IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2017

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:

A2.1.1. - Semantics of programming languages
A2.1.5. - Constraint programming
A2.1.6. - Concurrent programming
A2.1.8. - 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
B9.4.1. - Computer science
B9.8. - Privacy

1. Personnel

Research Scientists

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

Post-Doctoral Fellow

Ali Kassem [Inria, from Jun 2017]

PhD Students

Michell Guzman [Inria]
Anna Pazii [Ecole polytechnique, from Oct 2017]
Tymofii Prokopenko [Inria]
Marco Romanelli [Inria, from Oct 2017]

Interns

Hector Delgado Rios [Ecole polytechnique, from May 2017 until Jul 2017]
Georgi Dikov [Ecole polytechnique, from Aug 2017 until Nov 2017]
Anna Pazii [Inria, Jan 2017]
Joaquin Rodriguez Felici [Inria, from Sep 2017]
Marco Romanelli [Inria, from Jun 2017 until Sep 2017]

Administrative Assistants

Jessica Gameiro [Inria]
Hélèna Kutniak [Inria]

Visiting Scientists

Giovanni Cherubin [Royal Holloway University of London, UK, Nov 2017]
Mario Ferreira Alvim Junior [Federal University of Minas Gerais, Brazil, Dec 2017]
David Frutos Escrig [Universidad Complutense Madrid, Spain, until Feb 2017]
Yusuke Kawamoto [AIST, Japan, Nov 2017]
Santiago Quintero [Universidad Javeriana de Cali, Colombia, from Nov to Dec 2017]

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: Michell Guzman, 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, Ali Kassem, Anna Pazii, Tymofii Prokopenko.

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. 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.

In 2017 there was a major update to the Firefox version of Location Guard, to make it compatible with the Firefox Quantum. This latest Firefox version discontinued support for the legacy addon API, so Location Guard had to be adapted to the new WebExtensions API.

Moreover, the latest version implements new features requested by users, such as the ability to search for a fixed location, as well as bugfixes.

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

5.2. 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 2017 with several new added features. The project's git repository shows for this year 33 commits by 2 contributors. The new functionality was directly applied to the exeperimental results of several publications of the team (PETS'17, GameSec'17, VALUETOOLS'17).

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

5.3. 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. Information Leakage Games

In [19] we studied a game-theoretic setting to model the interplay between attacker and defender in the context of information flow, and to reason about their optimal strategies. In contrast with standard game theory, in our games the utility of a mixed strategy is a convex function of the distribution on the defender's pure actions, rather than the expected value of their utilities. Nevertheless, the important properties of game theory, notably the existence of a Nash equilibrium, still hold for our (zero-sum) leakage games, and we provided algorithms to compute the corresponding optimal strategies. As typical in (simultaneous) game theory, the optimal strategy is usually mixed, i.e., probabilistic, for both the attacker and the defender. From the point of view of information flow, this was to be expected in the case of the defender, since it is well known that randomization at the level of the system design may help to reduce information leaks. Regarding the attacker, however, this seems the first work (w.r.t. the literature in information flow) proving formally that in certain cases the optimal attack strategy is necessarily probabilistic.

6.1.2. Efficient Utility Improvement 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 [24], 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 [12], we studied methods for substantially improving the utility of location obfuscation, while maintaining practical applicability as a main goal. 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 with respect to the standard planar Laplace approach.

6.1.3. Trading Optimality for Performance in Location Privacy

Location-Based Services (LBSs) provide invaluable aid in the everyday activities of many individuals, however they also pose serious threats to the user' privacy. There is, therefore, a growing interest in the development of mechanisms to protect location privacy during the use of LBSs. Nowadays, the most popular methods are probabilistic, and the so-called optimal method achieves an optimal trade-off between privacy and utility by using linear optimization techniques.

Unfortunately, due to the complexity of linear programming, the method is unfeasible for a large number N of locations, because the constraints are $O(N^3)$. In [20], we have proposed a technique to reduce the number of constraints to $O(N^2)$, at the price of renouncing to perfect optimality. We have showed however that on practical situations the utility loss is quite acceptable, while the gain in performance is significant.

6.1.4. Methods for Location Privacy: A comparative overview

The growing popularity of location-based services, allowing to collect huge amounts of information regarding users' location, has started raising serious privacy concerns. In [13] we analyzed the various kinds of privacy breaches that may arise in connection with the use of location-based services, and we surveyd and compared the metrics and the mechanisms that have been proposed in the literature.

6.1.5. 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.

6.1.6. Differential Inference Testing: A Practical Approach to Evaluate Anonymized Data

In order to protect individuals' privacy, governments and institutions impose some obligations on data sharing and publishing. Mainly, they require the data to be "anonymized". In this paper, we have shortly discussed the criteria introduced by European General Data Protection Regulation to assess anonymized data. We have argued that the evaluation of anonymized data should be based on whether the data allows individual based inferences, instead of being centered around the concept of re-identification as the regulation has proposed.

Then, we have proposed an inference-based framework that can be used to evaluate the robustness of a given anonymized dataset against a specific inference model, e.g. a machine learning model.

Our approach evaluates the anonymized data itself, and deals with the related anonymization technique as a black-box. Thus, it can be used to assess datasets that are anonymized by organizations which may prefer not to provide access to their techniques. Finally, we have used our framework to evaluate two datasets after being anonymized using k-anonymity and l-diversity.

6.1.7. Formal Analysis and Offline Monitoring of Electronic Exams

More and more universities are moving toward electronic exams (in short e-exams). This migration exposes exams to additional threats, which may come from the use of the information and communication technology. In [17], we have identified and defined several security properties for e-exam systems. Then, we have showed how to use these properties in two complementary approaches: model-checking and monitoring.

We have illustrated the validity of our definitions by analyzing a real e-exam used at the pharmacy faculty of University Grenoble Alpes (UGA) to assess students. On the one hand, we have instantiated our properties as queries for ProVerif, a process calculus based automatic verifier for cryptographic protocols,

and we have used it to check our modeling of UGA exam specifications. ProVerif found some attacks. On the other hand, we have expressed our properties as Quantified Event Automata (QEAs), and we have synthesized them into monitors using MarQ, a Java tool designed to implement QEAs. Then, we have used these monitors to verify real exam executions conducted by UGA. Our monitors found fraudulent students and discrepancies between the specifications of UGA exam and its implementation.

6.1.8. 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 [18] 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.

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. Declarative Framework for Semantical Interpretations of Structured Information — An Applicative Approach.

Spatial constraint systems are algebraic structures from concurrent constraint programming to specify spatial and epistemic behavior in multi-agent system. In [21], [15] we studied the applicability of declarative models to encode and describe structured information by means of semantics. Specifically, we introduced D-SPACES, an implementation of constraint systems with space and extrusion operators. D-SPACES provides property-checking methods as well as an implementation of a specific type of constraint systems (a spatial boolean algebra). We showed the applicability of this framework with two examples; a scenario in the form of a social network where users post their beliefs and utter their opinions, and a semantical interpretation of a logical language to express time behaviors and properties.

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

In [23] spatial constraint systems were 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 was identified and the abstract notion of normality is shown to correspond to the preservation of finite suprema. Furthermore, a taxonomy of normal right inverses was 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 citegadducci:hal-01675060 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.

6.2.4. On the Expressiveness of Spatial Constraint Systems

The dissertation [11] focused on the expressiveness of spatial constraint systems in the broader perspective of modal and epistemic behaviour. It was shown that that spatial constraint systems are sufficiently robust to capture inverse modalities and to derive new results for modal logics. It was shown that one can use scs's to express a fundamental epistemic behaviour such as knowledge. The dissertation also provided an algebraic characterization of the notion of distributed information by means of constructors over scs's.

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 - 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.

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 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.

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: 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.

7.3.2. Inria International Partners

7.3.2.1. Informal International Partners

Giovanni Cherubin, Royal Holloway, University of London, UK

Geoffrey Smith, Florida International University, USA

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 de Cali, Colombia

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

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

7.3.3. Participation in Other International Programs

7.3.3.1. 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. 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..

7.3.3.2. EPIC

Program: STIC-Amsud.

Project acronym: EPIC.

Project title: EPistemic Interactive Concurrency/

Duration: Oct 2016 - Oct 2019.

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. 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.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

David de Frutos Escrig. Professor, Universidad Complutense Madrid, Spain. Jan-Feb 2017

Giovanni Cherubin, PhD student, Royal Holloway, University of London, UK. May 2017 and Oct 2017

Yusuke Kawamoto, Assistant Professor, National Institute of Advanced Industrial Science and Technology (AIST), Japan. July 2017 and Nov 2017

Carlos Olarte, Assistant Professor, Universidade Federal do Rio Grande do Norte, Brazil. July 2017

Camilo Rocha, Associate Professor, Universidad Javeriana de Cali, Colombia. Oct 2017

Camilo Rueda, Professor, Universidad Javeriana de Cali, Colombia. Nov 2017

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil. Dec 2017

7.4.2. Internships

Anna Pazii. Univ. of Kiev, Ukraine. From July 2016 until Jan 2017.

Hector Delgado, Universidad Javeriana de Cali, Colombia. From May 2017 until July 2017.

Marco Romanelli. Univ. of Siena, Italy. From June 2017 until Sept 2017.

Georgi Dikov. Tech. Univ. of Munich, Germany. From Sept 2017 until Nov 2017.

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

Santiago Quintero, Universidad Javeriana de Cali, Colombia. From Nov until Dec 2017.

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

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

The IFIP Working Group 1.8 – Concurrency Theory.

Frank D. Valencia is member of:

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

8.1.2. Scientific events selection

8.1.2.1. Member of conference program committees

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

PETS 2019. The 19th Privacy Enhancing Technologies Symposium. July 2019.

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.

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.

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

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

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

RADICAL-2017. International Workshop Recent Advances in Concurrency and Logic - RADICAL

CP-ICLP-SAT-DP-17. Doctoral Program of the 23rd International Conference on Principles and Practice of Constraint Programming

8.1.2.2. Reviewing

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

8.1.3. Journals

8.1.3.1. Member of the editorial board

Catuscia Palamidessi is:

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

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.

8.1.3.2. Reviewing

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

8.1.4. 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.

8.1.5. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

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

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

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

8.1.6. Invited talks

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

FACS 2017. The 14th International Conference on Formal Aspects of Component Software. Barga, Portugal. 10-13 Oct, 2017.

Cybersecurity 2017. Focus Day on Cyber Security and Helthcare. In the context of the European Cyber Week. Rennes, France, 30 November 2017.

QuaSy 2017. Quantitative Systems: Theory and Applications. Como, Italy, 16-17 October 2017.

Women in Logic 2017, Reykjavik, Island, June 2017.

CrossFyre 2017 Workshop on Cryptography, Robustness, and Provably Secure Schemes. Paris. April 2017.

FORSE 2017 (Keynote speaker). 1st International Workshop on FORmal methods for Security Engineering. Porto, Portugal. 19–21 February, 2017.

8.1.7. 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.

Frank Valencia has served as:

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

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, 2017.

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, 2017.

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 and 2017-18. Total for each semester: 24 hours plus 6 hours for the exam and the exercise session is preparation to the exam.

8.2.2. Supervision

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

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

PhD terminated (2015-17) Joris Lamare. Ecole Polytechnique. Grant MSR Center. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis. Joris has stopped his PhD due to personal reasons.

PhD completed (2014-17) Michel Guzman. Titile: On the Expressiveness of Spatial Constraint Systems [11]. Ecole Polytechnique. Grant Inria CORDI-S. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

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:

Nicolas Bonifas (Ecole Polytechnique, France). Member of the committee board at the PhD defense. Title of the thesis: *Geometric and Dual Approaches to Cumulative Scheduling*. Supervised by Philippe Baptiste. Defended in December 2017.

Maggie Mhanna (CentraleSupelec, France). Member of the committee board at the PhD defense. Supervised by Pablo Piantanida. Defended in January 2017.

8.2.4. Other didactical duties

Catuscia Palamidessi is:

Member of the advising committee for Hamid Ebadi, PhD student supervised by David Sands, Chalmers University, Sweden, since 2014. Also reviewer and member of the committee for the half-way thesis defense (Licentiate) that took place in June 2015.

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. 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. Since 2015.

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] 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] 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

[6] 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

[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^{o} 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

Doctoral Dissertations and Habilitation Theses

[11] M. GUZMÁN. *On the Expressiveness of Spatial Constraint Systems*, École Polytechnique X, September 2017, https://hal.inria.fr/tel-01674956

Articles in International Peer-Reviewed Journals

[12] K. CHATZIKOKOLAKIS, E. ELSALAMOUNY, C. PALAMIDESSI. *Efficient Utility Improvement for Location Privacy*, in "Proceedings on Privacy Enhancing Technologies", 2017, vol. 2017, n^{o} 4, pp. 308-328 [*DOI :* 10.1515/POPETS-2017-0051], https://hal.inria.fr/hal-01422842

[13] K. CHATZIKOKOLAKIS, E. ELSALAMOUNY, C. PALAMIDESSI, A. PAZII. *Methods for Location Privacy: A comparative overview*, in "Foundations and Trends® in Privacy and Security ", 2017, vol. 1, n^{o} 4, pp. 199-257, Submitted for publication, https://hal.inria.fr/hal-01421457

[14] 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

[15] S. HAAR, S. PERCHY, F. VALENCIA. *Declarative Framework for Semantical Interpretations of Structured Information — An Applicative Approach*, in "International Journal of Semantic Computing", December 2017, vol. 11, n° 04, pp. 451 - 472 [*DOI :* 10.1142/S1793351X17400189], https://hal.inria.fr/hal-01673529

[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, vol. 88, pp. 27-52, To appear, https://hal.inria.fr/hal-01421417

[17] A. KASSEM, Y. FALCONE, P. LAFOURCADE. *Formal analysis and offline monitoring of electronic exams*, in "Formal Methods in System Design", August 2017, vol. 51, n° 1, pp. 117 - 153 [*DOI :* 10.1007/s10703-017-0280-0], https://hal.inria.fr/hal-01653884

[18] Y. KAWAMOTO, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *On the Compositionality of Quantitative Information Flow*, in "Logical Methods in Computer Science", August 2017, vol. 13, n° 3, pp. 1-31, https://arxiv.org/abs/1611.00455 - Submitted for publication to Logical Methods in Computer Science, https://hal.inria.fr/hal-01421424

International Conferences with Proceedings

[19] M. S. ALVIM, K. CHATZIKOKOLAKIS, Y. KAWAMOTO, C. PALAMIDESSI. *Information Leakage Games*, in "Decision and Game Theory for Security - 8th International Conference", Vienna, Austria, S. RASS, B. AN, C. KIEKINTVELD, F. FANG, S. SCHAUER (editors), Lecture Notes in Computer Science, Springer, October 2017, vol. 10575, pp. 437-457 [*DOI :* 10.1007/978-3-319-68711-7_23], https://hal.inria.fr/hal-01678950

[20] K. CHATZIKOKOLAKIS, S. HADDAD, A. KASSEM, C. PALAMIDESSI. *Trading Optimality for Performance in Location Privacy*, in "11th EAI International Conference on Performance Evaluation Methodologies and Tools", Venice, Italy, December 2017, forthcoming, https://hal.inria.fr/hal-01678256

[21] 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

Research Reports

[22] A. KASSEM, G. ACS, C. CASTELLUCCIA. *Differential Inference Testing A Practical Approach to Evaluate Anonymized Data*, Inria, January 2018, https://hal.inria.fr/hal-01681014

Other Publications

[23] M. GUZMÁN, S. PERCHY, C. RUEDA, F. VALENCIA. *Characterizing Right Inverses for Spatial Constraint Systems with Applications to Modal Logic* , January 2018, Submitted to Theoretical Computer Science (TCS), https://hal.inria.fr/hal-01675010

References in notes

[24] 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