INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Comète

Concurrence, Mobilité et Transactions

Saclay - Île-de-France

THEME COM

Activity Report

2008

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 [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]
Romain Beauxis [Allocataire Region Ile de France]
Christelle Braun [Allocataire École Polytechnique - Ministère]
Mario Sergio Ferreira Alvim Junior [Allocataire DGA/CNRS]
Carlos Olarte [Allocataire INRIA/CORDIS]
Sylvain Pradalier [Allocataire ENS Cachan. Co-supervised by Cosimo Laneve, University of Bologna, Italy]

Post-Doctoral Fellow

Simon Kramer [Post Doctorant INRIA. Till 30/10/2008]

Visiting Scientist

Srecko Brlek [Professor, École Polytechnique of Montreal, Canada. Two months visit]
Diletta Romana Cacciagrano [Assistant Professor, University of Camerino, Italy. One month visit]
Moreno Falaschi [Professor, University of Siena, Italy. Two months visit]
Vladimiro Sassone [Professor, University of Soouthampton. Three months visit]
Angelo Troina [Assistant Professor, University of Turin, Italy. Two months visit]
Andrea Turrini [PhD student, University of Verona, Italy. Three months visit]

Administrative Assistant

Lydie Fontaine [Secretary (SAR) INRIA]

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* [45]). *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

- Konstantinos Chatzikokolakis, ex PhD student of Comète who defended his thesis the 26th of October 2007, has won one of the two second prices Specif / Gilles Kahn for the best PhD thesis in France in Computer Science for the year 2008 (http://www.specif.org/prix-these/historique.html).
- Catuscia Palamidessi and Frank Valencia have been invited to serve 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 been invited to serve 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).

3. Scientific Foundations

3.1. Probabilistic aspects

Keywords: *Probability*.

Participants: Romain Beauxis, Christelle Braun, Mario Sergio Ferreira Alvim Junior, Simon Kramer, Catuscia Palamidessi, Sylvain Pradalier, Vladimiro Sassone, Angelo Troina, Andrea Turrini.

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

Keywords: *Expressiveness*.

Participants: Jesus Aranda, Romain Beauxis, Diletta Romana Cacciagrano, Catuscia Palamidessi, Carlos Olarte, 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

Keywords: *Process calculi*.

Participants: Jesus Aranda, Romain Beauxis, Catuscia Palamidessi, Angelo Troina, 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

Keywords: *anonymity*, *privacy*, *security*, *unobservability*.

Participants: Romain Beauxis, Christelle Braun, Mario Sergio Ferreira Alvim Junior, Simon Kramer, Catuscia Palamidessi, Vladimiro Sassone, Angelo Troina.

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

Keywords: *automatic verification*.

Participants: 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, 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 [13] 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 [14] 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, Diletta Romana Cacciagrano, Catuscia Palamidessi, Frank Valencia.

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

Busi et al. [39] showed that $\mathrm{CCS}_!$ (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 [38] they had shown that there is no encoding of RAMs into $\mathrm{CCS}_!$ which preserves and reflects divergence.

In [20] we studied the expressive power of restriction and its interplay with replication. We did this by considering several syntactic variants of $\mathrm{CCS}_!$ 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: $\mathrm{CCS}_!^{-!\nu}$ is the fragment of $\mathrm{CCS}_!$ not allowing restrictions under the scope of a replication. $\mathrm{CCS}_!^{-\nu}$ is the restriction-free fragment of $\mathrm{CCS}_!$. The third variant is $\mathrm{CCS}_{!+pr}^{-!\nu}$ which extends $\mathrm{CCS}_!^{-!\nu}$ with PhillipÕs priority guards. We have shown that the use of unboundedly many restrictions in $\mathrm{CCS}_!$ 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 $\mathrm{CCS}_!^{-!\nu}$ which preserves and reflects convergence. We have also proved that up to failures equivalence, there is no encoding from $\mathrm{CCS}_!$ into $\mathrm{CCS}_!^{-!\nu}$ nor from $\mathrm{CCS}_!^{-!\nu}$ into $\mathrm{CCS}_!^{-\nu}$. As lemmata for the above results we have proved that convergence is decidable for $\mathrm{CCS}_!^{-!\nu}$ and that language equivalence is decidable for $\mathrm{CCS}_!^{-\nu}$. 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 $\mathrm{CCS}_{!+pr}^{-!\nu}$: 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. Fairness

In [11] we have defined fair computations in the π-calculus. We have followed Costa and Stirling's approach for CCS-like languages [41], [42] but exploited a more natural labeling method of process actions to filter out unfair process executions. The new labeling allowed us to prove all the significant properties of the original one, such as unicity, persistence and disappearance of labels. It also turned out that the labeled π-calculus is a conservative extension of the standard one. We contrasted the existing fair testing notions [37], [46] 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.

6.1.3. Linearity vs. persistence

In [25] we have compared the expressive power of linear and persistent communication in the context of weak bisimilarity. We have considered four fragments of the π-calculus, corresponding to combinations of linearity/persistence also present in other frameworks such as Concurrent Constraint Programming and several calculi for security. The study is presented by providing (or proving the non-existence of) encodings among the fragments, a processes-as-formulae interpretation and a reduction from Minsky machines.

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

In [18] 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, Vladimiro Sassone.

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. 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 [40]. This is known as the problem of the *information-leaking scheduler*. In [12] 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.

6.2.2. Information theory

In [13], [22] we have proposed a framework in which anonymity protocols are interpreted as particular kinds of channels, and the degree of anonymity provided by the protocol as the converse of the channel's capacity. We have then illustrated how various notions of anonymity can be expressed in this framework, and showed the relation with some definitions of probabilistic anonymity in literature. Finally, we have discussed how to compute the channel matrix on the basis of the transition system associated to the protocol, and how to perform the computation automatically using a model-checker like PRISM.

In [26] we have established a monotonicity principle for convex functions that enables high-level reasoning about capacity in information theory. Despite its simplicity, this single idea is remarkably applicable. It has led to a significant extension of algebraic information theory, a solution of the capacity reduction problem, intuitive graphical methods for comparing channels, new inequalities that provide useful estimates on the information transmitting capability of a channel operating in an unknown environment, further explication of the fascinating relationship between capacity and Euclidean distance, and the solution of an open problem in quantum steganography.

6.2.3. Bayes risk

The degree of protection provided by a protocol can be expressed in terms of the probability of error associated to the inference of the secret information. In [14] we have investigated how the adversary can test the system to try to infer the user's identity, and we have studied how the probability of error depends on the characteristics of the channel. In particular we have considered the Bayes approach, and we have been able to characterize the associated probability of error (Bayes risk) in terms of the solution of certain systems of equations derived from the channel. This has allowed us to compute tight bounds for the Bayes risk, thus improving long-standing results in literature.

6.2.4. Compositional analysis of information hiding

In [24] we have considered a probabilistic process calculus approach to the specification of protocols for information hiding, and we have studied how the operators affect the probability of error. In particular, we have characterized constructs that have the property of not decreasing the degree of protection, and that can therefore be considered safe in the modular construction of protocols. As a case study, we have applied these techniques to the Dining Cryptographers, and we are able to derive a generalization of Chaum's strong anonymity result.

6.2.5. Bounds on the leakage of the inputÕs 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 [23] 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: Srecko Brlek, Simon Kramer, Catuscia Palamidessi, Angelo Troina.

6.3.1. The probabilistic applied π-calculus

In order to obtain a language suitable for the specification and verification of a large class of security protocols, we aim at enriching the probabilistic π-calculus with value passing, encryption and decryption, other primitive functions, and data types, along the lines of the *applied π-calculus* [36].

Some preliminary work in this direction is represented by [35]. We have investigated an extension of the Applied π-calculus obtained by introducing nondeterministic and probabilistic choice operators. The semantics of the resulting model, in which probability and nondeterminism are combined, is given by Segala's Probabilistic Automata driven by schedulers which resolve the nondeterministic choice among the probability distributions over target states. We have provided notions of static and observational equivalence for the enriched calculus. In order to model the possible interaction of a process with its surrounding environment, we have given a labeled semantics together with a notion of weak bisimulation which is shown to coincide with the observational equivalence. Finally, we have proved that results in the probabilistic framework are preserved in a purely nondeterministic setting.

6.3.2. Cryptographic protocol logic: Satisfaction for (timed) DolevÐYao cryptography

In [16] we have xplored logical concepts in cryptography and their linguistic abstraction and model-theoretic combination in a comprehensive logical system, called CPL (for Cryptographic Protocol Logic). We have focused on two fundamental aspects of cryptography. Namely, the security of communication (as opposed to security of storage) and cryptographic protocols (as opposed to cryptographic operators). The logical concepts explored are the following. Primary concepts The modal concepts of knowledge, norms, provability, space, and time. Secondary concepts Individual and propositional knowledge, confidentiality norms, truth-functional and relevant (in particular, intuitionistic) implication, multiple and complex truth values, and program types. The distinguishing feature of CPL is that it unifies and refines a variety of existing approaches. This feature is the result of our wholistic conception of property-based (modal logics) and model-based (process algebra) formalisms. We have illustrated the expressiveness of CPL on representative requirements engineering case studies. Further, we have extended (core) CPL (qualitative time) with rational-valued time, i.e. time stamps, timed keys, and potentially drifting local clocks, to tCPL (quantitative time). Our extension is conservative and provides further evidence for LamportÕs claim that adding real time to an untimed formalism is really simple.

6.3.3. A General definition of malware

In [31] 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.

6.3.4. Reducing provability to knowledge in multi-agent systems

In [27] we have shown that provability can be reduced to a combination of four kinds of knowledge in multi-agent systems. These kinds are: *individual* knowledge (knowledge of messages), plain *propositional* knowledge (knowledge that a state of affairs is the case), *common* knowledge (propositional knowledge shared in a community of agents), and a new kind of knowledge, namely *adductive* knowledge (propositional knowledge contingent on the adduction of certain individual knowledge, e.g., through *oracle invocation*) employing *relevant implication*.

6.3.5. Dolev-Yao encryption is Urquhart-Routley implication

In [34] we have proposed a logico-algebraic analysis of static (only local computation) Dolev-Yao cryptography. Our main result is that static Dolev-Yao cryptography can be modelled as a contextual (with respect to a protocol agent and an execution state) complete modular algebra, called Dolev-Yao algebra, in which encryption is Urquhart-Routley implication.

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`, [48]) 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 [47], 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.

In [21] we have proposed an extension of concurrent constraint programming with probabilistic executions. We were interested in extending the original operational and denotational semantics so as to bridge the gap between the original closure operator semantics and the vector space approach as defined in [43]. The main challenge was to give a mathematical framework for defining a maximal probabilistic execution. Indeed, for a (possibly infinite) sequence of probabilistic execution states which are probability measures on the atomic states of the process, it is not guaranteed that a limit state can be defined, or that this limit will enjoy the same properties as the finite probabilistic states do. We have addressed this issue by using a topological notion of probability measures, namely the (simple) valuations, and by defining a mathematical space for which we prove that this limit exists and enjoys the expected properties. Using this result, a denotational semantics has been defined for this language that is the lifted denotational semantics of the original concurrent constraint programming, dealing with vector spaces and linear closure operators instead of set of constraints and closure operators.

6.4.2. Universal timed concurrent constraint programming

In [30] we have introduced the *universal timed concurrent constraint programming* (`utcc`) process calculus; a generalisation of timed concurrent constraint programming (`tcc`). The `utcc` calculus allows for the specification of mobile behaviours in the sense of Milner's π-calculus: Generation and communication of private channels or links. We first endowed `utcc` with an *operational* semantics and then with a *symbolic* semantics to deal with problematic operational aspects involving infinitely many substitutions and divergent internal computations. The novelty of the symbolic semantics is to use *temporal constraints* to represent finitely infinitely-many substitutions. We have also showed that `utcc` has a strong connection with Pnueli's temporal logic, and we have exploited this connection to prove reachability properties of `utcc` processes. As a compelling example, we have used `utcc` to exhibit the secrecy flaw of the Needham-Schroeder security protocol.

6.4.3. The expressiveness of universal timed ccp: Undecidability of Monadic FLTL and Closure Operators for Security

In [29] we have studied 1) the expressiveness of utccand 2) its semantic foundations. As applications of this study, we also 3) have stated a noteworthy decidability result for the well-established framework of FLTL and 4) have brought new semantic insights into the modeling of security protocols.

More precisely, we have showed that in contrast to tcc, utccis Turing-powerful by encoding Minsky machines. The encoding proposed makes use of a monadic constraint system allowing us to prove a new result for a fragment of FLTL: The undecidability of the validity problem for monadic FLTL without equality and function symbols. This result justifies the restriction imposed in previous decidability results on the quantification of flexible-variables. We have also shown that, as in tcc, utccprocesses can be semantically represented as partial closure operators. The representation has been proved to be fully abstract wrt the input-output behavior of processes for a meaningful fragment of the utcc. This has shown that mobility can be captured as closure operators over an underlying constraint system. As an application of the semantic study of utcc, we have identified a language for security protocols that can be represented as closure operators over a cryptographic constraint system.

6.4.4. Abstract interpretation

In [33] we have introduced a general framework for data-flow (static) analyzes of utccprograms by abstract interpretation techniques. Being more expressive than its predecessor tcc, the operational semantics of utcc may induce infinitely many internal reductions. Thus we had to deal with the problems caused by the synchronization mechanisms in this language, as well as with the infinite internal computations. The framework is parametric w.r.t. the abstract domain, and we have given the conditions which have to be satisfied for ensuring the soundness of our methodology. In order to deal with infinite sequences of constraints, we have defined an approximation of the output of a program by a finite cut. Being compositional, our method has a complexity lower than the usual (non-compositional) data-flow analyzes. Furthermore, since utcc is more general than tcc, we obtain also a framework for data-flow analyzes of tcc as a special case. We have showed that our framework allows us to reuse the most popular abstract domains previously defined for logic programming. As an example, we have presented a groundness analysis on a utcc program. Finally, we have showed how to make use of the abstract semantics to detect flaws in security protocols. This semantics allows us to get round the state-explosion problem inherent in this kind of applications.

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.

In [17], 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 [50], 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.

6.6. Modeling biological systems

Participants: Jesus Aranda, Sylvain Pradalier, Frank Valencia.

6.6.1. Stochastic bigraphs

In [28] we have presented a stochastic semantics for Bigraphical Reactive Systems. A reduction and a labelled stochastic semantics for bigraphs have been defined. As a sanity check, we have proved that the two semantics are consistent with each other. We have also illustrated the expressiveness of the framework with an example of membrane budding in a biological system.

6.6.2. The `nano`κ *calculus*

In [15] we have developed a process calculus – the `nano`κ calculus – for modeling, analyzing and predicting the properties of molecular devices. The `nano`κ calculus is equipped with a simple stochastic model, that we use to model and simulate the behaviour of a molecular shuttle, a basic nano device currently used for building more complex systems.

6.6.3. Timed concurrent constraint programming for biological applications

In [19] we have proposed a stochastic version of timed concurrent constraint programming, and we have discussed its potentialities for biological applications. We have defined stochastic events in terms of the time units provided by the calculus: this has given us great flexibility for modeling and allowed for a clean semantics. Most importantly, by considering stochastic information and adhering to explicit discrete time, it has been possible to reason about processes using quantitative logics (both discrete and continuous), while retaining the simplicity of calculi such as ntcc for deriving qualitative reasoning techniques such as denotational semantics and proof systems.

7. Other Grants and Activities

7.1. Actions nationales

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

This project is finanged by the DGA, for the years 2007 and 2008. The teams involved are:

- Hipercom. Responsible: Philippe Jacquet
- Comète. Responsible: C. Palamidessi
- Algorithmes et Optimisation. Responsible: Philippe Baptiste
- MAX. Responsible: Michel Fliess. 2007-2008.

7.2. Actions internationales

7.2.1. DREI Equipe Associée PRINTEMPS

The project has started in December 2005 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/.

Some publications representative of this collaboration are [13], [14].

7.2.2. REACT: Robust theories for Emerging Applications in Concurrency Theory

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

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

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

Some publications representative of this collaboration is [44] and [19].

7.2.3. PAI project MONACO: MOdels for New Applications of COncurrency

. The project has started in January 2007 and will end in December 2008. It involves the following sites:

- Imperial College, UK. Responsible I. Phillips
- INRIA Futurs. Responsible: C. Palamidessi
- Technische Universität Berlin, Germany. Responsible: U. Nestmann.

A publications representative of this collaboration is [49].

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 IFIP Technical Committee 1 – Foundations of Computer Science. Since 2007
- The Council of EATCS, the European Association for Theoretical Computer Science. Since 2005
- 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 in occasion of the opening of the MT-Lab in Copenhagen, 19-20 Oct 2008.
- Workshop on Informatic Phenomena. New Orleans, 13-17 Oct 2008. http://www.math.tulane.edu/~mwm/wip/Workshop%20on%20Informatic%20Phenomena.html.
- Workshop on Logic And Information Security. Leiden, 22-26 Sept 2008. http://www.lorentzcenter.nl/lc/web/2008/302/info.php3?wsid=302.
- SecCo 2008: 6th International Workshop on Security Issues in Concurrency. Toronto, 23 August 2008. http://www.lsv.ens-cachan.fr/SecCo08/.
- ICE'08: Synchronous and Asynchronous Interactions in Concurrent Distributed Systems. ICALP 2008 affiliated workshop - Reykjavik, 6 July 2008. http://ice08.dimi.uniud.it/doku.php.
- 1st Canada-France MITACS Workshop on Foundations & Practice of Security. Montreal, 31 May - June 2, 2008. http://www.mitacs.ca/conferences/FPS2008/.

8.1.4. Organization of workshops and conferences

- Catuscia Palamidessi and Frank Valencia have been invited to serve 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.
- Catuscia Palamidessi has been invited to serve 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.
-

8.1.5. Participation in program committees

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

- CONCUR 2009. 20th International Conference on Concurrency Theory. Bologna, Italy, September 2009.
- FOSSACS 2009. 12th International Conference on Foundations of Software Science and Computation Structures. (Part of ETAPS 2009.) York, UK, March 2009.
- QEST'08. International Conference on Quantitative Evaluation of SysTems. Saint Malo, France, September 2008.
- CONCUR 2008. 19th International Conference on Concurrency Theory. Toronto, Canada, August 2008.
- CiE 2008: Logic and Theory of Algorithms. Athens, Greece. June 2008.
- FICS 2008. Foundations of Informatics, Computing and Software. Shanghai, China, June 2008.
- LICS 2008. 23rd Symposium on Logic in Computer Science. Pittsburgh, USA. June 2008.
- MFPS XXIV. Twenty-fourth Conference on the Mathematical Foundations of Programming Semantics. University of Pennsylvania, Philadelphia, USA, May 2008.
- ESOP 2008. 17th European Symposium on Programming. (Part of ETAPS 2008.) Budapest, Hungary, March - April 2008.
- VMCAI 2008. 9th International Conference on Verification, Model Checking, and Abstract Interpretation. San Francisco, USA. January 2008.

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

- FMWS 2008. Formal Methods for Wireless Systems. CONCUR 2008 affiliated workshop. Toronto, Canada. August 2008.
- SOS 2008. Structural operational semantics. ICALP 2008 affiliated workshop - Reykjavik, Iceland. July 2008.
- TFIT 2008. The Fourth Taiwanese-French Conference on Information Technology. Taipei, Taiwan, March 2008.

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.
- ICLP 2008. 24th International Conference on Logic Programming. Udine, Italy, December 2008.
- EXPRESS'08. 15th International Workshop on Expressiveness in Concurrency. CONCUR 2008 affiliated workshop. Toronto, Canada. August 2008.

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.
- SAC 2008. 23rd Annual ACM Symposium on Applied Computing. Track on Constraint Satisfaction and Programming. Fortaleza, Brazil, March 2008.

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 Disciplinaire pour les Programmes Non Thématiques et Jeunes Chercheurs de l'ANR, 2008.
- 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").
- Member of the panel to evaluate project proposals for the 2008 programme "Information and Communication Technology - ICT", sponsored by the Vienna Science and Technology Fund WWTF.
- 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 courses:

- 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 semester 2008-09.

8.3.2. Undergraduate courses:

- Frank D. Valencia has been a lecturer on "Concurrency Theory" at Universidad Javeriana de Cali. July 2008.

8.4. Advising

8.4.1. PhD students

Catuscia Palamidessi has supervised the following PhD students:

- Romain Beauxis. Allocataire Region Ile de France.
- Christelle Braun. Allocataire École Polytechnique - Ministère.
- Mario Sergio Ferreira Alvim Junior. Allocataire CNRS/DGA.
- Sylvain Pradalier. Allocataire ENS Cachan. Co-supervised by Cosimo Laneve, University of Bologna, Italy.

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

- Carlos Olarte. Allocataire INRIA/CORDIS.
- Jesus Aranda. Co-supervised by Juan Francisco Diaz, Universidad del Valle, Colombia.

8.4.2. Internships

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

- Abhishek Bhowmick. Junior, Bachelor of Technology, Computer Science and Engineering, IIT Kanpur. May-July 2008.

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:

- Han Chen (Queen Mary, University of London, UK). PhD thesis on *Information-Theoretic Approaches to Non-Interference*. Defended on December 17, 2008. Advised by Pasquale Malacaria.
- Augusto Parma (Università di Verona, Italy). PhD thesis on *Axiomatic and Logical Characterizations of Probabilistic Preorders and Trace Semantics*. Defended on May 8, 2008. Advised by Roberto Segala.
- Sardaouna Hamadou (École Polytechnique of Montreal, Canada). PhD thesis on *Analyse formelle des protocoles cryptographiques et flux d'information admissible*. Defended of March 26, 2008. Advised by John Mullins and Srecko Brlek.

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

Articles in International Peer-Reviewed Journal

[11] D. CACCIAGRANO, F. CORRADINI, C. PALAMIDESSI. *Explicit Fairness in Testing Semantics*, in "Logical Methods in Computer Science", Conditionally accepted, 2009.

[12] K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Making Random Choices Invisible to the Scheduler*, in "Information and Computation", Invited submission, 2009.

[13] 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/.

[14] 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/.

[15] A. CREDI, M. GARAVELLI, C. LANEVE, S. PRADALIER, S. SILVI, G. ZAVATTARO. *nanoK: A calculus for the modeling and simulation of nano devices*, in "Theoretical Computer Science", vol. 408, n^{o} 1, 2008, p. 17-30.

[16] S. KRAMER. *Cryptographic protocol logic: Satisfaction for (timed) Dolev-Yao cryptography*, in "Journal of Logic and Algebraic Programming", vol. 77, n^{o} 1-2, 2008, p. 60 - 91.

[17] G. NORMAN, C. PALAMIDESSI, D. PARKER, P. WU. *Model checking probabilistic and stochastic extensions of the π-calculus*, in "IEEE Transactions of Software Engineering", To appear, 2009.

Invited Conferences

[18] 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/.

International Peer-Reviewed Conference/Proceedings

[19] J. ARANDA, J. A. PÉREZ, C. RUEDA, F. D. VALENCIA. *Stochastic Behavior and Explicit Discrete Time in Concurrent Constraint Programming*, in "24th International Conference on Logic Programming", M. G. DE LA BANDA, E. PONTELLI (editors), Lecture Notes in Computer Science, vol. 5366, Springer, 2008, p. 682-686.

[20] J. ARANDA, F. D. VALENCIA, C. VERSARI. *On the Expressive Power of Restriction in CCS with Replication*, in "Proceedings of the 12th Int. Conf. on Foundations of Software Science and Computation Structures (FOSSACS)", L. DE ALFARO (editor), Lecture Notes in Computer Science, To appear, Springer, 2009, http://www.lix.polytechnique.fr/Labo/Jesus.Aranda/publications/trccs.pdf.

[21] R. BEAUXIS. *Probabilistic and Concurrent Models for Security*, in "24th International Conference on Logic Programming", M. G. DE LA BANDA, E. PONTELLI (editors), Lecture Notes in Computer Science, vol. 5366, Springer, 2008, p. 801-802.

[22] R. BEAUXIS, K. CHATZIKOKOLAKIS, C. PALAMIDESSI, P. PANANGADEN. *Formal Approaches to Information-Hiding (Tutorial)*, in "Proceedings of the Third Symposium on Trustworthy Global Computing (TGC 2007)", G. BARTHE, C. FOURNET (editors), Lecture Notes in Computer Science, vol. 4912, Springer, 2008, p. 347-362, http://hal.inria.fr/inria-00261827/en/.

[23] 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)", To appear, 2009.

[24] C. BRAUN, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Compositional Methods for Information-Hiding*, in "Proceedings of FOSSACS", R. AMADIO (editor), Lecture Notes in Computer Science, vol. 4962, Springer, 2008, p. 443-457, http://hal.inria.fr/inria-00349227/en/.

[25] D. CACCIAGRANO, F. CORRADINI, J. ARANDA, F. D. VALENCIA. *Linearity, Persistence and Testing Semantics in the Asynchronous Pi-Calculus*, in "Proc. of 14th International Workshop on Expressiveness of Concurrency, (EXPRESS'07)", R. AMADIO, T. T. HILDENBRANDT (editors), ENTCS, vol. 194, Elsevier, 2008, p. 59-84, http://hal.inria.fr/inria-00201502/en/.

[26] K. CHATZIKOKOLAKIS, K. MARTIN. *A Monotonicity Principle for Information Theory.*, in "Proceedings of the Twenty-fourth Conference on the Mathematical Foundations of Programming Semantics", A. BAUER, M. MISLOVE (editors), Electronic Notes in Theoretical Computer Science, vol. 218, Elsevier B.V., 2008, p. 111-129.

[27] S. KRAMER. *Reducing Provability to Knowledge in Multi-Agent Systems*, in "Proceedings of the LiCS-affiliated Intuitionistic Modal Logics and Applications Workshop", Electronic Notes in Theoretical Computer Science, To appear. Extended version submitted to Information and Computation, Elsevier B.V., 2008.

[28] J. KRIVINE, R. MILNER, A. TROINA. *Stochastic Bigraphs*, in "Proceedings of the 24th Conference on the Mathematical Foundations of Programming Semantics (MFPS XXIV)", A. BAUER, M. MISLOVE (editors), Electronic Notes in Theoretical Computer Science, vol. 218, Elsevier B.V., 2008, p. 73-96.

[29] C. Olarte, F. D. Valencia. *The expressivity of universal timed CCP: undecidability of Monadic FLTL and closure operators for security*, in "Proceedings of the 10th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming", S. Antoy, E. Albert (editors), 2008, p. 8-19.

[30] C. Olarte, F. D. Valencia. *Universal Concurrent Constraint Programing: Symbolic Semantics and Applications to Security*, in "Proceedings of the 23rd ACM Symposium on Applied Computing (SAC)", ACM, 2008, p. 145-150, http://hal.inria.fr/inria-00201497/en/.

Workshops without Proceedings

[31] S. Kramer, J. C. Bradfield. *A General Definition of Malware*, in "Proceedings of the Workshop on the Theory of Computer Viruses", Extended version submitted to the Journal of Computer Virology, 2008.

Books or Proceedings Editing

[32] C. Palamidessi, F. D. Valencia (editors). *Proceedings of the LIX Colloquium on Emerging Trends in Concurrency Theory (LIX 2006)*, vol. 209, Elsevier B.V., 2008, p. 1-200.

Research Reports

[33] M. Falaschi, C. Olarte, C. Palamidessi. *A Framework for Abstract Interpretation of Universal Timed Concurrent Constraint Programs*, Technical report, LIX, Ecole Polytechnique, 2008, http://www.lix.polytechnique.fr/~colarte/report-abs-utcc.pdf.

[34] S. Kramer. *Dolev-Yao Encryption is Urquhart-Routley Implication*, Submitted to Information Processing Letters, Technical report, LIX, Ecole Polytechnique, 2008.

[35] A. Troina, J. Goubault-Larrecq, C. Palamidessi. *A Probabilistic Applied Pi-Calculus*, Technical report, LIX, Ecole Polytechnique, 2008.

References in notes

[36] M. Abadi, C. Fournet. *Mobile Values, New Names, and Secure Communication*, in "28th Annual Symposium on Principles of Programming Languages (POPL)", ACM, January 2001, p. 104–115.

[37] 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.

[38] N. Busi, M. Gabbrielli, G. Zavattaro. *Replication vs. recursive definition in Channel Based Calculi*, in "Proc. of ICALP 03", LNCS, Springer-Verlag, 2003.

[39] N. Busi, M. Gabbrielli, G. Zavattaro. *Comparing Recursion, Replication, and Iteration in Process Calculi*, in "Proc. of ICALP 04", LNCS, Springer-Verlag, 2004.

[40] R. Canetti, L. Cheung, N. Lynch, O. Pereira. *On the Role of Scheduling in Simulation-Based Security*, 2007, Cryptology ePrint Archive, Report 2007/102.

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

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

[43] A. DI PIERRO, H. WIKLICKY. *Probabilistic Concurrent Constraint Programming: Towards a Fully Abstract Model*, in "Proceedings of the 23rd International Symposium on Mathematical Foundations of Computer Science", L. BRIM, J. GRUSKA, J. ZLATUSKA (editors), Lecture Notes in Computer Science, vol. 1450, Springer, 1998, p. 446-455.

[44] J. GUTIERREZ, J. PEREZ, C. RUEDA, F. D. VALENCIA. *Timed Concurrent Constraint Programming for Analyzing Biological Systems.*, in "Proceedings of Workshop on Membrane Computing and Biologically Inspired Process Calculi.", Electronic Notes in Theoretical Computer Science, vol. 171 (2), Elsevier Science B.V., 2007, p. 117–137, http://www.brics.dk/~fvalenci/papers/bioccp.pdf.

[45] T. HOARE, R. MILNER. *Grand Challenges for Computing Research*, in "Computer Journal", vol. 48, n° 1, 2005, p. 49-52.

[46] 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.

[47] 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.

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

[49] M. G. VIGLIOTTI, I. PHILLIPS, C. PALAMIDESSI. *Tutorial on separation results in process calculi via leader election problems*, in "Theoretical Computer Science", vol. 388, n° 1-3, 2007, p. 267-289, http://hal.inria.fr/inria-00201071/en/.

[50] 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° 1, 2004, p. 38–66.