
IN PARTNERSHIP WITH:
**CNRS**

**Ecole Polytechnique**

Activity Report 2016

# 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. - Model-checking
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]

**Engineer**

Yamil Salim Perchy [Inria, granted by ERC (European Research Council Excecutive Agency)]

**PhD Students**

Tymofii Prokopenko [Inria, from Sep 2016]
Michell Guzman [Inria]
Joris Lamare [Inria]
Yamil Salim Perchy [Inria, until Nov 2016]

**Post-Doctoral Fellow**

Ehab Elsalamouny [Inria, until Nov 2016]

**Visiting Scientists**

Mario Ferreira Alvim Junior [Assistant Professor, Federal University of Minas Gerais, Dec 2016]
Annabelle Mciver [Associate Professor, Macquarie University, Dec 2016]
Charles Carroll Morgan [Professor, University of New South Wales, Dec 2016]
Geoffrey Smith [Professor, Florida International University, USA, Dec 2016]
Yusuke Kawamoto [Research Scientist, AIST, Japan, May, Sep, Nov 2016]
Linda Brodo [University of Sassari, September-October 2016]
Moreno Falashi [University of Siena, September-October 2016]
Carlos Olarte [Universidade Federal do Rio Grande do Norte, Dec 2016]

**Administrative Assistants**

Marie Enee [Inria, until Nov 2016]

Hélèna Kutniak [Inria]

**Others**

Anna Pazii [Inria, Intern, from Jul 2016]
Thomas Ragel [Inria, Intern, from Jun 2016 until Jul 2016]
Susheel Suresh [Ecole Polytechnique, Intern, from May 2016 until Aug 2016]
Tymofii Prokopenko [Inria, Intern, from Apr 2016 until Aug 2016]

# 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, Tymofii Prokopenko, 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, 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, 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, Tymofii Prokopenko, 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 $\pi$-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. Notable New Projects and Contracts*

- New ANR project REPAS: Reliable and Privacy-Aware Software Systems via Bisimulation Metrics (Section 9.3.4.1)
- New industrial contract with Renault: Protection techniques for location data (Section 8.1.1)

# 6. New Software and Platforms

## 6.1. libqif - A Quantitative Information Flow C++ Toolkit Library

**Participants:** Konstantinos Chatzikokolakis [correspondant], Susheel Suresh, Tymofii Prokopenko.

https://github.com/chatziko/libqif

The goal of libqif is to provide an efficient C++ toolkit implementing a variety of techniques and algorithms from the area of quantitative information flow and differential privacy. We plan to implement all techniques produced by Comète in recent years, as well as several ones produced outside the group, giving the ability to privacy researchers to reproduce our results and compare different techniques in a uniform and efficient framework.

Some of these techniques were previously implemented in an ad-hoc fashion, in small, incompatible with each-other, non-maintained and usually inefficient tools, used only for the purposes of a single paper and then abandoned. We aim at reimplementing those – as well as adding several new ones not previously implemented – in a structured, efficient and maintainable manner, providing a tool of great value for future research. Of particular interest is the ability to easily re-run evaluations, experiments and case-studies from all our papers, which will be of great value for comparing new research results in the future.

The library was under constant development in 2016 with several new features added this year. The project's git repository shows for this year 77 commits by 2 contributors, containing 5697 line additions and 4067 line removals. Some of the techniques already implemented are:

- Standard leakage measures: Shannon, min-entropy, guessing entropy
- Measures from the $g$-leakage framework [26]
- Channel factorization
- Hyper distribution produced by a channel run under a prior
- Standard differential privacy mechanisms from the literature
- The planar Laplace mechanism of [27]
- The planar Geometric mechanism
- The tight-constraints mechanism of [29] (also with equality constraints)
- Optimal mechanism construction under DP
- The standard Kantorovich metric as well as the multiplicative variant from [28]
- Additive capacity for specific prior over all gain functions [2]
- All operations are supported for both doubles (for precision) and floats (for memory efficiency)
- All operations involving only rational quantities are supported using arbitrary precision rational arithmetic, allowing to obtain exact results
- Native linear programing for rationals
- Simple installation in OSX via Homebrew

Many more are scheduled to be added in the near future.

## 6.2. D-SPACES - constraint systems with space and extrusion operators

**Participants:** Frank Valencia, Yamil Salim Perchy.

http://www.lix.polytechnique.fr/~perchy/d-spaces/

D-SPACES is an implementation of constraint systems with space and extrusion operators. Constraint systems are algebraic models that allow for a semantic language-like representation of information in systems where the concept of space is a primary structural feature. We give this information mainly an epistemic interpretation and consider various agents as entities acting upon it. D-SPACES is coded as a c++11 library providing implementations for constraint systems, space functions and extrusion functions. The interfaces to access each implementation are minimal and thoroughly documented. D-SPACES also provides property-checking methods as well as an implementation of a specific type of constraint systems (a boolean algebra). This last implementation serves as an entry point for quick access and proof of concept when using these models. In [22] an illustrative example of using the library is given, in the form of a small social network where users post their beliefs and utter their opinions.

## 6.3. Trace Slicer for Timed Concurrent Constraint Programming

**Participants:** Catuscia Palamidessi, Carlos Olarte.

http://subsell.logic.at/slicer/

Concurrent Constraint Programming (CCP) is a declarative model for concurrency aimed at specifying reactive systems, i.e. systems that continuously interact with the environment. Some previous works have developed (approximated) declarative debuggers for CCP languages. However, the task of debugging concurrent programs remains difficult. This tool is a companion for the existing debugging techniques. Slicing in our proposal consists of considering partial computations, which show the presence of bugs. Often, the quantity of information in a trace is overwhelming, and the user gets easily lost, since she cannot focus on the sources of the bugs. Our slicer allows for marking part of the state of the computation and assists the user to eliminate most of the redundant information in order to highlight the errors. See [19] for further details.

# 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. Axioms for Information Leakage*

Quantitative information flow aims to assess and control the leakage of sensitive information by computer systems. A key insight in this area is that no single leakage measure is appropriate in all operational scenarios; as a result, many leakage measures have been proposed, with many different properties. To clarify this complex situation, we studied in [17] information leakage axiomatically, showing important dependencies among different axioms. We also established a completeness result about the $g$-leakage family, showing that any leakage measure satisfying certain intuitively-reasonable properties can be expressed as a $g$-leakage.

### *7.1.2. Up-To Techniques for Generalized Bisimulation Metrics*

Bisimulation metrics allow us to compute distances between the behaviors of probabilistic systems. In [18] we presented enhancements of the proof method based on bisimulation metrics, by extending the theory of up-to techniques to (pre)metrics on discrete probabilistic concurrent processes.

Up-to techniques have proved to be a powerful proof method for showing that two systems are bisimilar, since they make it possible to build (and thereby check) smaller relations in bisimulation proofs. We defined soundness conditions for up-to techniques on metrics, and studied compatibility properties that allow us to safely compose up-to techniques with each other. As an example, we derived the soundness of the up-to-bisimilarity-metric-and-context technique.

The study was carried out for a generalized version of the bisimulation metrics, in which the Kantorovich lifting is parametrized with respect to a distance function. The standard bisimulation metrics, as well as metrics aimed at capturing multiplicative properties such as differential privacy, are specific instances of this general definition.

### *7.1.3. Compositional methods for information-hiding*

Systems concerned with information hiding often use randomization to obfuscate the link between the observables and the information to be protected. The degree of protection provided by a system can be expressed in terms of the probability of error associated with the inference of the secret information. In [12] we considered a probabilistic process calculus to specify such systems, and we studied how the operators affect the probability of error. In particular, we 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 these systems. As a case study, we applied these techniques to the Dining Cryptographers, and we derive a generalization of Chaum's strong anonymity result.

### *7.1.4. Differential Privacy Models for Location-Based Services*

In [13], we considered the adaptation of differential privacy to the context of location-based services (LBSs), which personalize the information provided to a user based on his current position. Assuming that the LBS provider is queried with a perturbed version of the position of the user instead of his exact one, we relied on differential privacy to quantify the level of indistinguishability (i.e., privacy) provided by this perturbation with respect to the user's position. In this setting, the adaptation of differential privacy can lead to various models depending on the precise form of indistinguishability required. We discussed the set of properties that hold for these models in terms of privacy, utility and also implementation issues. More precisely, we first introduced and analyzed one of these models, the (D,eps)-location privacy, which is directly inspired from the standard differential privacy model. In this context, we described a general probabilistic model for obfuscation mechanisms for the locations whose output domain is the Euclidean space $E^2$. In this model, we characterized the satisfiability conditions of (D,eps)-location privacy for a particular mechanism and also measured its utility with respect to an arbitrary loss function. Afterwards, we presented and analyzed symmetric mechanisms in which all locations are perturbed in a unified manner through a noise function, focusing in particular on circular noise functions. We proved that, under certain assumptions, the circular functions are rich enough to provide the same privacy and utility levels as other more complex (i.e., non-circular) noise functions, while being easier to implement. Finally, we extended our results to a generalized notion for location privacy, called 'l-privacy' capturing both (D,eps)-location privacy and also the notion of geo-indistinguishability recently introduced by Andrès, Bordenabe, Chatzikokolakis and Palamidessi.

### *7.1.5. Practical Mechanisms for Location Privacy*

The continuously increasing use of location-based services poses an important threat to the privacy of users. A natural defense is to employ an obfuscation mechanism, such as those providing geo-indistinguishability, a framework for obtaining formal privacy guarantees that has become popular in recent years.

Ideally, one would like to employ an optimal obfuscation mechanism, providing the best utility among those satisfying the required privacy level. In theory optimal mechanisms can be constructed via linear programming. In practice, however, this is only feasible for a radically small number of locations. As a consequence, all known applications of geo-indistinguishability simply use noise drawn from a planar Laplace distribution.

In [23] we studied methods for substantially improving the utility of location obfuscation, while having practical applicability as a central constraint. We provided such solutions for both infinite (continuous or discrete) as well as large but finite domains of locations, using a Bayesian remapping procedure as a key ingredient. We evaluated our techniques in two real world complete datasets, without any restriction on the evaluation area, and showed important utility improvements wrt the standard planar Laplace approach.

### *7.1.6. Preserving differential privacy under finite-precision semantics*

The approximation introduced by finite-precision representation of continuous data can induce arbitrarily large information leaks even when the computation using exact semantics is secure. Such leakage can thus undermine design efforts aimed at protecting sensitive information. In [14] we focussed on differential privacy, an approach to privacy that emerged from the area of statistical databases and is now widely applied also in other domains. In this approach, privacy is protected by adding noise to the values correlated to the private data. The typical mechanisms used to achieve differential privacy have been proved correct in the ideal case in which computations are made using infinite-precision semantics. We analyzed the situation at the implementation level, where the semantics is necessarily limited by finite precision, i.e., the representation of real numbers and the operations on them are rounded according to some level of precision. We showed that in general there are violations of the differential privacy property, and we studied the conditions under which we can still guarantee a limited (but, arguably, acceptable) variant of the property, under only a minor degradation of the privacy level. Finally, we illustrated our results on two examples: the standard Laplacian mechanism commonly used in differential privacy, and a bivariate version of it recently introduced in the setting of privacy-aware geolocation.

### 7.1.7. Quantifying Leakage in the Presence of Unreliable Sources of Information

Belief and min-entropy leakage are two well-known approaches to quantify information flow in security systems. Both concepts stand as alternatives to the traditional approaches founded on Shannon entropy and mutual information , which were shown to provide inadequate security guarantees. In [16] we unified the two concepts in one model so as to cope with the frequent (potentially inaccurate, misleading or outdated) attackers' side information about individuals on social networks, online forums, blogs and other forms of online communication and information sharing. To this end we proposed a new metric based on min-entropy that takes into account the adversary's beliefs.

### 7.1.8. On the Compositionality of Quantitative Information Flow

In the min-entropy approach to quantitative information flow, the leakage is defined in terms of a minimization problem, which, in the case of large systems, can be computationally rather heavy. The same happens for the recently proposed generalization called $g$-vulnerability. In [25] we studied the case in which the channel associated to the system can be decomposed into simpler channels, which typically happens when the observables consist of several components. Our main contribution is the derivation of bounds on the $g$-leakage of the whole system in terms of the $g$-leakages of its components. We also considered the particular cases of min-entropy leakage and of parallel channels, generalizing and systematizing results from the literature. We demonstrated the effectiveness of our method and evaluate the precision of our bounds using examples.

## 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. Belief, Knowledge, Lies and Other Utterances in an Algebra for Space and Extrusion

Spatial constraint systems are algebraic structures from concurrent constraint programming to specify spatial and epistemic behavior in multi-agent system. In [15], [11] we developed the theory of spatial constraint systems with operators to specify information and processes moving from a space to another. 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 such as hoaxes or intentional lies. Spatial constraint system can express the epistemic notion of belief by means of space functions that specify local information. We showed that spatial constraint can also express the epistemic notion of knowledge by means of a derived spatial operator that specifies global information. In [21] we reported on our progress using spatial constraint system as an abstract representation of modal and epistemic behaviour.

### 7.2.2. Deriving Inverse Operators for Modal Logic

In [20] we used spatial constraint systems to give an abstract characterization of the notion of normality in modal logic and to derive right inverse/reverse operators for modal languages. In particular, we identified the weakest condition for the existence of right inverses and showed that the abstract notion of normality corresponds to the preservation of finite suprema. We applied our results to existing modal languages such as the weakest normal modal logic, Hennessy-Milner logic, and linear-time temporal logic. We also discussed our results in the context of modal concepts such as bisimilarity and inconsistency invariance.

#### *7.2.3. D-SPACES: Implementing Declarative Semantics for Spatially Structured Information*

In [22] we introduced D-SPACES, an implementation of constraint systems with space and extrusion operators. D-SPACES is coded as a c++11 library providing implementations for constraint systems, space functions and extrusion functions. D-SPACES provides property-checking methods as well as an implementation of a specific type of constraint systems (boolean algebras). We illustrated the implementation with a small social network where users post their beliefs and utter their opinions.

#### *7.2.4. Slicing Concurrent Constraint Programs*

Concurrent Constraint Programming (CCP) is a declarative model for concurrency where agents interact by telling and asking constraints (pieces of information) in a shared store. Some previous works have developed (approximated) declarative debuggers for CCP languages. However, the task of debugging concurrent programs remains difficult. In [19] we defined a dynamic slicer for CCP and we showed it to be a useful companion tool for the existing debugging techniques. Our technique starts by considering a partial computation (a trace) that shows the presence of bugs. Often, the quantity of information in such a trace is overwhelming, and the user gets easily lost, since she cannot focus on the sources of the bugs. Our slicer allows for marking part of the state of the computation and assists the user to eliminate most of the redundant information in order to highlight the errors. We showed that this technique can be tailored to timed variants of CCP. We also developed a prototypical implementation freely available for making experiments.

# 8. Bilateral Contracts and Grants with Industry

## 8.1. Bilateral Contracts with Industry

#### *8.1.1. Contract with Renault*

Project title: Protection techniques for location data

Duration: July 2016 - December 2016

Budget: 38K euros, financed by Renault

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Abstract: The goal of this project is to produce a survey of the state of the art methods for protecting location data, as well as a protytype showing the application of some of these methods in the context of a “connected car”.

Stage: A six month intern (Anna Pazii) was funded by this project.

# 9. Partnerships and Cooperations

## 9.1. Regional Initiatives

#### *9.1.1. Projects funded by Digiteo-DigiCosme*

##### *9.1.1.1. OPTIMEC*

Project title: Optimal Mechanisms for Privacy Protection

Duration: September 2016 - August 2019

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI’s: Serge Haddadm ENS Cachan.

Abstract: In this project we plan to investigate classes of utility and privacy measures, and to devise methods to obtain optimal mechanisms with respect to the trade-off between utility and privacy. In order to represent the probabilistic knowledge of the adversary and of the user, and the fact that mechanisms themselves can be randomized, we will consider a probabilistic setting. We will focus, in particular, on measures that are expressible as linear functions of the probabilities.

*9.1.1.2. D-SPACES*

Project title: D-spaces : Distributed Spaces in Concurrent Epistemic Systems

Duration: Nov 2013 - Oct 2016

Coordinator: Frank Valencia, CNRS-LIX and Inria Saclay, EPI Comète

Other PI's: Stefan Haar ENS Cachan.

Abstract: In this project we developed an innovative and expressive computational model for these systems that coherently combines techniques for the analysis of concurrent systems such as process calculi with epistemic and spatial formalisms.

## 9.2. National Initiatives

### *9.2.1. Large-scale initiatives*

Project acronym: CAPPRIS

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

Duration: September 2013 - December 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.

## 9.3. International Initiatives

### *9.3.1. Inria-MSR joint lab*

*9.3.1.1. 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.

### *9.3.2. Inria Associate Teams*

*9.3.2.1. LOGIS*

Title: Logical and Formal Methods for Information Security

Inria principal investigator: Konstantinos Chatzikokolakis

International Partners:

Mitsuhiro Okada, Keio University (Japan)

Yusuke Kawamoto, AIST (Japan)

Tachio Terauchi, JAIST (Japan)

Masami Hagiya, University of Tokyo (Japan)

Start year: 2016

URL: http://www.lix.polytechnique.fr/~kostas/projects/logis/

Abstract: The project aims at integrating the logical / formal approaches to verify security protocols with (A) complexity theory and (B) information theory. The first direction aims at establishing the foundations of logical verification for security in the computational sense, with the ultimate goal of automatically finding attacks that probabilistic polynomial-time adversaries can carry out on protocols. The second direction aims at developing frameworks and techniques for evaluating and reducing information leakage caused by adaptive attackers.

### *9.3.3. Inria International Partners*

#### *9.3.3.1. Informal International Partners*

Geoffrey Smith, Florida International University (United States)

Carroll Morgan, NICTA (Australia)

Annabelle McIver, Maquarie University (Australia)

Moreno Falaschi, Professor, University of Siena, Italy

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

Camilo Rueda, Professor, Universidad Javeriana Cali, Colombia

### *9.3.4. Participation in Other International Programs*

#### *9.3.4.1. REPAS*

Program: ANR Blanc

Project title: Reliable and Privacy-Aware Software Systems via Bisimulation Metrics

Duration: October 2016 - September 2021

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's and partner institutions: Ugo del Lago, Inria Sophia Antipolis (EPI Focus) and University of Bologna (Italy). Vincent Danos, ENS Paris. Filippo Bonchi, ENS Lyon.

Abstract: In this project, we aim at investigating quantitative notions and tools for proving program correctness and protecting privacy. In particular, we will focus on bisimulation metrics, which are the natural extension of bisimulation on quantitative systems. As a key application, we will develop a mechanism to protect the privacy of users when their location traces are collected.

#### *9.3.4.2. 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, Frank Valencia, CNRS-LIX and Inria Saclay (France). 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.

*9.3.4.3. 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 $\pi$ 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.

*9.3.4.4. 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.

*9.3.4.5. CLASSIC*

Program: Colciencias - Conv. 712.

Project title: Concurrency, Logic and Algebra for Social and Spatial Interactive Computation.

Duration: Oct 2016 - Oct 2019

URL: http://goo.gl/Gv6Lij

Coordinator: Camilo Rueda PUJ Cali (Colombia).

Other PI's and partner institutions: Carlos Olarte, Universidade Federal do Rio Grande do Norte (Brazil). Frank Valencia, CNRS-LIX and Inria Saclay (France).

Abstract:This project will advance the state of the art of domains such as mathematical logic, order theory and concurrency for reasoning about spatial and epistemic behaviour in multi-agent systems..

## 9.4. International Research Visitors

### *9.4.1. Visits of International Scientists*

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil, Dec 2016

Annabelle McIver, Associate Professor, Macquarie University, Australia, Dec 2016

Carroll Morgan, Professor, University of New South Wales and NICTA, Australia, Dec 2016

Geoffrey Smith, Professor, Florida International University, USA, Dec 2016

Camilo Rueda, Professor, PUJ Cali, Colombia, May 2016 and Nov 2016.

Camilo Rocha, Professor, PUJ Cali, Colombia, Oct 2016.

#### *9.4.2. Visits to International Teams*

Catuscia Palamidessi visited the Computer Security team of Roberto Focardi at the University of Venice, Italy, from 4 April to 30 April, 2016.

# 10. Dissemination

## 10.1. Promoting Scientific Activities

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

### *10.1.1. Scientific events organisation*

*10.1.1.1. 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 Steering Committee of CONCUR, the International Conference in Concurrency Theory. Since 2016.

The Steering Committee of FORTE, the International Conference on Formal Techniques for Distributed Objects, Components, and Systems. Since 2014.

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.

### 10.1.2. Scientific events selection

*10.1.2.1. Member of conference program committees*

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

ICTAC 2017. The 14th International Colloquium on Theoretical Aspects of Computing. Hanoi, Vietnam, 23-27 October 2017.

TASE 2017. The 11th International Symposium on Theoretical Aspects of Software Engineering. Nice, France, 13-15 September 2017.

CONCUR 2017. The 28th International Conference on Concurrency Theory. Berlin, Germany, 5-8 September 2017.

CSL 2017. The 26th EACSL Annual Conference on Computer Science Logic. Stockholm, Sweden, 20-25 August 2017.

ICSOFT-PT 2017. The 12th International Conference on Software Paradigm Trends. Lisbon, Portugal, 24-26 July 2017.

ICALP 2017 (Track B). The 44th International Colloquium on Automata, Languages, and Programming. Warsaw, Poland, 10–14 July 2017.

FORTE 2017. The 37th IFIP International Conference on Formal Techniques for Distributed Objects, Components, and Systems. Neuchâtel, Switzerland, 19-22 June 2017.

CSR 2017. The 12th International Computer Science Symposium in Russia. Kazan, Russia, 8–12 June 2017.

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

LOPSTR 2016. The 26th International Symposium on Logic-Based Program Synthesis and Transformation, 6-8 September 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.

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

ICDE 2017: IEEE International Conference on Data Engineering

CSF 2017: 30th IEEE Computer Security Foundations Symposium

POST 2017: 6th International Conference on Principles of Security and Trust

BIGQP 2017: International Workshop on Big Geo Data Quality and Privacy

PETS 2016: The 16th Privacy Enhancing Technologies Symposium

WWW 2016: 25th World Wide Web conference

APVP 2016: 7ème 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).

ICLP DC 2016. 12th ICLP Doctoral Consortium.

*10.1.2.2. Reviewer*

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

### *10.1.3. Journals*

*10.1.3.1. 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 Springer.

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

*10.1.3.2. Reviewer*

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

### *10.1.4. Other Editorial Activities*

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.

### *10.1.5. Other Activities*

*10.1.5.1. Invited talks*

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

DISCOTEC 2016 (Keynote speaker). The 11th International Federated Conference on Distributed Computing Techniques. Crete, Greece, 6-9 June 2016.

Journée sur la Securité, la Sureté et la Confidentialité. Organized by Paris VII, Paris XIII and Systematic. Paris, France, 10 May 2016.

*10.1.5.2. Participation in other committees*

Catuscia Palamidessi has been serving in the following committees:

Member of the Alonzo Church Award Committee. Since 2015. This award is for an outstanding contribution to Logic and Computation within the past 25 years.

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

*10.1.5.3. Service*

Catuscia Palamidessi has served as:

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 a position for Maitre de Conferences at l'Université de Paris VII (Paris Diderot). Spring 2016.

Frank Valencia has served as:

Directeur adjoint de l'UMR 7161, le Laboratoire d'Informatique de l'Ecole Polytechnique (LIX). May 2016 - .

## 10.2. Teaching - Supervision - Juries

### *10.2.1. Teaching*

PhD : Catuscia Palamidessi has been teaching a course for PhD students, on Protection of sensitive information, at the University of Venice, Italy. April 2016. Total 30 hours.

Master : Frank D. Valencia has been teaching the undergraduate course "Computability", 45 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. July 27 - Nov 1, 2016.

Master : Frank D. Valencia has been teaching the masters course "Foundations of Computer Science", 45 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. Jan 27 - Jun 1, 2016.

Master: Konstantinos Chatzikokolakis and Catuscia Palamidessi have been teaching a course on the Foundations of Privacy at the MPRI, the Master Parisien pour la Recherche en Informatique. University of Paris VII. A.Y. 2016-17. Total: 24 hours plus 6 hours for the exam and the exercise session is preparation to the exam.

### *10.2.2. Supervision*

PhD in progress (2016-) Tymofii Prokopenko. Ecole Polytechnique and ENS Cachan. Grant Digiteo-Digicosme. Co-supervised by Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Serge Haddad.

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 completed (2013-16) Salim Percy. Ecole Polytechnique. Grant Digiteo-Digicosme. Co-supervised by Frank D. Valencia and Stefan Haar.

### *10.2.3. Juries*

Catuscia Palamidessi has been reviewer and member of the board at the PhD defense for the thesis of the following PhD student:

Huu-Hiep Nguyen, PhD student supervised by Abdessamad Imine, University of Lorraine, France. November 2016. Title of the thesis: Social Graph Anonymization.

### *10.2.4. Other didactical duties*

Catuscia Palamidessi is:

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. 2014-16.

Konstantinos Chatzikokolakis and Catuscia Palamidessi have designed, and coordinate, a course on the Foundations of Privacy at the MPRI, the Master Parisien pour la Recherche en Informatique. University of Paris VII. A.Y. 2016-17.

# 11. Bibliography

## Major publications by the team in recent years

[1] 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° 4, pp. 427-469 [*DOI :* 10.3233/JCS-150528], https://hal.inria.fr/hal-00940425

[2] M. S. ALVIM, K. CHATZIKOKOLAKIS, A. MCIVER, C. MORGAN, C. PALAMIDESSI, G. SMITH. *Additive and multiplicative notions of leakage, and their capacities*, in "27th Computer Security Foundations Symposium (CSF 2014)", Vienna, Austria, IEEE, July 2014, pp. 308–322 [*DOI :* 10.1109/CSF.2014.29], https://hal.inria.fr/hal-00989462

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

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

[9] M. GUZMAN, S. HAAR, S. PERCHY, C. RUEDA, F. VALENCIA. *Belief, Knowledge, Lies and Other Utterances in an Algebra for Space and Extrusion*, in "Journal of Logical and Algebraic Methods in Programming", September 2016 [*DOI :* 10.1016/J.JLAMP.2016.09.001], https://hal.inria.fr/hal-01257113

[10] 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

## Publications of the year

### Doctoral Dissertations and Habilitation Theses

[11] S. PERCHY. *Opinions, Lies and Knowledge. An Algebraic Approach to Mobility of Information and Processes*, Université Paris-Saclay, October 2016, https://hal.inria.fr/tel-01413970

### Articles in International Peer-Reviewed Journals

[12] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, C. BRAUN. *Compositional methods for information-hiding*, in "Mathematical Structures in Computer Science", September 2016, vol. 26, n$^{o}$ 6, pp. 908-932 [*DOI :* 10.1017/S0960129514000292], https://hal.inria.fr/hal-01006384

[13] E. ELSALAMOUNY, S. GAMBS. *Differential Privacy Models for Location- Based Services*, in "Transactions on Data Privacy", 2016, vol. 9, n$^{o}$ 1, pp. 15 - 48, https://hal.inria.fr/hal-01418136

[14] I. GAZEAU, D. MILLER, C. PALAMIDESSI. *Preserving differential privacy under finite-precision semantics*, in "Journal of Theoretical Computer Science (TCS)", 2016, https://hal.inria.fr/hal-01390927

[15] M. GUZMAN, S. HAAR, S. PERCHY, C. RUEDA, F. VALENCIA. *Belief, Knowledge, Lies and Other Utterances in an Algebra for Space and Extrusion*, in "Journal of Logical and Algebraic Methods in Programming", September 2016 [*DOI :* 10.1016/J.JLAMP.2016.09.001], https://hal.inria.fr/hal-01257113

[16] S. HAMADOU, C. PALAMIDESSI, V. SASSONE. *Quantifying Leakage in the Presence of Unreliable Sources of Information*, in "Journal of Computer and System Sciences", 2017, forthcoming, https://hal.inria.fr/hal-01421417

### International Conferences with Proceedings

[17] M. S. ALVIM, K. CHATZIKOKOLAKIS, A. MCIVER, C. MORGAN, C. PALAMIDESSI, G. SMITH. *Axioms for Information Leakage*, in "29th Computer Security Foundations Symposium (CSF 2016)", Lisbon, Portugal, IEEE, June 2016, 16 p. , https://hal.inria.fr/hal-01330414

[18] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, V. VIGNUDELLI. *Up-To Techniques for Generalized Bisimulation Metrics*, in "27th International Conference on Concurrency Theory (CONCUR 2016)", Québec City, Canada, Leibniz International Proceedings in Informatics (LIPIcs), August 2016, vol. 59, pp. 35:1–35:14 [*DOI :* 10.4230/LIPICS.CONCUR.2016.35], https://hal.inria.fr/hal-01335234

[19] M. FALASCHI, M. GABBRIELLI, C. OLARTE, C. PALAMIDESSI. *Slicing Concurrent Constraint Programs*, in "Pre-proceedings of the 26th International Symposium on Logic-Based Program Synthesis and Transformation

(LOPSTR 2016)", Edinburgh, United Kingdom, M. V. HERMENEGILDO, P. LOPEZ-GARCIA (editors), 2016, https://hal.inria.fr/hal-01421407

[20] M. GUZMAN, S. PERCHY, C. RUEDA, F. VALENCIA. *Deriving Inverse Operators for Modal Logic*, in "Theoretical Aspects of Computing – ICTAC 2016", Taipei, Taiwan, A. SAMPAIO, F. WANG (editors), Theoretical Aspects of Computing – ICTAC 2016, Springer, October 2016, vol. 9965, pp. 214-232 [*DOI :* 10.1007/978-3-319-46750-4_13], https://hal.inria.fr/hal-01328188

[21] M. GUZMÁN, F. D. VALENCIA. *On the Expressiveness of Spatial Constraint Systems* , in "ICLP 2016 - Proceedings of the Technical Communications of the 32nd International Conference on Logic Programming", New York, United States, M. CARRO, A. KING, N. SAEEDLOEI, M. D. VOS (editors), Technical Communications of the 32nd International Conference on Logic Programming (ICLP 2016), John Gallagher and Germán Vidal, October 2016, vol. OASICS Vol. 52, pp. 16:1 - 16:12, Appears as a Technical Communications of the 32nd International Conference on Logic Programming (ICLP 2016) [*DOI :* 10.4230/OASIcs.ICLP.2016.16], https://hal.inria.fr/hal-01418166

[22] S. HAAR, S. PERCHY, F. VALENCIA. *D-SPACES: Implementing Declarative Semantics for Spatially Structured Information*, in "11th International Conference on Semantic Computing", San Diego, California, United States, IEEE ICSC 2017, IEEE, January 2017, vol. 11, https://hal.inria.fr/hal-01328189

### Other Publications

[23] K. CHATZIKOKOLAKIS, E. ELSALAMOUNY, C. PALAMIDESSI. *Practical Mechanisms for Location Privacy*, 2016, working paper or preprint, https://hal.inria.fr/hal-01422842

[24] K. CHATZIKOKOLAKIS, C. PALAMIDESSI, A. PAZII. *Methods for Location Privacy: A comparative overview*, 2016, Submitted for publication, https://hal.inria.fr/hal-01421457

[25] Y. KAWAMOTO, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *On the Compositionality of Quantitative Information Flow*, 2016, Submitted for publication to Logical Methods in Computer Science, https://hal.inria.fr/hal-01421424

## References in notes

[26] 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

[27] 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

[28] K. CHATZIKOKOLAKIS, D. GEBLER, C. PALAMIDESSI, L. XU. *Generalized bisimulation metrics*, in "CONCUR - 25th Conference on Concurrency Theory", Rome, Italy, P. BALDAN, D. GORLA (editors), Lecture Notes in Computer Science, Springer, September 2014, vol. 8704, pp. 32-46 [*DOI :* 10.1007/978-3-662-44584-6_4], https://hal.inria.fr/hal-01011471

[29] E. ELSALAMOUNY, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *Generalized differential privacy: regions of priors that admit robust optimal mechanisms*, in "Horizons of the Mind. A Tribute to Prakash Panangaden", F.

VAN BREUGEL, E. KASHEFI, C. PALAMIDESSI, J. RUTTEN (editors), Lecture Notes in Computer Science, Springer International Publishing, 2014, vol. 8464, pp. 292-318 [*DOI :* 10.1007/978-3-319-06880-0_16], https://hal.inria.fr/hal-01006380