IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2015

Project-Team COMETE

Concurrency, Mobility and Transactions

IN COLLABORATION WITH: Laboratoire d'informatique de l'école polytechnique (LIX)

RESEARCH CENTER
Saclay - Île-de-France

THEME
Security and Confidentiality

Table of contents

Project-Team COMETE

Creation of the Project-Team: 2008 January 01

Keywords:

Computer Science and Digital Science:

2.1.1. - Semantics of programming languages
2.1.5. - Constraint programming
2.1.6. - Concurrent programming
2.1.8. - Synchronous languages
2.4.1. - Analysis
2.4.2. - Verification
4.5. - Formal methods for security
4.8. - Privacy-enhancing technologies

Other Research Topics and Application Domains:

6.1. - Software industry
6.6. - Embedded systems
9.4.1. - Computer science
9.8. - Privacy

1. Members

Research Scientists

Catuscia Palamidessi [Team leader, Inria, Senior Researcher]
Konstantinos Chatzikokolakis [CNRS, Researcher]
Frank Valencia [CNRS, Researcher]

PhD Students

Michell Guzman [Inria]
Joris Lamare [Inria]
Yamil Salim Perchy [Inria]
Marco Stronati [Ecole Polytechnique, grant Monge, until Sep 2015]

Post-Doctoral Fellows

Ehab Elsalamouny [Inria]
Luis Pino [Ecole Polytechnique, until Jan 2015]
Marco Stronati [Inria, Oct 2015 until Dec 2015]
Yusuke Kawamoto [Inria, until Mar 2015]

Visiting Scientists

Carlos Olarte [Junior Professor at the Universidade Federal do Rio Grande do Norte, Brazil, until Jul 2015]
Mario Ferreira Alvim Junior [Assistant Professor, Federal University of Minas Gerais, Dec 2015]
Annabelle Mciver [Associate Professor, Macquarie University, Dec 2015]
Charles Carroll Morgan [Professor, University of New South Wales, Dec 2015]
Geoffrey Smith [Professor, Florida International University, USA, Dec 2015]
Gabriel Senno [Universidad de Buenos Aires]

Administrative Assistants

Martine Thirion [Inria, until Feb 2015]
Hélèna Kutniak [Inria, since Sep 2015]

2. Overall Objectives

2.1. Overall Objectives

Our times are characterized by the massive presence of highly *distributed systems* consisting of diverse and specialized devices, forming heterogeneous networks, and providing different services and applications. Revolutionary phenomena such as *social networks* and *cloud computing* are examples of such systems.

In Comète we study emerging concepts of this new era of computing. *Security* and *privacy* are some of the fundamental concerns that arise in this setting. In particular, in the modern digital world the problem of keeping information secret or confidential 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 malicious agents the opportunity to gather and store huge amount of information, often without the individual even being aware of it. Mobility is an additional source of vulnerability, since tracing may reveal significant information. To avoid these kinds of hazards, *security protocols* and various techniques for privacy protection have been designed. However, the properties that they are supposed to ensure are rather subtle, and, furthermore, it is difficult to foresee all possible expedients that a potential attacker may use. As a consequence, even protocols that seem at first "obviously correct" are later (often years later) found to be prone to attacks.

In addition to the security problems, the problems of correctness, robustness and reliability are made more challenging by the complexity of these systems, since they are highly concurrent and distributed. Despite being based on impressive engineering technologies, they are still prone to faulty behavior due to errors in the software design.

To overcome these drawbacks, we need to develop formalisms, reasoning techniques, and verification methods, to specify systems and protocols, their intended properties, and to guarantee that these intended properties of correctness and security are indeed satisfied.

In Comète we study formal computational frameworks for specifying these systems, theories for defining the desired properties of correctness and security and for reasoning about them, and methods and techniques for proving that a given system satisfies the intended properties.

3. Research Program

3.1. Probability and information theory

Participants: Konstantinos Chatzikokolakis, Catuscia Palamidessi, Ehab Elsalamouny, Yusuke Kawamoto, Marco Stronati, Joris Lamare.

Much of the research of Comète focuses on security and privacy. In particular, we are interested in the problem of the leakage of secret information through public observables.

Ideally we would like systems to be completely secure, but in practice this goal is often impossible to achieve. Therefore, we need to reason about the amount of information leaked, and the utility that it can have for the adversary, i.e. the probability that the adversary is able to exploit such information.

The recent tendency is to use an information theoretic approach to model the problem and define the leakage in a quantitative way. The idea is to consider the system as an information-theoretic *channel*. The input represents the secret, the output represents the observable, and the correlation between the input and output (*mutual information*) represents the information leakage.

Information theory depends on the notion of entropy as a measure of uncertainty. From the security point of view, this measure corresponds to a particular model of attack and a particular way of estimating the security threat (vulnerability of the secret). Most of the proposals in the literature use Shannon entropy, which is the most established notion of entropy in information theory. We, however, consider also other notions, in particular Rényi min-entropy, which seems to be more appropriate for security in common scenarios like one-try attacks.

3.2. Expressiveness of Concurrent Formalisms

Participants: Catuscia Palamidessi, Luis Pino, Frank Valencia.

We study computational models and languages for distributed, 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, also taking into account the issue of (efficient) implementability.

3.3. Concurrent constraint programming

Participants: Michell Guzman, Yamil Salim Perchy, Luis Pino, Frank Valencia.

Concurrent constraint programming (ccp) is a well established process calculus for modeling systems where agents interact by posting and asking information in a store, much like in users interact in *social networks*. This information is represented as first-order logic formulae, called constraints, on the shared variables of the system (e.g., $X > 42$). The most distinctive and appealing feature of ccp is perhaps that it unifies in a single formalism the operational view of processes based upon process calculi with a declarative one based upon first-order logic. It also has an elegant denotational semantics that interprets processes as closure operators (over the set of constraints ordered by entailment). In other words, any ccp process can be seen as an idempotent, increasing, and monotonic function from stores to stores. Consequently, ccp processes can be viewed as: computing agents, formulae in the underlying logic, and closure operators. This allows ccp to benefit from the large body of techniques of process calculi, logic and domain theory.

Our research in ccp develops along the following two lines:

1. **(a)** The study of a bisimulation semantics for ccp. The advantage of bisimulation, over other kinds of semantics, is that it can be efficiently verified.
2. **(b)** The extension of ccp with constructs to capture emergent systems such as those in social networks and cloud computing.

3.4. Model checking

Participants: Konstantinos Chatzikokolakis, Catuscia Palamidessi.

Model checking addresses the problem of establishing whether a given specification satisfies a certain property. We are interested in developing model-checking techniques for verifying concurrent systems of the kind explained above. In particular, we focus on security and privacy, i.e., on the problem of proving that a given system satisfies the intended security or privacy properties. Since the properties we are interested in have a probabilistic nature, we use probabilistic automata to model the protocols. A challenging problem is represented by the fact that the interplay between nondeterminism and probability, which in security presents subtleties that cannot be handled with the traditional notion of a scheduler,

4. Application Domains

4.1. Security and privacy

Participants: Konstantinos Chatzikokolakis, Catuscia Palamidessi, Ehab Elsalamouny, Marco Stronati, Joris Lamare.

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 *information hiding*.

Information hiding is a generic term which we use here to refer to the problem of preventing the disclosure of information which is supposed to be secret or confidential. The most prominent research areas which are concerned with this problem are those of *secure information flow* and of *privacy*.

Secure information flow refers to the problem of avoiding the so-called *propagation* of secret data due to their processing. It was initially considered as related to software, and the research focussed on type systems and other kind of static analysis to prevent dangerous operations, Nowadays the setting is more general, and a large part of the research effort is directed towards the investigation of probabilistic scenarios and treaths.

Privacy denotes the issue of preventing certain information to become publicly known. 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 solution is then to obfuscate the link between secrets and observables as much as possible, and often the use randomization, i.e. the introduction of *noise*, can help to achieve this purpose. The system can then 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 quantitive information flow and of privacy, and to develop heuristics and methods to improve mechanisms for the protection of secret information. 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.

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- SIGSAC Doctoral Dissertation Award 2015 for the thesis "Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy" [29] by Nicolás Bordenabe (Defended on Sep 12, 2014)
- Prix de thèse de l'Ecole Polytechnique 2015 for the thesis "Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy" [29] by Nicolás Bordenabe (Defended on Sep 12, 2014)

6. New Software and Platforms

6.1. Location Guard

Participants: Konstantinos Chatzikokolakis [correspondant], Marco Stronati.

https://github.com/chatziko/location-guard

The purpose of Location Guard is to protect the user's location during the use of a location-based service, in an easy and intuitive way that makes it available to the general public. Various modern applications, running either on smartphones or on the web, allow third parties to obtain the user's location. A smartphone application can obtain this information from the operating system using a system call, while web application obtain it from the browser using a JavaScript call.

Although both mobile operating systems and browsers require the user's permission to disclose location information, the user faces an "all-or-nothing" choice: either disclose his exact location and give up his privacy, or stop using the application. This forces many users to disclose their location, although ideally they would like to enjoy some privacy.

The API level of a browser or an operating system is an ideal place for integrating a location obfuscation technique, in a way that is easy to understand for the average user, and readily available to all applications. When an application asks for the user's location, the browser or operating system can ask the user's permission, but including the option to provide an obfuscated location instead of the real one! Different levels of obfuscation can be also offered, so that the user can chose to provide more accurate location to applications that really need it, and more noisy location to those that don't.

In 2015, Location Guard matured with several additions and fixes throughout the year, and was selected by Mozilla as the pick of the month for June 2015, confirming the users' general interest in location privacy.

Moreover in 2015 we set the foundations for actively using Location Guard as a platform for performing research on location privacy. Since location data are sensitive, since the creation of Location Guard we chose to collect no data whatsoever from the users. However, such data are invaluable for research purposes. As a consequence, we created a framework for *locally* collecting data at the user's machine, perform an analysis also locally, and collect back only the results of the analysis for research purposes.

7. New Results

7.1. Foundations of information hiding

Information hiding refers to the problem of protecting private information while performing certain tasks or interactions, and trying to avoid that an adversary can infer such information. This is one of the main areas of research in Comète; we are exploring several topics, described below.

7.1.1. On the information leakage of differentially-private mechanisms

Differential privacy aims at protecting the privacy of participants in statistical databases. Roughly, a mechanism satisfies differential privacy if the presence or value of a single individual in the database does not significantly change the likelihood of obtaining a certain answer to any statistical query posed by a data analyst. Differentially-private mechanisms are often oblivious: first the query is processed on the database to produce a true answer, and then this answer is adequately randomized before being reported to the data analyst. Ideally, a mechanism should minimize leakage, i.e., obfuscate as much as possible the link between reported answers and individuals' data, while maximizing utility, i.e., report answers as similar as possible to the true ones. These two goals, however, are in conflict with each other, thus imposing a trade-off between privacy and utility.

In [12] we used quantitative information flow principles to analyze leakage and utility in oblivious differentially-private mechanisms. We introduced a technique that exploits graph symmetries of the adjacency relation on databases to derive bounds on the min-entropy leakage of the mechanism. We considered a notion of utility based on identity gain functions, which is closely related to min-entropy leakage, and we derived bounds for it. Finally, given some graph symmetries, we provided a mechanism that maximizes utility while preserving the required level of differential privacy.

7.1.2. Geo-indistinguishability: A Principled Approach to Location Privacy

With the increasing popularity of handheld devices, location-based applications and services have access to accurate and real-time location information, raising serious privacy concerns for their users. In [17] we reported on our ongoing project aimed at protecting the privacy of the user when dealing with location-based services. The starting point of our approach is the principle of geo-indistinguishability, a formal notion of privacy that protects the user's exact location, while allowing approximate information – typically needed to obtain a certain desired service – to be released. We then presented two mechanisms for achieving geo-indistinguishability, one generic to sanitize locations in any setting with reasonable utility, the other custom-built for a limited set of locations but providing optimal utility. Finally we extended our mechanisms to the case of location traces, where the user releases his location repeatedly along the day and we provide a method to limit the degradation of the privacy guarantees due to the correlation between the points. All the mechanisms were tested on real datasets and compared both among themselves and with respect to the state of the art in the field.

7.1.3. Constructing elastic distinguishability metrics for location privacy

The recently introduced notion of geo-indistinguishability tries to address the problem of accessing location-aware services in a privacy-friendly way by adapting the well-known concept of differential privacy to the area of location-based systems. Although geo-indistinguishability presents various appealing aspects, it has the problem of treating space in a uniform way, imposing the addition of the same amount of noise everywhere on the map.

In [13] we proposed a novel elastic distinguishability metric that warps the geometrical distance, capturing the different degrees of density of each area. As a consequence, the obtained mechanism adapts the level of noise while achieving the same degree of privacy everywhere. We also showed how such an elastic metric can easily incorporate the concept of a "geographic fence" that is commonly employed to protect the highly recurrent locations of a user, such as his home or work. We performed an extensive evaluation of our technique by building an elastic metric for Paris' wide metropolitan area, using semantic information from the OpenStreetMap database. We compared the resulting mechanism against the Planar Laplace mechanism satisfying standard geo-indistinguishability, using two real-world datasets from the Gowalla and Brightkite location-based social networks. The results showed that the elastic mechanism adapts well to the semantics of each area, adjusting the noise as we move outside the city center, hence offering better overall privacy.

7.1.4. Quantitative Information Flow for Scheduler-Dependent Systems

Quantitative information flow analyses measure how much information on secrets is leaked by publicly observable outputs. One area of interest is to quantify and estimate the information leakage of composed systems. Prior work has focused on running disjoint component systems in parallel and reasoning about the leakage compositionally, but has not explored how the component systems are run in parallel or how the leakage of composed systems can be minimised.

In [23] we considered the manner in which parallel systems can be combined or scheduled. This considers the effects of scheduling channels where resources may be shared, or whether the outputs may be incrementally observed. We also generalised the attacker's capability, of observing outputs of the system, to consider attackers who may be imperfect in their observations, e.g. when outputs may be confused with one another, or when assessing the time taken for an output to appear. Our main contribution was to present how scheduling and observation affect information leakage properties. In particular, that scheduling can hide some leaked information from perfect observers, while some scheduling may reveal secret information that is hidden to imperfect observers. In addition we presented an algorithm to construct a scheduler that minimises the min-entropy leakage and min-capacity in the presence of any observer.

7.2. Foundations of Concurrency

Distributed systems have changed substantially in the recent past with the advent of phenomena like social networks and cloud computing. In the previous incarnation of distributed computing the emphasis was on consistency, fault tolerance, resource management and related topics; these were all characterized by *interaction between processes*. Research proceeded along two lines: the algorithmic side which dominated the Principles Of Distributed Computing conferences and the more process algebraic approach epitomized by CONCUR where the emphasis was on developing compositional reasoning principles. What marks the new era of distributed systems is an emphasis on managing access to information to a much greater degree than before.

7.2.1. An Algebraic View of Space/Belief and Extrusion/Utterance for Concurrency/Epistemic Logic

The notion of constraint system (cs) is central to declarative formalisms from concurrency theory such as process calculi for concurrent constraint programming (ccp). Constraint systems are often represented as lattices: their elements, called constraints, represent partial information and their order corresponds to entailment. Recently a notion of n-agent spatial cs was introduced to represent information in concurrent constraint programs for spatially distributed multi-agent systems. From a computational point of view a

spatial constraint system can be used to specify partial information holding in a given agent's space (local information). From an epistemic point of view a spatial cs can be used to specify information that a given agent considers true (beliefs). Spatial constraint systems, however, do not provide a mechanism for specifying the mobility of information/processes from one space to another. Information mobility is a fundamental aspect of concurrent systems.

In the poster paper [24] we discussed using constraint systems with an algebraic operator that correspond to moving information in-between spaces as to mimic the mobility of data of distributed systems such as posting opinions/lies to other spaces or publicly disclosing data. In the conference paper [22] we enriched spatial constraint systems with operators to specify information and processes moving from a space to another. We referred to these news structures as spatial constraint systems with extrusion. We investigated the properties of this new family of constraint systems and illustrated their applications. From a computational point of view the new operators provide for process/information extrusion, a central concept in formalisms for mobile communication. From an epistemic point of view extrusion corresponds to a notion we called utterance; a piece of information that an agent communicates to others but that may be inconsistent with the agent's beliefs. Utterances can then be used to express instances of epistemic notions, which are commonplace in social media, such as hoaxes or intentional lies. Spatial constraint systems with extrusion can be seen as complete Heyting algebras equipped with maps to account for spatial and epistemic specifications. In the journal paper [28] we extended our work in [22] by showing that spatial constraint systems can also express the epistemic notion of knowledge by means of a derived spatial operator that specifies global information.

7.2.2. A Labelled Semantics for Soft Concurrent Constraint Programming

In [21] we presented a labelled semantics for Soft Concurrent Constraint Programming (SCCP), a language where concurrent agents may synchronize on a shared store by either posting or checking the satisfaction of (soft) constraints. SCCP generalizes the classical formalism by parametrising the constraint system over an order-enriched monoid: the monoid operator is not required to be idempotent, thus adding the same information several times may change the store. The novel operational rules are shown to offer a sound and complete co-inductive technique to prove the original equivalence over the unlabelled semantics.

7.2.3. Verification methods for concurrent Constraint Programming

Concurrent Constraint Programming (CCP) is a well-established declarative framework from concurrency theory. Its foundations and principles e.g., semantics, proof systems, axiomatizations, have been thoroughly studied for over the last two decades. In contrast, the development of algorithms and automatic verification procedures for CCP have hitherto been far too little considered.

To the best of our knowledge there is only one existing verification algorithm for the standard notion of CCP program (observational) equivalence. In [16] we first showed that this verification algorithm has anexponential-time complexity even for programs from a representative sub-language of CCP; the summation-free fragment (CCP+). We then significantly improved on the complexity of this algorithm by providing two alternative polynomial-time decision procedures for CCP+ program equivalence. Each of these two procedures has an advantage over the other. One has a better time complexity. The other can be easily adapted for the full language of CCP to produce significant state space reductions. The relevance of both procedures derives from the importance of CCP+. This fragment, which has been the subject of many theoretical studies, has strong ties to first-order logic and an elegant denotational semantics, and it can be used to model real-world situations. Its most distinctive feature is that of confluence, a property we exploit to obtain our polynomial procedures.

Bisimilarity is a standard behavioral equivalence in concurrency theory. However, only recently a well-behaved notion of bisimilarity for CCP, and a CCP partition refinement algorithm for deciding the strong version of this equivalence have been proposed. Weak bisimilarity is a central behavioral equivalence in process calculi and it is obtained from the strong case by taking into account only the actions that are observable in the system. Typically, the standard partition refinement can also be used for deciding weak bisimilarity simply by using Milner's reduction from weak to strong bisimilarity; a technique referred to as saturation. In [15] we demonstrated that, because of its involved labeled transitions, the above-mentioned saturation technique does not work for CCP. We also gave an alternative reduction from weak CCP bisimilarity to the strong one that

allows us to use the CCP partition refinement algorithm for deciding this equivalence. We also proved that due to distinctive nature of CCP, the new method does not introduce infinitely-branching in the resulting transition systems. Finally, we derived an algorithm to automatically verify the notion of weak bisimilarity in CCP.

The ntcc calculus extends CCP with the notion of discrete time-units for the specification of reactive systems. Moreover, ntcc features constructors for non-deterministic choices and asynchronous behavior, thus allowing for (1) synchronization of processes via constraint entailment during a time-unit and (2) synchronization of processes along time-intervals. In [20] we developed the techniques needed for the automatic verification of ntcc programs based on symbolic model checking. We showed that the internal transition relation, modeling the behavior of processes during a time-unit (1 above), could be symbolically represented by formulas in a suitable fragment of linear time temporal logic. Moreover, by using standard techniques as difference decision diagrams, we provided a compact representation of these constraints. Then, relying on a fixpoint characterization of the timed constructs, we obtained a symbolic model of the observable transition (2 above). We proved that our construction is correct with respect to the operational semantics. Finally, we introduced a prototypical tool implementing our method.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. Large-scale initiatives

Project acronym: CAPPRIS

Project title: Collaborative Action on the Protection of Privacy Rights in the Information Society

Duration: September 2013 - September 2016

URL: https://cappris.inria.fr/

Coordinator: Daniel Le Metayer, Inria Grenoble

Other partner institutions: The project involves four Inria research centers (Saclay, Saphia-Antipolis, Rennes and Grenoble), CNRS-LAAS, Eurecom and the university of Namur. Besides computer scientists, the consortium also includes experts in sociology and in law, thus covering the complementary areas of expertise required to reach the objectives.

Abstract: The goal of this project is to study the challenges related to privacy in the modern information society, trying to consider not only the technical, but also the social and legal ones, and to develop methods to enhance the privacy protection.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. MEALS

Program: FP7-PEOPLE-2011-IRSES

Project acronym: MEALS

Project title: Mobility between Europe and Argentina applying Logic to Systems

Duration: October 2011 - September 2015

URL: http://www.meals-project.eu/

Coordinator: Holger Hermans, Saarland University, Germany

Coordinator for the Inria sites: Catuscia Palamidessi, Inria Saclay

Other partner institutions: Rheinisch-Westfälische Technische Hochschule Aachen, Germany. Technische Universität Dresden, Germany. Inria, France. Imperial College of Science, Technology and Medicine, UK, University of Leicester, UK. Technische Universiteit Eindhoven, NL. Universidad Nacional de Cordoba, AR. Universidad de Buenos Aires, AR. Instituto Tecnologico de Buenos Aires, AR. Universidad Nacional de Rio Cuarto, AR.

Abstract: In this project we focus on three aspects of formal methods: specification, verification, and synthesis. We consider the study of both qualitative behavior and quantitative behavior (extended with probabilistic information). We aim to study formal methods in all their aspects: foundations (their mathematical and logical basis), algorithmic advances (the conceptual basis for software tool support) and practical considerations (tool construction and case studies).

8.3. International Initiatives

8.3.1. Inria-MSR joint lab

8.3.1.1. Privacy-Friendly Services and Apps

Title: Privacy-Friendly Services and Applications

Inria principal investigator: Catuscia Palamidessi

International Partners:

Cedric Fournet, Microsoft Research Lab, Cambridge, UK

Andy Gordon, Microsoft Research Lab, Cambridge, UK

Duration: 2014 - 2016

URL: http://www.msr-inria.fr/projects/privacy-friendly-services-and-apps/

Abstract: This is a project sponsored by Microsoft Research Lab, on methods to preserve privacy in web services and location-based services.

8.3.2. Inria Associate Teams

8.3.2.1. PRINCESS

Title: Protecting privacy while preserving data access

Inria principal investigator: Catuscia Palamidessi

International Partners:

Geoffrey Smith, Florida International University (United States)

Carroll Morgan, NICTA (Australia)

Annabelle McIver, Maquarie University (Australia)

Duration: 2013 - 2015

URL: http://www.lix.polytechnique.fr/comete/Projects/Princess/

Abstract: PRINCESS is an Inria associated team focusing on the protection of privacy and confidential information. In particular, we study the issues related to the leakage of confidential information through public observables.

We aim at developing a meaningful notion of measure in order to quantify the leakage of information, and to design mechanisms to limit the amount of leakage, without interfering too severely with the utility of the information that is meant to be disclosed.

The main topics currently investigated are quantitative information flow, where we are developing a decision-theoretic approach, and differential privacy, where we are developing an extension which lifts the basic notion of privacy meant for databases to arbitrary domains.

8.3.3. Inria International Partners

8.3.3.1. Informal International Partners

Moreno Falaschi, Professor, University of Siena, Italy

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil

Charles Carroll Morgan, Professor, University of New South Wales, Australia

Daniel Gebler, PhD student at the Free University of Amsterdam, The Netherlands

Camilo Rueda, Professor, Universidad Javeriana Cali, Colombia

8.3.4. Participation In other International Programs

8.3.4.1. PACE

Program: ANR Blanc International

Project title: Beyond plain Processes: Analysis techniques, Coinduction and Expressiveness

Duration: January 2013 - December 2016

URL: http://perso.ens-lyon.fr/daniel.hirschkoff/pace/

Coordinator: Daniel Hirschkoff, Ecole Normale Supérieure de Lyon

Other PI's and partner institutions: Catuscia Palamidessi, Inria Saclay. Davide Sangiorgi, University of Bologna (Italy). Yuxi Fu, Shanghai Jiao Tong University (China).

Abstract: This project objective is to enrich and adapt these methods, techniques, and tools to much broader forms of interactive models, well beyond the realm of "traditional" processes.

8.3.4.2. LOCALI

Program: ANR Blanc International

Project title: Logical Approach to Novel Computational Paradigms

Duration: January 2012 - December 2016

URL: http://www.agence-nationale-recherche.fr/?Project=ANR-11-IS02-0002

Coordinator: Gilles Dowek, Inria Rocquencourt

Other PI's and partner institutions: Catuscia Palamidessi, Inria Saclay. Thomas Erhard, Paris VII. Ying Jiang , Chinese Academy of Science in Beijin (China).

Abstract: This project aims at exploring the interplays between logic and sequential/distributed computation in formalisms like the lambda calculus and the π calculus. Going back to the fundamentals of the definitions of these calculi, the project plans to design new programming languages and proof systems via a logical approach.

8.3.4.3. MUSICAL

Program: CNPq Science Without Borders.

Project title: Music and Spatial Interaction with Constraints, Algebra and Logic: Foundations and Applications.

Duration: Oct 2014 - Oct 2016

URL: http://cic.puj.edu.co/~caolarte/musical/Musical/Welcome.html

Coordinator: Elaine Pimentel, Universidade Federal do Rio Grande do Norte (Brazil),

Other PI's and partner institutions: Camilo Rueda, PUJ Cali (Colombia). Carlos Olarte, Universidade Federal do Rio Grande do Norte (Brazil). Frank Valencia, CNRS-LIX and Inria Saclay (France). Gerard Assayag, IRCAM (France).

Abstract: This multi-disciplinary project aims to develop and integrate tools from logic and concurrency theory for the design and analysis of reactive systems and to their application to musical processes and multimedia systems.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Santiago Quintero, Undergraduate Student, Universidad Javeriana Cali, Colombia, Nov 2015 to Dec 2015

Camilo Rueda, Professor, Universidad Javeriana Cali, Colombia, Nov 2015 to Dec 2015

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil, Dec 2015

Annabelle McIver, Associate Professor, Macquarie University, Australia, Dec 2015

Carroll Morgan, Professor, University of New South Wales and NICTA, Australia, Dec 2015

Geoffrey Smith, Professor, Florida International University, USA, Dec 2014

8.4.2. Visits to International Teams

Frank Valencia visited the team of Camilo Rueda (AVISPA) at Pontifical Universidad Javeriana Cali, from Feb 2015 until Feb 2015

Frank Valencia visited the team of Camilo Rueda (AVISPA) at Pontifical Universidad Javeriana Cali, from July 2015 until July 2015

9. Dissemination

9.1. Promoting Scientific Activities

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

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committee

Catuscia Palamidessi is member of:

The Executive Committee of SIGLOG, the ACM Special Interest Group on Logic and Computation. Since 2014.

The Organizing Committee of LICS, the ACM/IEEE Symposium on Logic in Computer Science. Since 2010.

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 Steering Committee of EACSL, the European Association for Computer Science Logics. Since 2015.

The IFIP Technical Committee 1 – Foundations of Computer Science. Since 2007.

The IFIP Working Group 2.2 – Formal Description of Programming Concepts. Since 2001.

The IFIP Working Group 1.7 – Theoretical Foundations of Security Analysis and Design. Since 2010.

Frank D. Valencia is member of:

The steering committee of the International Workshop in Concurrency EXPRESS. Since 2010.

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committee

Catuscia Palamidessi:

has served as PC chair of LICS 2015. 30th Annual ACM/IEEE Symposium on Logic in Computer Science. Kyoto, Japan, 6-10 July 2015.

Frank Valencia:

has served as PC chair (with Camilo Rueda and Martin Leucker as co-chairs) of ICTAC 2015: The 12th International Colloquium on Theoretical Aspects of Computing. Cali, Colombia Oct 29-31 2015. Co-located with 11th International Workshop on Developments in Computational Models DCM 2015.

as general chair of ICTAC 2015: The 12th International Colloquium on Theoretical Aspects of Computing. Cali, Colombia Oct 29-31 2015.

9.1.2.2. Member of the conference program committee

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

ICTAC 2016. 13th International Colloquium on Theoretical Aspects of Computing Taipei, Taiwan, 24-31 October 2016.

CONCUR 2016. The 27th International Conference on Concurrency Theory. Québec City, Canada, 23-26 August 2016.

TASE 2016. The 10th International Symposium on Theoretical Aspects of Software Engineering. Shanghai, China, 17-19 July 2016.

FCS 2016. The Workshop on Foundations of Computer Security. Lisbon, Portugal, 27 June 2016.

MFPS XXXII. The Thirty-second Conference on the Mathematical Foundations of Programming Semantics. Carnegie Mellon University, Pittsburgh, USA, 23-26 May 2016.

PhDs in Logic VIII. Darmstadt, Germany, 9-11 May 2016.

UEOP 2016. The 1st Workshop on Understanding and Enhancing Online Privacy. San Diego, USA, 21 February 2016.

ATVA 2015. The 13th International Symposium on Automated Technology for Verification and Analysis. Shanghai, China, 12-15 October 2015.

WPES 2015. The Workshop on Privacy in the Electronic Society. Denver, Colorado, USA, 12 October 2015.

QEST 2015. The 12th International Conference on Quantitative Evaluation of SysTems. Madrid, Spain, 1-3 September 2015.

LOPSTR 2015. The 25th International Symposium on Logic-Based Program Synthesis and Transformation. Siena, Italy, 13-15 July 2015.

FORTE 2015. The 35th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems. Inria Grenoble, France, 2-4 June 2015.

TPDP 2015. Theory and Practice of Differential Privacy London, UK, 18 April 2015.

Konstantinos Chatzikokolakis is/has been a member of the program committees of the following conferences and workshops:

PETS 2016: The 16th Privacy Enhancing Technologies Symposium

WWW 2016: 25th World Wide Web conference

ICISSP 2015: 1st International Conference on Information Systems Security and Privacy

PETS 2015: The 15th Privacy Enhancing Technologies Symposium

FCS 2015: Workshop on Foundations of Computer Security

TPDP 2015: 1st workshop on the Theory and Practice of Differential Privacy

QAPL 2015: 13th Workshop on Quantitative Aspects of Programming Languages

APVP 2015: 6ème Atelier sur la Protection de la Vie Privée

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

PPDP 2016. The 18th International Symposium on Principles and Practice of Declarative Programming (PPDP 2016).

ICTAC 2016. The 13th International Colloquium on Theoretical Aspects of Computing (ICTAC 2016).

PPDP 2015. The 17th International Symposium on Principles and Practice of Declarative Programming (PPDP 2014). Siena, Italy, July 14-16, 2015.

ICLP DC 2015. 11th ICLP Doctoral Consortium.

9.1.2.3. Reviewer

The members of the team reviewed several papers for international conferences and workshops.

9.1.3. Journal

9.1.3.1. Member of the editorial board

Catuscia Palamidessi is:

Member of the Editorial Board of Mathematical Structures in Computer Science, published by the Cambridge University Press.

Member of the Editorial Board of Acta Informatica, published by the Springer.

Member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, Elsevier Science.

Member of the Editorial Board of LIPIcs: Leibniz International Proceedings in Informatics, Schloss Dagstuhl –Leibniz Center for Informatics.

Konstantinos Chatzikokolakis is:

Editorial board member of the newly established Proceedings on Privacy Enhancing Technologies (PoPETs), a scholarly journal for timely research papers on privacy.

9.1.3.2. Reviewer

The members of the team reviewed several papers for international journals.

9.1.4. Other Editorial Activities

Catuscia Palamidessi is/has been:

Co-editor of the special issue on Quantitative Information Flow on Mathematical Structures in Computer Science. 2015.

Frank D. Valencia has been:

Co-editor of the special issue on Mathematical Structures in Computer Science dedicated to the best papers from the 12th International Colloquium on Theoretical Aspects of Computing.

9.1.5. Other Activities

9.1.5.1. Invited talks

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

ETAPS 2015 (Unifying speaker). The European Joint Conferences on Theory and Practice of Software. London, UK, 11-18 April 2015.

QAPL 2015 (Invited speaker). Thirteenth International Workshop on Quantitative Aspects of Programming Languages and Systems. London, UK, 11-12 April 2015.

ICTAC 2015 (Keynote speaker). The 12th International Colloquium on Theoretical Aspects of Computing. Cali, Colombia, 29-31 October 2015.

9.1.5.2. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

Member of the Alonzo Church Award Committee. Since 2014. This award is for an outstanding contribution to Logic and Computation within the past 25 years.

Member of the Swedish Research Council Committee for Computer Science, 2015. The main duty of this committee is to evaluate and select the grant applications.

President of the selection committee for the EATCS Best Paper Award at the ETAPS conferences. Since 2006.

Member of the EAPLS PhD Award committee. Since 2010.

9.1.5.3. Service

Catuscia Palamidessi serves as:

Member of the Comité d'Orientation Scientifique et Technique, Groupe de travail Relation Internationales (COST-GTRI). Since November 2007.

Directrice adjointe du LIX, le Laboratoire d'Informatique de l'Ecole Polytechnique. April 2010 - December 2015.

Member of the Comité de These for Mathematics and Computer Science at the École Polytechnique. October 2007 - September 2015.

Reviewer for the projects proposal for the program PRIN, sponsored by the Italian MIUR ("Ministero dell'Istruzione, dell'Università e della Ricerca"). Since 2004.

Member of the comité de selection for two full professor positions at l'Université de Paris VII (Paris Diderot). Spring 2015.

Member of the comité de selection for a position for Maitre de Conferences à l'Université de Lorraine.

Frank Valencia served as:

President of the Selection Committee for the LIX Postdoctoral Fellowship. May - July 2014.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

PhD : Catuscia Palamidessi has been teaching a course for PhD students, on Protection of sensitive information, at the BISS 2015, the Bertinoro International Spring School. Bertinoro, Italy. March 2015. Total 13 hours.

PhD: Konstantinos Chatzikokolakis has been teaching a course for PhD students, on Security and Information Flow, at the ICTAC 2015 Summer School. Cali, Colombia. Oct 2015. Total 5 hours.

Master : Frank D. Valencia has been teaching the masters course "Computability Theory", 60 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. July 27 - Nov 1, 2015.

Master: Konstantinos Chatzikokolakis and Catuscia Palamidessi have been teaching a course on the Foundations of Privacy at the MPRI, the Master Parisien puor la Recherche en Informatique. University of Paris VII. A.Y. 2015-16. Total: 24 hours plus 6 hours for the exam and the exercise session is preparation to the exam.

9.2.2. Supervision

PhD in progress (2015-) Joris Lamare. Ecole Polytechnique. Grant MSR Center. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis.

PhD in progress (2014-) Michel Guzman. Ecole Polytechnique. Grant Inria CORDI-S. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

PhD in progress (2013-) Salim Percy. Ecole Polytechnique. Grant Digiteo-Digicosme. Co-supervised by Frank D. Valencia and Stefan Haar.

PhD in progress (2012-15) Marco Stronati. Ecole Polytechnique. Grant EDX Monge. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis.

PhD in progress (2011-15) Lili Xu. Ecole Polytechnique and Chinese academy of Science, Beijing, China. Co-supervised by Catuscia Palamidessi and Huimin Li.

9.2.3. Juries

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

Hamid Ebadi, PhD student supervised by David Sands, Chalmers University, Sweden. June 2015. The thesis is still in progress, Catuscia Plamidessi was reviewer and member of the committee for for the half-way thesis defense, that in Sweden is called Licentiate.

Frank Valencia has been a member of the committee board for the following PhD students:

Thierry Martinez, Title of the thesis: *Execution models for Constraint Programming: kernel language design through semantics equivalence.*. Advised by Francois Fages. University Paris-Diderot. Defended in Dec 2015.

Jaime Arias, Title of the thesis: *Formal Semantics and Automatic Verification of Hierarchical Multimedia Scenarios with Inter- active Choice.*. Advised by Myriam Desainte-Catherine. University of Bordeaux. Defended in Nov 2015.

9.2.4. Other didactical duties

Catuscia Palamidessi is:

Co-responsible of the Master 2 course on Concurrency since 2003, first at the DEA in Theoretical Computer Science (Paris) and then at the MPRI.

External member of the scientific council for the PhD in Computer Science at the University of Pisa, Italy. Since 2012.

Member of the Committee d'Encadrement de Thèse of Jun Wang (PhD student supervised by Qiang Tang and Peter Ryan), University of Luxembourg. Since December 2014.

Member of the advising committee for the PhD of Andrea Margheri (PhD student supervised by Rosario Pugliese), University of Florence, Italy. Since 2014.

Konstantinos Chatzikokolakis and Catuscia Palamidessi have designed, and coordinate, a course on the Foundations of Privacy at the MPRI, the Master Parisien puor la Recherche en Informatique. University of Paris VII. A.Y. 2015-16.

10. Bibliography

Major publications by the team in recent years

[1] M. ALVIM, M. ANDRÉS, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *On the relation between Differential Privacy and Quantitative Information Flow*, in "38th International Colloquium on Automata, Languages and Programming (ICALP 2011)", Zurich, Switzerland, J. S. LUCA ACETO (editor), Lecture Notes in Computer Science, Springer, 2011, vol. 6756, pp. 60-76 [*DOI :* 10.1007/978-3-642-22012-8_4], http://hal.inria.fr/inria-00627937/en

[2] M. ALVIM, K. CHATZIKOKOLAKIS, C. PALAMIDESSI, G. SMITH. *Measuring Information Leakage using Generalized Gain Functions*, in "Computer Security Foundations", Cambridge MA, United States, IEEE, 2012, pp. 265-279 [*DOI :* 10.1109/CSF.2012.26], http://hal.inria.fr/hal-00734044

[3] M. ANDRÉS, N. BORDENABE, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Geo-Indistinguishability: Differential Privacy for Location-Based Systems*, in "20th ACM Conference on Computer and Communications Security", Berlin, Allemagne, ACM Press, 2013, pp. 901-914, DGA, Inria large scale initiative CAPPRIS [*DOI :* 10.1145/2508859.2516735], http://hal.inria.fr/hal-00766821

[4] A. ARISTIZÁBAL, F. BONCHI, C. PALAMIDESSI, L. PINO, D. VALENCIA. *Deriving Labels and Bisimilarity for Concurrent Constraint Programming*, in "FOSSACS 2011 : 14th International Conference on Foundations of Software Science and Computational Structures", Saarbrücken, Germany, M. HOFMANN (editor), Lecture Notes in Computer Science, Springer, March 2011, vol. 6604, pp. 138-152 [*DOI :* 10.1007/ISBN 978-3-642-19804-5], https://hal.archives-ouvertes.fr/hal-00546722

[5] N. E. BORDENABE, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Optimal Geo-Indistinguishable Mechanisms for Location Privacy*, in "CCS - 21st ACM Conference on Computer and Communications Security", Scottsdale, Arizona, United States, G.-J. AHN, M. YUNG, N. LI (editors), Proceedings of the 21st ACM Conference on Computer and Communications Security, ACM, November 2014, pp. 251-262 [*DOI :* 10.1145/2660267.2660345], https://hal.inria.fr/hal-00950479

[6] K. CHATZIKOKOLAKIS, M. ANDRÉS, N. BORDENABE, C. PALAMIDESSI. *Broadening the Scope of Differential Privacy Using Metrics*, in "The 13th Privacy Enhancing Technologies Symposium", Bloomington, Indiana, États-Unis, E. DE CRISTOFARO, M. WRIGHT (editors), Springer, 2013, vol. 7981, pp. 82-102, DGA, Inria large scale initiative CAPPRIS [*DOI :* 10.1007/978-3-642-39077-7], http://hal.inria.fr/hal-00767210

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

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

[9] S. KNIGHT, C. PALAMIDESSI, P. PANANGADEN, F. D. VALENCIA. *Spatial and Epistemic Modalities in Constraint-Based Process Calculi*, in "CONCUR 2012 - Concurrency Theory - 23rd International Conference, CONCUR 2012", Newcastle upon Tyne, United Kingdom, September 2012, vol. 7454, pp. 317-332 [*DOI :* 10.1007/978-3-642-32940-1], http://hal.inria.fr/hal-00761116

[10] 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, pp. 59–68, http://hal.inria.fr/inria-00201096/en/

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] M. STRONATI. *Designing Location Privacy Mechanisms for flexibility over time and space*, Ecole Polytechnique, September 2015, https://pastel.archives-ouvertes.fr/tel-01243295

Articles in International Peer-Reviewed Journals

[12] M. S. ALVIM, M. E. ANDRÉS, K. CHATZIKOKOLAKIS, P. DEGANO, C. PALAMIDESSI. *On the information leakage of differentially-private mechanisms*, in "Journal of Computer Security", 2015, vol. 23, n^{o} 4, pp. 427-469 [*DOI :* 10.3233/JCS-150528], https://hal.inria.fr/hal-00940425

[13] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, M. STRONATI. *Constructing elastic distinguishability metrics for location privacy*, in "Proceedings on Privacy Enhancing Technologies", June 2015, vol. 2015, n^{o} 2, pp. 156-170 [*DOI :* 10.1515/POPETS-2015-0023], https://hal.inria.fr/hal-01270197

[14] M. FALASCHI, C. OLARTE, C. PALAMIDESSI. *Abstract Interpretation of Temporal Concurrent Constraint Programs*, in "Theory and Practice of Logic Programming", 2015, vol. 15, n^{o} 3, pp. 312-357, https://hal.inria.fr/hal-00945462

[15] L. PINO, A. ARISTIZABAL, F. BONCHI, F. VALENCIA. *Weak CCP bisimilarity with strong procedures*, in "Science of Computer Programming", 2015, vol. 100, pp. 84-104 [*DOI :* 10.1016/J.SCICO.2014.09.007], https://hal.inria.fr/hal-00976768

[16] L. F. PINO DUQUE, F. BONCHI, F. VALENCIA. *Efficient Algorithms for Program Equivalence for Confluent Concurrent Constraint Programming*, in "Science of Computer Programming", 2015, vol. 111, pp. 135-155 [*DOI :* 10.1016/J.SCICO.2014.12.003], https://hal.archives-ouvertes.fr/hal-01098502

Invited Conferences

[17] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, M. STRONATI. *Geo-indistinguishability: A Principled Approach to Location Privacy*, in "ICDCIT 2015 - Proceedings of the 11th International Conference on Distributed Computing and Internet Technology", Bhubaneswar, India, G. B. RAJA NATARAJAN, M. R. PATRA (editors), Lecture Notes in Computer Science, Springer, February 2015, vol. 8956, pp. 49-72 [*DOI :* 10.1007/978-3-319-14977-6_4], https://hal.inria.fr/hal-01114241

[18] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, M. STRONATI. *Location Privacy via Geo-Indistinguishability*, in "Proceedings of the 12th International Colloquium on Theoretical Aspects of Computing (ICTAC)", Cali, Colombia, M. LEUCKER, C. RUEDA, F. D. VALENCIA (editors), Lectures Notes in Computer Science, Springer, 2015, vol. 9399, pp. 28-38, https://hal.archives-ouvertes.fr/hal-01271276

[19] C. PALAMIDESSI. *Quantitative Approaches to the Protection of Private Information: State of the Art and Some Open Challenges*, in "Proceedings of the 4th International Conference on Principles of Security and Trust (POST)", London, United Kingdom, R. FOCARDI, A. C. MYERS (editors), Lecture Notes in Computer Science, Springer, 2015, vol. 9036, pp. 3-7, https://hal.archives-ouvertes.fr/hal-01271518

International Conferences with Proceedings

[20] J. ARIAS, M. GUZMÁN, C. OLARTE. *A Symbolic Model for Timed Concurrent Constraint Programming*, in "Ninth Workshop on Logical and Semantic Frameworks, with Applications (LSFA 2014)", Brasília D.F., Brazil, M. AYALA-RINCÓN, I. MACKIE (editors), Electronic Notes in Theoretical Computer Science, Elsevier, 2015, vol. 312, pp. 161-177 [*DOI :* 10.1016/J.ENTCS.2015.04.010], https://hal.inria.fr/hal-01257078

[21] F. GADDUCCI, F. SANTINI, L. PINO, F. VALENCIA. *A Labelled Semantics for Soft Concurrent Constraint Programming*, in "Proceedings of the 16th IFIP WG 6.1 International Conference on Coordination Models and Languages (COORDINATION 2015)", Grenoble, France, T. HOLVOET, M. VIROLI (editors), Lecture Notes

in Computer Science, Springer, June 2015, vol. 9037, pp. 133-149 [*DOI :* 10.1007/978-3-319-19282-6_9], https://hal.inria.fr/hal-01149227

[22] S. HAAR, S. PERCHY, C. RUEDA, F. VALENCIA. *An Algebraic View of Space/Belief and Extrusion/Utterance for Concurrency/Epistemic Logic*, in "17th International Symposium on Principles and Practice of Declarative Programming (PPDP 2015)", Siena, Italy, E. ALBERT, M. FALASCHI (editors), ACM SIGPLAN, July 2015, pp. 161-172 [*DOI :* 10.1145/2790449.2790520], https://hal.inria.fr/hal-01256984

[23] Y. KAWAMOTO, T. GIVEN-WILSON. *Quantitative Information Flow for Scheduler-Dependent Systems*, in "The 13th International Workshop on Quantitative Aspects of Programming Languages and Systems (QAPL 2015)", London, United Kingdom, Electronic Proceedings in Theoretical Computer Science, April 2015, forthcoming, https://hal.inria.fr/hal-01114778

[24] S. PERCHY, F. VALENCIA. *Opinions and Beliefs as constraint system operators*, in "Technical Communications of the 31st International Conference on Logic Programming (ICLP 2015)", Cork, Ireland, M. D. VOS, T. EITER, Y. LIERLER, F. TONI (editors), August 2015, vol. 1, 1 p. , Appears as Abstract Paper at the Technical Communications of the 31st International Conference on Logic Programming (ICLP 2015), https://hal.inria.fr/hal-01257098

Scientific Books (or Scientific Book chapters)

[25] M. E. ANDRÉS, G. SMITH, C. PALAMIDESSI. *Special Issue on Quantitative Information Flow*, Mathematical Structures in Computer Science, Cambridge University Press, 2015, vol. 25, n^{o} 2 [*DOI :* 10.1017/S0960129513000583], https://hal.archives-ouvertes.fr/hal-01271678

[26] D. CHIARUGI, M. FALASCHI, C. PALAMIDESSI. *A Declarative View of Signaling Pathways*, in "Programming Languages with Applications to Biology and Security", C. BODEI, G. L. FERRARI, C. PRIAMI (editors), Lecture Notes in Computer Science, Springer, 2015, vol. 9465, pp. 183-201, https://hal.archives-ouvertes.fr/hal-01271650

[27] M. LEUCKER, C. RUEDA, F. VALENCIA. *Theoretical Aspects of Computing - ICTAC 2015*, Springer, October 2015, vol. 9399 [*DOI :* 10.1007/978-3-319-25150-9], https://hal.inria.fr/hal-01257171

Other Publications

[28] M. GUZMAN, S. HAAR, S. PERCHY, C. RUEDA, F. VALENCIA. *Space and Extrusion in Epistemic Concurrent Constraint Systems*, January 2016, Submitted to the Journal of Logical and Algebraic Methods in Programming, https://hal.inria.fr/hal-01257113

References in notes

[29] N. E. BORDENABE. *Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy*, École Polytechnique, September 2014, https://pastel.archives-ouvertes.fr/tel-01098088