IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2018

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

1. Team, Visitors, External Collaborators **1**
2. Overall Objectives **2**
3. Research Program **2**
3.1. Probability and information theory 2
3.2. Expressiveness of Concurrent Formalisms 3
3.3. Concurrent constraint programming 3
3.4. Model checking 3
4. Application Domains **4**
5. New Software and Platforms **4**
5.1. libqif - A Quantitative Information Flow C++ Toolkit Library 4
5.2. F-BLEAU 5
5.3. Location Guard 5
5.4. dspacenet 5
6. New Results **6**
6.1. Foundations of information hiding 6
6.1.1. Secure Information Flow and Game Theory 6
6.1.2. The additive capacity problem for Quantitative Information Flow 7
6.1.3. Local Differential Privacy and Statistical Utility 7
6.1.4. Information-Theoretic Methods for Feature Selection in Machine Learning 7
6.1.5. A Logical Characterization of Differential Privacy via Behavioral Metrics 8
6.1.6. Probability and Nondeterminism in Process Calculi from a Logical Perspective 8
6.2. Foundations of Concurrency 8
6.2.1. Real-time Rewriting Logic Semantics for Spatial Concurrent Constraint Programming 9
6.2.2. Characterizing Right Inverses for Spatial Constraint Systems with Applications to Modal Logic 9
6.2.3. Observational and Behavioural Equivalences for Soft Concurrent Constraint Programming 9
7. Partnerships and Cooperations **9**
7.1. Regional Initiatives 9
7.1.1. OPTIMEC 9
7.1.2. SUPREME 10
7.2. National Initiatives 10
7.2.1. REPAS 10
7.2.2. MAGIC 10
7.3. International Initiatives 10
7.3.1. Inria Associate Teams 10
7.3.2. Participation in International Programs 11
7.3.2.1. CLASSIC 11
7.3.2.2. EPIC 11
7.3.2.3. FACTS 11
7.3.3. Inria International Partners 12
7.3.3.1. PriDat 12
7.3.3.2. Informal International Partners 12
7.4. International Research Visitors 12
7.4.1. Visits of International Scientists 12
7.4.2. Internships 12
8. Dissemination **13**
8.1. Promoting Scientific Activities 13
8.1.1. Scientific events organisation 13

8.1.2. Scientific events selection committee 13
8.1.2.1. Chair of conference program committee 13
8.1.2.2. Member of conference program committees 14
8.1.3. Journals 14
8.1.3.1. Member of the editorial board 14
8.1.3.2. Reviewing 15
8.1.4. Other Editorial Activities 15
8.1.5. Participation in other committees 15
8.1.6. Invited talks 16
8.1.7. Service 16
8.2. Teaching - Supervision - Juries 16
8.2.1. Teaching 16
8.2.2. Supervision 16
8.2.3. Juries 17
8.2.4. Other didactical duties 17
8.3. Popularization 17
8.3.1. Education 17
8.3.2. Interventions 18
9. Bibliography **18**

Project-Team COMETE

Creation of the Project-Team: 2008 January 01

Keywords:

Computer Science and Digital Science:

A2.1.1. - Semantics of programming languages
A2.1.5. - Constraint programming
A2.1.6. - Concurrent programming
A2.1.9. - Synchronous languages
A2.4.1. - Analysis
A2.4.2. - Model-checking
A3.4. - Machine learning and statistics
A4.1. - Threat analysis
A4.5. - Formal methods for security
A4.8. - Privacy-enhancing technologies

Other Research Topics and Application Domains:

B6.1. - Software industry
B6.6. - Embedded systems
B9.5.1. - Computer science
B9.10. - Privacy

1. Team, Visitors, External Collaborators

Research Scientists

Catuscia Palamidessi [Team leader, Inria, Senior Researcher]
Frank Valencia [CNRS, Researcher]
Konstantinos Chatzikokolakis [CNRS, Researcher, external member since Sep 2018 (détachement at the Univ. of Athens)]

Post-Doctoral Fellows

Valentina Castiglioni [Inria]
Ali Kassem [Inria, until Aug 2018]

PhD Students

Natasha Fernandes [Macquarie University, from Jul 2018]
Anna Pazii [Ecole Polytechnique]
Tymofii Prokopenko [Inria, until June 2018, Digicosme]
Santiago Quintero [Ecole Polytechnique, from Oct 2018]
Marco Romanelli [Inria, CORDI-S]

Technical staff

Ehab Elsalamouny [Inria, from Nov 2018, STIC]

Interns

Pedro Ignacio Bahamondes Walters [Ecole Polytechnique, from Sept 2017 until Mar 2018]
Noemie Fong [ENS Paris, from Apr 2018]
Kacem Lefki [Univ Paris-Saclay, from Jun 2018 until Oct 2018]
Arthur Passos de Rezende [Federal University of Minas Gerais, from Apr 2018 until Jun 2018]

Joaquín Rodríguez Felici [National University of Cordoba, until Jan 2018]
Haoteng Yin [University of Beijin, from Jun 2018 until Sep 2018]
Jason Lopez Narvaez [Universidad Javeriana Cali, Colombia, from May 2018 until Aug 2018]

Administrative Assistants

Jessica Gameiro [Inria, until Apr 2018]
Maria Agustina Ronco [Inria, from May 2018]

Visiting Scientists

Mario Ferreira Alvim Junior [Federal University of Minas Gerais, Brazil, Dec 2018]
Yusuke Kawamoto [AIST, Japan, Mar 2018 and Nov-Dec 2018]
Sergio Ramirez [Universidad Javeriana Cali, Colombia, from May 2018 until Jun 2018]
Carlos Olarte [Universidade Federal do Rio Grande do Norte, from Oct 2018 until Dec 2018]
Camilo Rueda [Universidad Javeriana Cali, Colombia, May 2018 and Nov 2018]

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, Marco Romanelli, Anna Pazii.

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: Frank Valencia, Santiago Quintero.

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: Catuscia Palamidessi, Konstantinos Chatzikokolakis, Ehab Elsalamouny, Ali Kassem, Anna Pazii, Marco Romanelli, Natasha Fernandes.

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. New Software and Platforms

5.1. libqif - A Quantitative Information Flow C++ Toolkit Library

KEYWORDS: Information leakage - Privacy - C++ - Linear optimization
FUNCTIONAL DESCRIPTION: 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's development continued in 2018 with several new added features. 82 new commits were pushed to the project's git repository during this year. The new functionality was directly applied to the exeperimental results of several publications of the team (QEST'18, Entropy'18, POST'18, CSF'18).

- Contact: Konstantinos Chatzikokolakis
- URL: https://github.com/chatziko/libqif

5.2. F-BLEAU

KEYWORDS: Information leakage - Machine learning - Privacy
FUNCTIONAL DESCRIPTION: F-BLEAU is a tool for estimating the leakage of a system about its secrets in a black-box manner (i.e., by only looking at examples of secret inputs and respective outputs). It considers a generic system as a black-box, taking secret inputs and returning outputs accordingly, and it measures how much the outputs "leak" about the inputs.

F-BLEAU is based on the equivalence between estimating the error of a Machine Learning model of a specific class and the estimation of information leakage.

This code was also used for the experiments of a paper under submission, on the following evaluations: Gowalla, e-passport, and side channel attack to finite field exponentiation.

RELEASE FUNCTIONAL DESCRIPTION: First F-BLEAU release. Supports frequentist and k-NN estimates with several parameters, and it allows stopping according to delta-convergence criteria.

- Contact: Konstantinos Chatzikokolakis
- URL: https://github.com/gchers/fbleau

5.3. Location Guard

KEYWORDS: Privacy - Geolocation - Browser Extensions
SCIENTIFIC DESCRIPTION: The purpose of Location Guard is to implement obfuscation techniques for achieving location privacy, in a an easy and intuitive way that makes them 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.
FUNCTIONAL DESCRIPTION: Websites can ask the browser for your location (via JavaScript). When they do so, the browser first asks your permission, and if you accept, it detects your location (typically by transmitting a list of available wifi access points to a geolocation provider such as Google Location Services, or via GPS if available) and gives it to the website.

Location Guard is a browser extension that intercepts this procedure. The permission dialog appears as usual, and you can still choose to deny. If you give permission, then Location Guard obtains your location and adds "random noise" to it, creating a fake location. Only the fake location is then given to the website.

Location Guard is by now a stable tool with a large user base. No new features were added in 2018, however the tool is still actively maintained, and several issues have beed fixed during this year (new geocoder API, manual installation method for Opera users, etc).

- Participants: Catuscia Palamidessi, Konstantinos Chatzikokolakis, Marco Stronati, Miguel Andrés and Nicolas Bordenabe
- Contact: Konstantinos Chatzikokolakis
- URL: https://github.com/chatziko/location-guard

5.4. dspacenet

Distributed-Spaces Network.
KEYWORDS: Social networks - Distributed programming

FUNCTIONAL DESCRIPTION: DSpaceNet is a tool for social networking based on multi-agent spatial and timed concurrent constraint language.

I - The fundamental structure of DSPaceNet is that of *space*: A space may contain

(1) spatial-mobile-reactive tcc programs, and (2) other spaces.

Furthermore, (3) each space belongs to a given agent. Thus, a space of an agent j within the space of agent i means that agent i allows agent j to use a computation sub-space within its space.

II - The fundamental operation of DSPaceNet is that of *program posting*: In each time unit, agents can post spatial-mobile-reactive tcc programs in the spaces they are allowed to do so (ordinary message posting corresponds to the posting of tell processes). Thus, an agent can for example post a watchdog tcc process to react to messages in their space, e.g. whenever (*happy b*frank*) do tell("thank you!"). More complex mobile programs are also allowed (see below).

The language of programs is a spatial mobile extension of tcc programs:

$P, Q... := tell(c)|whencdoP||nextP|P||Q|unlesscnextP|[P]\_i|\uparrow \_iP|recX.P$

computation of timed processes proceeds as in tcc. The spatial construct [P]_i runs P in the space of agent i and the mobile process uparrow_i P, extrudes P from the space of i. By combining space and mobility, arbitrary processes can be moved from one a space into another. For example, one could send a trojan watchdog to another space for spying for a given message and report back to one's space.

III- Constraint systems can be used to specify advance text message deduction, arithmetic deductions, scheduling, etc.

IV - Epistemic Interpretation of spaces can be used to derive whether they are users with conflicting/inconsistent information, or whether a group of agents may be able to deduce certain message.

V - The scheduling of agent requests for program posts, privacy settings, friendship lists are handled by an external interface. For example, one could use type systems to check whether a program complies with privacy settings (for example checking that the a program does not move other program into a space it is not allowed into).

- Partner: Pontificia Universidad Javeriana Cali
- Contact: Frank Valencia
- URL: http://www.dspacenet.com

6. New Results

6.1. Foundations of information hiding

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

6.1.1. Secure Information Flow and Game Theory

In the inference attacks studied in Quantitative Information Flow (QIF), the attacker typically tries to interfere with the system in the attempt to increase its leakage of secret information. The defender, on the other hand, typically tries to decrease leakage by introducing some controlled noise. This noise introduction can be modeled as a type of protocol composition, i.e., a probabilistic choice among different protocols, and its effect on the amount of leakage depends heavily on whether or not this choice is visible to the attacker. In [21], [11], we considered operators for modeling visible and hidden choice in protocol composition, and we studied their algebraic properties. We then formalized the interplay between defender and attacker in a game-theoretic framework adapted to the specific issues of QIF, where the payoff is information leakage. We considered various kinds of leakage games, depending on whether players act simultaneously or sequentially, and on

whether or not the choices of the defender are visible to the attacker. In the case of sequential games, the choice of the second player is generally a function of the choice of the first player, and his/her probabilistic choice can be either over the possible functions (mixed strategy) or it can be on the result of the function (behavioral strategy). We showed that when the attacker moves first in a sequential game with a hidden choice, then behavioral strategies are more advantageous for the defender than mixed strategies. This contrasts with the standard game theory, where the two types of strategies are equivalent. Finally, we established a hierarchy of these games in terms of their information leakage and provide methods for finding optimal strategies (at the points of equilibrium) for both attacker and defender in the various cases.

6.1.2. The additive capacity problem for Quantitative Information Flow

Preventing information leakage is a fundamental goal in achieving confidentiality. In many practical scenarios, however, eliminating such leaks is impossible. It becomes then desirable to quantify the severity of such leaks and establish bounds on the threat they impose. Aiming at developing measures that are robust wrt a variety of operational conditions, a theory of channel capacity for the g-leakage model was developed in [25], providing solutions for several scenarios in both the multiplicative and the additive setting. In [16] we continued this line of work by providing substantial improvements over the results of [25] for additive leakage. The main idea of employing the Kantorovich distance remains, but it is now applied to quasimetrics, and in particular the novel "convex-separation" quasimetric. The benefits were threefold: first, it allowed to maximize leakage over a larger class of gain functions, most notably including the one of Shannon. Second, a solution was obtained to the problem of maximizing leakage over both priors and gain functions, left open in [25]. Third, it allowed to establish an additive variant of the " Miracle " theorem from [26].

6.1.3. Local Differential Privacy and Statistical Utility

Local differential privacy (LDP) is a variant of differential privacy (DP) where the noise is added directly on the individual records, before being collected. The main advantage with respect to DP is that we do not need a trusted third party to collect and sanitise the sensitive data of the user. The main disadvantage is that the trade-off between privacy and utility is usually worse than in DP, and typically to retrieve reasonably good statistics from the locally sanitised data it is necessary to have access to a huge collection of them. In [22], we focused on the problem of estimating the counting queries on numerical data, and we proposed a variant of LDP based on the addition of geometric noise. Such noise function is known to have appealing properties in the case of counting queries. In particular, it is universally optimal for DP, i.e., it provides the best utility for a given level of DP, regardless of the side knowledge of the attacker. We explored the properties of geometric noise for counting queries in the LDP setting, and we conjectured an optimality property, similar to the one that holds in the DP setting. In [15] we proposed a variant of LDP suitable for metric spaces, such as location data or energy consumption data, and we showed that it provides a better utility, for the same level of privacy, then the other known LPD mechanisms.

6.1.4. Information-Theoretic Methods for Feature Selection in Machine Learning

The identification of the "best" features for classification is a problem of increasing importance in machine learning. The size of available datasets is becoming larger and larger, both in terms of samples and in terms of features of the samples, and keeping the dimensionality of the data under control is necessary for avoiding an explosion of the training complexity and for the accuracy of the classification. The known methods for reducing the dimensionality can be divided in two categories: those which transform the feature space by reshaping the original features into new ones (feature extraction), and those which select a subset of the features (feature selection). Several proposals for feature selection have successfully applied concepts and techniques from information theory. In [19] we proposed a new information-theoretic algorithm for ordering the features according to their relevance for classification. The novelty of our proposal consisted in adopting Rényi min-entropy instead of the commonly used Shannon entropy. In particular, we adopted a notion of conditional min-entropy that has been recently proposed in the field of security and privacy, and that avoids the anomalies of previously-attempted information-theoretic definitions. This notion is strictly related to the Bayes error, which is a promising property for achieving accuracy in the classification. We evaluated our

method on various classifiers and datasets, and we showed that it compares favorably to the corresponding one based on Shannon entropy.

6.1.5. A Logical Characterization of Differential Privacy via Behavioral Metrics

Differential privacy (DP) is a formal definition of privacy ensuring that sensitive information relative to individuals cannot be inferred by querying a database. In [18], we exploited a modeling of this framework via labeled Markov Chains (LMCs) to provide a logical characterization of differential privacy: we considered a probabilistic variant of the Hennessy-Milner logic and we defined a syntactical distance on formulae in it measuring their syntactic disparities. Then, we defined a trace distance on LMCs in terms of the syntactic distance between the sets of formulae satisfied by them. We proved that such distance corresponds to the level of privacy of the LMCs. Moreover, we used the distance on formulae to define a real-valued semantics for them, from which we obtained a logical characterization of weak anonymity: the level of anonymity is measured in terms of the smallest formula distinguishing the considered LMCs. Then, we focused on bisimulation semantics on nondeterministic probabilistic processes and we provide a logical characterization of generalized bisimulation metrics, namely those defined via the generalized Kantorovich lifting. Our characterization is based on the notion of mimicking formula of a process and the syntactic distance on formulae, where the former captures the observable behavior of the corresponding process and allows us to characterize bisimilarity. We showed that the generalized bisimulation distance on processes is equal to the syntactic distance on their mimicking formulae. Moreover, we used the distance on mimicking formulae to obtain bounds on differential privacy.

6.1.6. Probability and Nondeterminism in Process Calculi from a Logical Perspective

Behavioral equivalences and modal logics have been successfully employed for the specification and verification of communicating concurrent systems, henceforth processes. The former ones, in particular the family of bisimulations, provide a simple and elegant tool for the comparison of the observable behavior of processes. The latter ones allow for an immediate expression of the desired properties of processes. Since the work on the Hennessy-Milner logic (HML), these two approaches are connected by means of logical characterizations of behavioral equivalences: two processes are behaviorally equivalent if and only if they satisfy the same formulae in the logic. Hence, the characterization of an equivalence subsumes both the fact that the logic is as expressive as the equivalence and the fact that the equivalence preserves the logical properties of processes. However, the connection between behavioral equivalences and modal logics goes even further: modal decomposition of formulae exploits the characterization of an equivalence to derive its compositional properties. Roughly speaking, the definition of the semantic behavior of processes by means of the Structural Operational Semantics (SOS) framework allowed for decomposing the satisfaction problem of a formula for a process into the verification of the satisfaction problem of certain formulae for its subprocesses. In [12] we extended the SOS-driven decomposition approach to processes in which the nondeterministic behavior coexists with probability. To deal with the probabilistic behavior of processes, and thus with the decomposition of formulae characterizing it, we introduced a SOS-like machinery allowing for the specification of the behavior of open distribution terms. By our decomposition, we obtained (pre)congruence formats for probabilistic bisimilarity, ready similarity and similarity.

The combination of nondeterminism and probability in concurrent systems leads to different interpretations of process behavior. If we restrict our attention to linear properties only, we can identify three main approaches to trace and testing semantics: the trace distributions, the trace-by-trace and the extremal probabilities approaches. In [17] we proposed novel notions of behavioral metrics that are based on the three classic approaches above, and that can be used to measure the disparities in the linear behavior of processes wrt. trace and testing semantics. We studied the properties of these metrics, like non-expansiveness, and we compare their expressive powers.

6.2. 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.

6.2.1. Real-time Rewriting Logic Semantics for Spatial Concurrent Constraint Programming

In [20] we used rewriting logic for specifying and analyzing a calculus for concurrent constraint programming (ccp) processes combining spatial and real-time behavior. These processes can run processes in different computational spaces (e.g., containers) while subject to real-time requirements (e.g., upper bounds in the execution time of a given operation), which can be specified with both discrete and dense linear time. The real-time rewriting logic semantics is fully executable in Maude with the help of rewriting modulo SMT: partial information (i.e., constraints) in the specification is represented by quantifier-free formulas on the shared variables of the system that are under the control of SMT decision procedures. The approach is used to symbolically analyze existential real-time reachability properties of process calculi in the presence of spatial hierarchies for sharing information and knowledge.

6.2.2. Characterizing Right Inverses for Spatial Constraint Systems with Applications to Modal Logic

In [14] spatial constraint systems are used 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, a necessary and sufficient condition for the existence of right inverses is identified and the abstract notion of normality is shown to correspond to the preservation of finite suprema. Furthermore, a taxonomy of normal right inverses is provided, identifying the greatest normal right inverse as well as the complete family of minimal right inverses. These results were applied to existing modal languages such as the weakest normal modal logic, Hennessy-Milner logic, and linear-time temporal logic. Some implications of these results were also discussed in the context of modal concepts such as bisimilarity and inconsistency invariance.

6.2.3. Observational and Behavioural Equivalences for Soft Concurrent Constraint Programming

In [13] we presented a labelled semantics for Soft Concurrent Constraint Programming (SCCP), a meta-language where concurrent agents may synchronise on a shared store by either posting or checking the satisfaction of (soft) constraints. SCCP generalises the classical formalism by parametrising the constraint system over an order-enriched monoid, thus abstractly representing the store with an element of the monoid, and the standard unlabelled semantics just observes store updates. The novel operational rules were shown to offer a sound and complete co-inductive technique to prove the original equivalence over the unlabelled semantics. Based on this characterisation, we provided an axiomatisation for finite agents.

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. OPTIMEC

Project title: Optimal Mechanisms for Privacy Protection

Funded by: DigiCosme

Duration: September 2016 - July 2018

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's: Serge Haddad, ENS Cachan.

Abstract: In this project we investigate classes of utility and privacy measures, and we 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 consider a probabilistic setting. We focus, in particular, on measures that are expressible as linear functions of the probabilities.

7.1.2. SUPREME

Project title: Statistical-Utility Preserving Methods for Privacy Protection

Funded by: Département STIC

Duration: 2018 - 2019

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's: Serge Haddad, ENS Cachan.

Abstract: In this project we study the theoretical foundations, methods and tools to protect the privacy of the individuals under certain constraints. In particular we focus on mechanisms that: (1) are robust with respect to combination of information from different sources, (2) can be applied directly by the user, thus avoiding the need of a trusted party, and (3) provide an optimal trade-off between privacy and utility.

7.2. National Initiatives

7.2.1. 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 investigate quantitative notions and tools for proving program correctness and protecting privacy. In particular, we 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.

7.2.2. MAGIC

Program: PEPS I3A

Project title: Machine Games for Information Protection

Duration: February 2018 - December 2018

Coordinator: Konstantinos Chatzikokolakis, CNRS (EPI Comète) and Ecole Polytechnique

Other PI's and partner institutions: Giovanni Cherubin, EPFL, Switzerland. Serge Haddad, ENS Cachan.

Abstract: In this project, we study a Machine Learning approach to develop methods for the Protection of Private Information. The idea is based on the Generative Adversarial Network (GAN) paradigm: the defender and the attacker are modeled as two adversaries in a game, where the payoff is the attacker's acquisition of the user's private data by exploiting the system vulnerabilities, side information, and probabilistic inference.

7.3. International Initiatives

7.3.1. Inria Associate Teams

7.3.1.1. 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: January 2016 - December 2018

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.

7.3.2. Participation in International Programs

7.3.2.1. CLASSIC

Program: Colciencias - Conv. 712.

Project acronym: CLASSIC.

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, Universidad Javeriana de Cali, Colombia.

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

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..

7.3.2.2. EPIC

Program: STIC-Amsud.

Project acronym: EPIC.

Project title: EPistemic Interactive Concurrency/

Duration: Oct 2016 - Oct 2018.

URL: https://sites.google.com/site/sticamsudepic/

Coordinator: Frank Valencia, CNRS-LIX and Inria Saclay.

Other PI's and partner institutions: Carlos Olarte, Universidade Federal do Rio Grande do Norte, Brazil and Camilo Rueda, Universidad Javeriana de Cali, Colombia.

Abstract: The aim of the project is to coherently combine and advance the state of the art of domains such as concurrency theory, information theory and rewriting systems for reasoning about social networks.

7.3.2.3. FACTS

Program: ECOS NORD.

Project acronym: FACTS.

Project title: Foundational Approach to Cognition in Today?s Society.

Duration: Jan 1 2019 - Dec 31, 2021.

URL: https://goo.gl/zVhg32

Coordinator: Frank Valencia, Ecole Polytechnique.

Other PI's and partner institutions: Jean-Gabriel Ganascia LIP6, Sorbonne University and Camilo Rueda, Universidad Javeriana de Cali, Colombia.

Abstract: This projects aims at studying the phenomenon of "Group Polarization"; the tendency for a group to learn or acquire beliefs or to make decisions that are more extreme than the initial inclinations of its members.

7.3.3. Inria International Partners

7.3.3.1. PriDat

Project title: Privacy-Friendly Data Analytics

Funded by: Siebel Energy Institute

Duration: September 2018 - August 2019

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's: Giovanni Cherubin, EPFL, Switzerland. Moreno Falaschi, University of Siena, Italy. Mario Ferreira, Federal University of Minas Gerais, Brazil.

Abstract: The objective of this project is to develop methodologies for protecting the privacy of individuals while letting their data be collected and used for analytical purposes.

7.3.3.2. Informal International Partners

Geoffrey Smith, Florida International University, USA

Carroll Morgan, NICTA , Australia

Annabelle McIver, Maquarie University, Australia

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

Camilo Rueda, Professor, Universidad Javeriana de Cali, Colombia

Carlos Olarte, Universidade Federal do Rio Grande do Norte, Brazil

Camilo Rocha, Associate Professor, Universidad Javeriana de Cali, Colombia

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil. Dec 2018

Borja de Balle Pigem. Sr. Machine Learning Scientist. Amazon, UK. Dec 2018

Takao Murakami, Assistant Professor, National Institute of Advanced Industrial Science and Technology (AIST), Japan. Dec 2018

Yusuke Kawamoto, Assistant Professor, National Institute of Advanced Industrial Science and Technology (AIST), Japan. March 2018 and Nov-Dec 2018

Carlos Olarte, Assistant Professor, Universidade Federal do Rio Grande do Norte, Brazil. Oct-Dec 2018

Daniele Gorla, Professor, University of Rome "La Sapienza". Aug - Sep 2018.

Giovanna Broccia, PhD student, University of Pisa, Italy, June 2018

Camilo Rueda, Professor, Universidad Javeriana de Cali, Colombia. May 2018 and Nov 2018

Prakash Panangaden, University of McGill, Montreal, Canada. Feb 2018

7.4.2. Internships

Haoteng Yin. Academy for Advanced Interdisceplinary Studies, Peking University. From June 2018 until Sept 2018.

Kacem Kefki. University of Paris Saclay. From June 2018 until July 2018.

Arthur Américo. Universidade Federal de Minas Gerais. From April 2018 until June 2018.

Noémie Fong. ENS Paris. From April 2018 until Sept 2019.

Pedro Bahamondes. Ecole Polytechnique. From Sept 2017 until March 2018.

Joaquin Felici. Univ. of Cordoba. From Sept 2017 until Jan 2018.

Jason Lopez, Universidad Javeriana de Cali, Colombia. From May until Agost 2018.

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

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

The Organizing Committee of LICS, the ACM/IEEE Symposium on Logic in Computer Science. 2014-18.

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 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 1.7 – Theoretical Foundations of Security Analysis and Design. Since 2010.

The IFIP Working Group 1.8 – Concurrency Theory. Since 2005.

Frank D. Valencia is member of:

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

Konstantinos Chatzikokolakis is member of:

The steering committee of the Privacy Enhancing Technologies Symposium. Since 2018.

8.1.2. Scientific events selection committee

8.1.2.1. Chair of conference program committee

Konstantinos Chatzikokolakis:

is serving as PC chair (with Carmela Troncoso as co-chair) of PETS 2019: The 19th Privacy Enhancing Technologies Symposium, July 16-20, 2019, Stockholm, Sweden.

8.1.2.2. Member of conference program committees

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

PETS 2019. The 19th Privacy Enhancing Technologies Symposium. Stockholm, Sweden, 16–20 July, 2019.

LICS 2019. The Thirty-Fourth Annual ACM/IEEE Symposium on Logic in Computer Science. Vancouver, Canada, 24–27 June 2019.

CSF 2019. The 32nd IEEE Computer Security Foundations Symposium. Hoboken, NJ, USA, June 24-27, 2019.

SAC 2019 (Security track). The 34th ACM/SIGAPP Symposium On Applied Computing. Limassol, Cyprus, 8-12 April 2019.

FACS 2018. The 15th International Conference on Formal Aspects of Component Software. Pohang, South Corea, 10-12 October 2018.

TASE 2018. The 12th International Symposium on Theoretical Aspects of Software Engineering. Guangzhou, China, 29-31 August 2018.

PETS 2018. The 18th Privacy Enhancing Technologies Symposium. Barcelona, Spain, 24-27 July 2018.

FOSSACS 2018. The 21st International Conference on Foundations of Software Science and Computation Structures. (Part of ETAPS 2018.) Thessaloniki, Greece, 14-21 April 2018.

SOFSEM 2018. The 44th Annual Int'l Conference on Current Trends in Theory and Practice of Computer Science (track on Foundations of Computer Science). Krems an der Donau, Austria, 29 January- 2 February, 2018.

PPML 2018. Privacy Preserving Machine Learning (NeurIPS 2018 Workshop). Montréal, Canada, 8 December 2018.

APVP 2018. Atelier sur la Protection de la Vie Privée. Porquerolles, France, 3-6 juin 2018.

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

BMDA 2018: Workshop on Big Mobility Data Analytics

QAPL 2018: International Workshop on Quantitative Aspects of Programming Languages and Systems

HotSpot 2018: 6th Workshop on Hot Issues in Security Principles and Trust

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

CP-ICLP-SAT-DP-18. Doctoral Program of the 23rd International Conference on Principles and Practice of Constraint Programming.

CONCUR 2019. The 30th International Conference on Concurrency Theory. Amsterdam, the Netherlands, August 26-31, 2019.

AAMAS 2019. International Conference on Autonomous Agents and Multiagent Systems. Montreal, Canada, 13th-17th of May 2019.

8.1.3. Journals

8.1.3.1. Member of the editorial board

Catuscia Palamidessi is:

Member of the Editorial Board of the Proceedings on Privacy Enhancing Technologies (PoPETs), published by De Gruyter. Since 2017.

Member of the Editorial Board of Mathematical Structures in Computer Science, published by the Cambridge University Press. Since 2006.

Member of the Editorial Board of Acta Informatica, published by Springer. Since 2015.

Member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, published by Elsevier Science. Since 2000.

Member of the Editorial Board of LIPIcs: Leibniz International Proceedings in Informatics, Schloss Dagstuhl–Leibniz Center for Informatics. Since 2014.

Konstantinos Chatzikokolakis is:

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

8.1.3.2. Reviewing

The members of the team regularly review papers for international journals, conferences and workshops.

8.1.4. Other Editorial Activities

Catuscia Palamidessi is/has been:

Co-editor (with Anca Muscholl and Anuj Dawar) of the special issue of Logical Methods in Computer Science dedicated to selected papers of ICALP 2017.

Co-editor (with Alexandra Silva and Natarajan Shankar) of the special issue of Logical Methods in Computer Science dedicated to selected papers of LICS 2015 and LICS 2016.

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.

8.1.5. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

Member of the panel for the Research Evaluation for Development 2019 (RED19) of the Department of Computer Science and Engineering at the University of Gothenburg, Sweden.

Chair of the Nominating Committee for the 2019 renewal of the office holders of SIGLOG, the ACM Special Interest Group on Logic and Computation.

Member of the evaluation panel for the SU-ICT-03-2018: “Dynamic countering of cyber-attacks” - H2020 Work Programme 2018-2020.

Member of the evaluation panel for the program IKTPLUSS on Digital Security, Research Council of Norway (2018).

Member of the committee for the Alonzo Church Award for Outstanding Contributions to Logic and Computation. From 2015. In 2018 Palamidessi is the president of this committee.

Reviewer for the projects proposal for the program PRIN, sponsored by the Italian MIUR (“Ministero dell’Istruzione, dell’Università e della Ricerca”). Since 2005.

President of the selection committee for the EATCS Best Paper Award. From 2006 until 2018.

Member of the EAPLS PhD Award Committee. From 2010.

8.1.6. Invited talks

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

CSL 2018. The 27th Computer Science Logic Annual Conference. Birmingham, UK, 4–7 September 2018.

CSF 2018. The 31st IEEE Computer Security Foundations Symposium, Oxford, UK, 9-12 July 2018.

PROOFS 2018 (Keynote speaker). The 7th International Workshop on Security Proofs for Embedded Systems. Amsterdam, The Netherlands, 13 September 2018.

PiMLAI 2018 Privacy in Machine Learning and Artificial Intelligence (FAIM 2018 Workshop). Stockholm, Sweden, 15 July 2018.

Bernoulli Symposium. Opening Symposium of the new institute for Artificial Intelligence, Mathematics, and Computer Science of the University of Groningen. Groningen, The Netherlands, 1 November 2018.

Konstantinos Chatzikokolakis has given invited talks at the following conference:

QEST 2018. 15th International Conference on Quantitative Evaluation of SysTems, Beijing, China, September 4-7, 2018.

8.1.7. Service

Catuscia Palamidessi has served as:

Member of the committee for the assignment of the Inria International Chairs. From 2017.

Frank Valencia has served as:

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

Konstantinos Chatzikokolakis has served as:

Member of the hiring committee for the "poste enseignants-chercheur Gaspard Monge", Ecole Polytechnique, 2018.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

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, 2018.

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, 2018

Master : Konstantinos Chatzikokolakis has been teaching the masters course "Privacy Technologies", 40 hours, at the University of Athens, Greece. Oct - Dec, 2018.

8.2.2. Supervision

PhD in progress (2018-) Natasha Fernandez. Co-supervised Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Annabelle McIver. Thesis subject: Privacy Protection Methods for Textual Documents.

PhD in progress (2018-) Santiago Quintero. Co-supervised by Frank Valencia and Catuscia Palamidessi. Thesis Subject: Foundations of Group Polarization.

PhD in progress (2017-) Marco Romanelli. Co-supervised by Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Moreno Falaschi (University of Siena, Italy). Thesis subject: Application of Information Flow to feature selection in machine learning.

PhD in progress (2017-) Anna Pazii. Co-supervised by Konstantinos Chatzikokolakis and Catuscia Palamidessi. Thesis subject: Local Differential Privacy.

PhD terminated (2016-18) Tymofii Prokopenko. Ecole Polytechnique and ENS Cachan. Grant Digiteo-Digicosme. Co-supervised by Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Serge Haddad (ENS Cachan). The PhD was terminated due to the lack of progress.

PhD in progress (2017-) Sergio Ramirez. Co-supervised by Frank Valencia and Camilo Rueda, Universidad Javeriana Cali. Thesis subject: Quantitive Spatial Constraint Systems.

8.2.3. Juries

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

Vittoria Nardone (University of Sannio, Italy). PhD thesis reviewer. Title of the thesis: *Formal Methods for Android Applications*. Supervised by Antonella Santone. Defended in January 2019.

Antoine Dallon (ENS Paris-Saclay). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Verification of indistinguishability properties in cryptographic protocols - Small attacks and efficient decision with SAT-Equiv*. Supervised by Veronique Cortier and Stephanie Delaune. Defended on November 26, 2018.

David Mestel (University of Oxford). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Quantifying information flow*. Supervised by Bill Roscoe. Defended on October 26, 2018.

Jun Wang (University of Luxembourg). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Privacy-preserving recommender systems facilitated by machine learning approach*. Supervised by Qiang Tang and Peter Ryan. Defended on October 19, 2018.

Hamid Ebadi (Chalmers University, Sweden). Member of the committee board at the PhD defense. Title of the thesis: *Dynamic Enforcement of Differential Privacy*. Supervised by David Sands. Defended on March 5, 2018.

Catuscia Palamidessi has been examiner of the following habilitation thesis:

Elham Kashefi (LIP6, CNRS, France). Title of the thesis: *Verification of Quantum Computing*. Defended on February 8, 2018.

8.2.4. Other didactical duties

Catuscia Palamidessi has been:

Member of the advising committee for Hamid Ebadi, PhD student supervised by David Sands, Chalmers University, Sweden. From 2014 until 2018.

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

Member of the advising committee for the PhD of Jun Wang (PhD student supervised by Qiang Tang and Peter Ryan), University of Luxembourg. From 2014 until 2018.

8.3. Popularization

8.3.1. Education

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. Since 2015.

Catuscia Palamidessi has been:

- Invited speaker at PLMW@POPL 2019, the Programming Logic Mentoring Workshop 2019 (affiliated to POPL 2019). This workshop aims at encouraging graduate students and senior undergraduate students to pursue careers in programming language research, and at educating them on the research career.
- A participant in the round table at the FLOC Women in Logic workshop, a workshop organized to encourage women's presence in the logic community. Oxford, UK, 8 July 2018.

8.3.2. Interventions

Catuscia Palamidessi and Frank Valencia have supervised a group of high school children in stage d'observation. April 2018.

Catuscia Palamidessi has given an invited talk at:

- JNIM 2018. Journées Nationales 2018 du GDR Informatique Mathématique (Journée du 6 Avril en Hommage à Maurice Nivat). Palaiseau, France, 3-6 April 2018.

9. 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^{o} 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. 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

[4] S. 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

[5] E. M. ANDRÉS, E. 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

[6] A. ARISTIZÁBAL, F. BONCHI, C. PALAMIDESSI, L. PINO, F. 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

[7] 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

[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. GUZMÁN, 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

Articles in International Peer-Reviewed Journals

[11] M. S. ALVIM, K. CHATZIKOKOLAKIS, Y. KAWAMOTO, C. PALAMIDESSI. *A Game-Theoretic Approach to Information-Flow Control via Protocol Composition*, in "Entropy", May 2018, vol. 20, n° 5, 382 p. [*DOI :* 10.3390/E20050382], https://hal.archives-ouvertes.fr/hal-01966862

[12] V. CASTIGLIONI, D. GEBLER, S. TINI. *SOS-based Modal Decomposition on Nondeterministic Probabilistic Processes*, in "Logical Methods in Computer Science", August 2018, vol. 14, n° 2 [*DOI :* 10.23638/LMCS-14(2:18)2018], https://hal.inria.fr/hal-01966954

[13] F. GADDUCCI, F. SANTINI, L. F. PINO DUQUE, F. VALENCIA. *Observational and Behavioural Equivalences for Soft Concurrent Constraint Programming*, in "Journal of Logical and Algebraic Methods in Programming", November 2018, vol. 92, pp. 45-63 [*DOI :* 10.1016/J.JLAMP.2017.06.001], https://hal.inria.fr/hal-01675060

[14] M. GUZMÁN, S. PERCHY, C. RUEDA, F. VALENCIA. *Characterizing Right Inverses for Spatial Constraint Systems with Applications to Modal Logic*, in "Theoretical Computer Science", October 2018, vol. 744, n° 56–77, https://hal.inria.fr/hal-01675010

Invited Conferences

[15] M. S. ALVIM, K. CHATZIKOKOLAKIS, C. PALAMIDESSI, A. PAZII. *Metric-based local differential privacy for statistical applications*, in "31st Computer Security Foundations Symposium (CSF 2018)", Oxford, United Kingdom, IEEE Computer Society, July 2018, pp. 262-267, https://hal.archives-ouvertes.fr/hal-01966869

[16] K. CHATZIKOKOLAKIS. *On the Additive Capacity Problem for Quantitative Information Flow*, in "15th International Conference on Quantitative Evaluation of SysTems (QEST 2018)", Beijing, China, Lecture Notes in Computer Science, Springer, September 2018, vol. 11024, pp. 1-19, https://hal.inria.fr/hal-01845330

International Conferences with Proceedings

[17] V. CASTIGLIONI. *Trace and Testing Metrics on Nondeterministic Probabilistic Processes*, in "Proceedings Combined 25th International Workshop on Expressiveness in Concurrency and 15th Workshop on Structural Operational Semantics and 15th Workshop on Structural Operational Semantics, (EXPRESS/SOS) 2018", Beijing, China, September 2018, vol. 276, pp. 19-36 [*DOI :* 10.4204/EPTCS.276.4], https://hal.inria.fr/hal-01966950

[18] V. CASTIGLIONI, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *A Logical Characterization of Differential Privacy via Behavioral Metrics*, in "Formal Aspects of Component Software (FACS 2018)", Pohang, South Korea, K. BAE, P. C. ÖLVECZKY (editors), Springer, October 2018, vol. 11222, pp. 75-96 [*DOI :* 10.1007/978-3-030-02146-7_4], https://hal.archives-ouvertes.fr/hal-01966870

[19] C. PALAMIDESSI, M. ROMANELLI. *Feature selection with Rényi min-entropy*, in "Artificial Neural Networks in Pattern Recognition - 8th IAPR TC3 Workshop (ANNPR 2018)", Siena, Italy, L. PANCIONI, F. SCHWENKER, E. TRENTIN (editors), Springer, September 2018, vol. 11081, pp. 226-239, https://hal.archives-ouvertes.fr/hal-01830177

[20] S. RAMÍREZ, M. ROMERO, C. ROCHA, F. D. VALENCIA. *Real-time Rewriting Logic Semantics for Spatial Concurrent Constraint Programming*, in "Rewriting Logic and Its Applications - 12th International Workshop", Thessaloniki, Greece, V. RUSU (editor), Rewriting Logic and Its Applications, Springer, June 2018, vol. 11152, pp. 226–244, https://hal.archives-ouvertes.fr/hal-01934953

Conferences without Proceedings

[21] M. S. ALVIM, K. CHATZIKOKOLAKIS, Y. KAWAMOTO, C. PALAMIDESSI. *Leakage and Protocol Composition in a Game-Theoretic Perspective*, in "7th International Conference on Principles of Security and Trust (POST 2018)", Thessaloniki, Greece, L. BAUER, R. KÜSTERS (editors), Springer, April 2018, vol. 10804, pp. 134-159, https://hal.archives-ouvertes.fr/hal-01966871

[22] L. KACEM, C. PALAMIDESSI. *Geometric Noise for Locally Private Counting Queries*, in "Proceedings of the 13th Workshop on Programming Languages and Analysis for Security (PLAS 2018)", Toronto, Canada, ACM, 2018, pp. 13-16 [*DOI :* 10.1145/3264820.3264827], https://hal.archives-ouvertes.fr/hal-01966872

Scientific Books (or Scientific Book chapters)

[23] M. S. ALVIM, K. CHATZIKOKOLAKIS, A. MCIVER, C. MORGAN, C. PALAMIDESSI, G. SMITH. *The Science of Quantitative Information Flow*, Springer, 2019, https://hal.inria.fr/hal-01971490

[24] M. LEUCKER, J. A. PÉREZ, C. RUEDA, F. D. VALENCIA. *Special Issue: Best Papers Presented at ICTAC 2015*, Mathematical Structures in Computer Science, Cambridge University Press, May 2018, https://hal.archives-ouvertes.fr/hal-01837891

References in notes

[25] 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

[26] S. 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