal.inria.fr/inria-00200916/en/.

[2] K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Probable Innocence Revisited*, in "Theoretical Computer Science", vol. 367, n^o 1-2, 2006, p. 123–138, http://hal.inria.fr/inria-00201072/en/.

[3] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, P. PANANGADEN. *Anonymity Protocols as Noisy Channels*, in "Information and Computation", vol. 206, n^o 2–4, 2008, p. 378–401, 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", vol. 16, n^o 5, 2008, p. 531–571, http://hal.inria.fr/inria-00349224/en/.

[5] Y. DENG, C. PALAMIDESSI. *Axiomatizations for probabilistic finite-state behaviors*, in "Theoretical Computer Science", vol. 373, n^o 1-2, 2007, 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, vol. 2987, Springer, 2004, 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", vol. 335, n^o 2-3, 2005, 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", vol. 13, n^o 5, 2003, 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", vol. 330, n^o 3, 2005, p. 577–607, http://www.brics.dk/~fvalenci/papers/tcs.pdf.

Year Publications

Doctoral Dissertations and Habilitation Theses

[11] J. ARANDA. *On the Expressivity of Infinite and Local Behaviour in Fragments of the pi-calculus*, LIX, Ecole Polytechnique, France, and EISC, Universidad del Valle, Colombia, 2009, http://tel.archives-ouvertes.fr/tel-00430495/en/, Ph. D. Thesis.

[12] R. BEAUXIS. *Asynchronous Process Calculi for Specification and Verification of Information Hiding Protocols*, LIX, Ecole Polytechnique, France, 2009, Ph. D. Thesis.

[13] C. OLARTE. *Universal Temporal Concurrent Constraint Programming*, LIX, Ecole Polytechnique, Palaiseau, France, 2009, http://tel.archives-ouvertes.fr/tel-00430446/en/, Ph. D. Thesis.

[14] S. PRADALIER. *An approach to the modeling, simulation and analysis of nano-devices*, LIX, Ecole Polytechnique, France, 2009, Ph. D. Thesis.

Articles in International Peer-Reviewed Journal

[15] R. BEAUXIS, C. PALAMIDESSI. *Probabilistic and nondeterministic aspects of anonymity*, in "Theoretical Computer Science", vol. 410, n^{o} 41, 2009, p. 4006–4025, http://hal.archives-ouvertes.fr/inria-00424855/en/.

[16] D. CACCIAGRANO, F. CORRADINI, C. PALAMIDESSI. *Explicit Fairness in Testing Semantics*, in "Logical Methods in Computer Science", vol. 5, n^{o} 2 - 15, 2009, http://hal.archives-ouvertes.fr/hal-00444580/en/IT.

[17] K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Making Random Choices Invisible to the Scheduler*, in "Information and Computation", 2010, http://hal.archives-ouvertes.fr/inria-00424860/en/NL.

[18] S. KRAMER, J. C. BRADFIELD. *A General Definition of Malware*, in "Journal in Computer Virology", 2009, http://dx.doi.org/10.1007/s11416-009-0137-1, To appear.

[19] S. KRAMER, C. PALAMIDESSI, R. SEGALA, A. TURRINI, C. BRAUN. *A Quantitative Doxastic Logic for Probabilistic Processes and Applications to Information-Hiding*, in "The Journal of Applied Non-Classical Logics", 2010, http://hal.archives-ouvertes.fr/inria-00445212/en/IT.

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

International Peer-Reviewed Conference/Proceedings

[21] M. E. ANDRÉS, C. PALAMIDESSI, P. VAN ROSSUM, G. SMITH. *Computing the Leakage of Information-Hiding Systems*, in "Proceedings of the Sixteenth International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)", 2010, http://hal.archives-ouvertes.fr/hal-00445445/en/NLUS.

[22] J. ARANDA, G. ASSAYAG, C. OLARTE, J. A. PÉREZ, C. RUEDA, M. TORO, F. D. VALENCIA. *An Overview of FORCES: An INRIA Project on Declarative Formalisms for Emergent Systems*, in "Proceeding of the 25th International Conference, ICLP'09", P. M. HILL, D. S. WARREN (editors), Lectures Notes in Computer Science, vol. 5649, Springer, 2009, p. 509-513, http://hal.inria.fr/inria-00426610/en/ITCO.

[23] J. ARANDA, F. D. VALENCIA, C. VERSARI. *On the Expressive Power of Restriction and Priorities in CCS with replication*, in "Proceedings of the 12th International Conference on Foundations of Software Science and Computational Structures, FOSSACS'09", L. DE ALFARO (editor), Lectures Notes in Computer Science, vol. 5504, Springer, 2009, p. 242-256, http://hal.inria.fr/inria-00430531/en/IT.

[24] A. BHOWMICK, C. PALAMIDESSI. *Bounds on the leakage of the input's distribution in information-hiding protocols*, in "Proceedings of the Fourth Symposium on Trustworthy Global Computing (TGC 2008)", C. KAKLAMANIS, F. NIELSON (editors), Lecture Notes in Computer Science, vol. 5474, Springer, 2009, p. 36–51, http://hal.archives-ouvertes.fr/hal-00444579/en/IN.

[25] C. BRAUN, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Quantitative Notions of Leakage for One-try Attacks*, in "Proceedings of the 25th Conf. on Mathematical Foundations of Programming Semantics", Electronic Notes in Theoretical Computer Science, vol. 249, Elsevier B.V., 2009, p. 75-91, http://hal.archives-ouvertes.fr/inria-00424852/en/NL.

[26] M. FALASCHI, C. OLARTE, C. PALAMIDESSI. *A framework for abstract interpretation of timed concurrent constraint programs*, in "Proceedings of the 11th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming, PPDP'09", A. PORTO, F. J. LÓPEZ-FRAGUAS (editors), ACM, 2009, p. 207-218, http://hal.inria.fr/inria-00426608/en/IT.

[27] S. HAMADOU, C. PALAMIDESSI, V. SASSONE, E. ELSALAMOUNY. *Probable innocence in the presence of independent knowledge*, in "Proceedings of the 6th International Workshop on Formal Aspects in Security and Trust", P. DEGANO, J. GUTTMAN (editors), Lectures Notes in Computer Science, Springer, 2010, http://hal.archives-ouvertes.fr/inria-00424853/en/GB.

[28] H. LÓPEZ, C. OLARTE, J. A. PÉREZ. *Towards a Unified Framework for Declarative Structured Communications*, in "Proceedings of the workshop on Programming Language Approaches to Concurrency and Communication-cEntric Software (PLACES)", Electronic Notes in Theoretical Computer Science, Elsevier, 2009, http://hal.inria.fr/inria-00426609/en/, To appearDKIT.

[29] C. OLARTE, C. RUEDA. *A Declarative Language for Dynamic Multimedia Interaction Systems*, in "Proceedings of the Second International Conference on Mathematics and Computation in Music (MCM)", E. CHEW, A. CHILDS, H.-H. CHUAN (editors), Communications in Computer and Information Science, vol. 38, Springer, 2009, p. 218-227, http://hal.inria.fr/inria-00426607/CO.

National Peer-Reviewed Conference/Proceedings

[30] C. OLARTE, C. RUEDA, F. D. VALENCIA. *Concurrent Constraint Programming: a Declarative Paradigm for Modeling Music Systems*, in "New Computational Paradigms for Computer Music, Paris, France", G. ASSAYAG, A. GERZSO (editors), Delatour France / Ircam-Centre Pompidou, 2009, p. 400–402, http://hal.inria.fr/inria-00429592/en/CO.

[31] A. VILLOTA, J. ARANDA, D. JUAN FRANCISCO. *Modelando Sistemas de Membranas en ntcc*, in "Proceedings of the XXXV Latin American Informatics Conference, CLEI'09", 2009, http://hal.inria.fr/inria-00430537/en/CO.

Books or Proceedings Editing

[32] S. ABRAMSKY, M. W. MISLOVE, C. PALAMIDESSI (editors). *Proceedings of the 25th Conference on Mathematical Foundations of Programming Semantics*, vol. 249, Elsevier B.V., 2009, p. 1-490, http://dx.doi.org/10.1016/j.entcs.2009.07.080.

[33] M. CARBONE, P. SOBOCINSKI, F. D. VALENCIA (editors). *Foreword: Festschrift for Mogens Nielsen's 60th birthday*, vol. 410, n^{o} 41, Elsevier B.V., 2009, http://dx.doi.org/10.1016/j.tcs.2009.06.007.

[34] M. FALASCHI, M. GABBRIELLI, C. PALAMIDESSI (editors). *Abstract Interpretation and Logic Programming: Festschrift in honor of professor Giorgio Levi*, vol. 410, n^{o} 46, Elsevier B.V., 2009, http://dx.doi.org/10.1016/j.tcs.2009.07.034.

[35] M. NIELSEN, A. KUCERA, P. B. MILTERSEN, C. PALAMIDESSI, P. TUMA, F. D. VALENCIA (editors). *SOFSEM 2009: Proceedings of the 35th Conference on Current Trends in Theory and Practice of Computer Science*, Lecture Notes in Computer Science, vol. 5404, Springer, Spindleruv Mlýn, Czech Republic, 2009, p. 1-670, http://www.springer.com/computer/foundations/book/978-3-540-95890-1.

Scientific Popularization

[36] G. LONGO, C. PALAMIDESSI, T. PAUL. *Randomnes: five questions and some challenges*, in "Randomnes: 5 questions", H. ZENIL (editor), Automatic Press / VIP, 2010, http://hal.archives-ouvertes.fr/hal-00445553/en/.

References in notes

[37] R. BEAUXIS, C. PALAMIDESSI, F. D. VALENCIA. *On the Asynchronous Nature of the Asynchronous pi-Calculus*, in "Concurrency, Graphs and Models", P. DEGANO, R. DE NICOLA, J. MESEGUER (editors), Lecture Notes in Computer Science, vol. 5065, Springer, 2008, p. 473-492, http://hal.inria.fr/inria-00349226/en/.

[38] E. BRINKSMA, A. RENSINK, W. VOGLER. *Fair Testing*, in "Proceedings of the 6th International Conference on Concurrency Theory (CONCUR)", I. LEE, S. A. SMOLKA (editors), Lecture Notes in Computer Science, vol. 962, Springer-Verlag, 1995, p. 313–327.

[39] N. BUSI, M. GABBRIELLI, G. ZAVATTARO. *Replication vs. recursive definition in Channel Based Calculi*, in "Proc. of ICALP 03", LNCS, Springer-Verlag, 2003.

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

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

[42] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, P. PANANGADEN. *Anonymity Protocols as Noisy Channels*, in "Information and Computation", vol. 206, n^{o} 2–4, 2008, p. 378–401, http://hal.inria.fr/inria-00349225/en/ CA.

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

[44] G. COSTA, C. STIRLING. *A Fair Calculus of Communicating Systems*, in "Acta Informatica", vol. 21, 1984, p. 417–441.

[45] G. COSTA, C. STIRLING. *Weak and Strong Fairness in CCS*, in "Information and Computation", vol. 73, n^{o} 3, June 1987, p. 207–244.

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

[47] K. HONDA, V. T. VASCONCELOS, M. KUBO. *Language Primitives and Type Discipline for Structured Communication-Based Programming*, in "Proceedings of the 7th European Symposium on Programming (ESOP)", C. HANKIN (editor), Lecture Notes in Computer Science, vol. 1381, Springer, 1998, p. 122-138.

[48] V. NATARAJAN, R. CLEAVELAND. *Divergence and Fair Testing*, in "Proceedings of the 22nd International Colloquium on Automata, Languages and Programming (ICALP)", Z. FÜLÖP, F. GÉCSEG (editors), Lecture Notes in Computer Science, vol. 944, Springer, 1995, p. 648–659.

[49] V. A. SARASWAT, M. RINARD, P. PANANGADEN. *Semantic foundations of concurrent constraint programming*, in "Conference Record of the Eighteenth Annual ACM Symposium on Principles of Programming Languages", ACM Press, 1991, p. 333–352.

[50] V. A. SARASWAT. *Concurrent Programming Languages*, Carnegie-Mellon University, 1989, In ACM distinguished dissertation series. The MIT Press, 1993, Ph. D. Thesis.

[51] G. SMITH. *On the Foundations of Quantitative Information Flow*, in "Proc. of the 12th Int. Conf. on Foundations of Software Science and Computation Structures, York, UK", L. DE ALFARO (editor), LNCS, vol. 5504, Springer, 2009, p. 288–302.

[52] P. YANG, C. R. RAMAKRISHNAN, S. A. SMOLKA. *A logical encoding of the pi-calculus: model checking mobile processes using tabled resolution*, in "International Journal on Software Tools for Technology Transfer", vol. 6, n^{o} 1, 2004, p. 38–66.