IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2019

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
A2.1.9. - 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
A8.6. - Information theory
A9.1. - Knowledge
A9.2. - Machine learning
A9.7. - AI algorithmics
A9.9. - Distributed AI, Multi-agent

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]

Post-Doctoral Fellow

Valentina Castiglioni [Inria, Post-Doctoral Fellow, until Apr 2019]

PhD Students

Ganesh Del Grosso Guzman [Inria, PhD Student, from Oct 2019]
Natasha Fernandes [Macquarie Univ., PhD Student]
Federica Granese [Inria, PhD Student, from Nov 2019]
Anna Pazii [École polytechnique, PhD Student]
Santiago Quintero [École polytechnique, PhD Student]
Marco Romanelli [Inria, PhD Student]

Technical staff

Ehab Elsalamouny [Inria, Engineer]

Interns and Apprentices

Sayan Biswas [Inria, from Jun 2019 until Sep 2019]
Noemie Fong [ENS Paris, until Feb 2019]
Federica Granese [Inria, from Mar 2019 until Jun 2019]
Boammani Lompo [Inria, from May 2019 until Jul 2019]

Administrative Assistant

Maria Agustina Ronco [Inria, Administrative Assistant]

Visiting Scientists

Yusuke Kawamoto [AIST, March 2019 and Nov–Dec 2019]
Sophia Knight [University of Minesota, May 2019]
Takao Murakami [AIST, March 2019]
Carlos Olarte [Universidade Federal do Rio Grande do Norte, Brazil, Nov 2019]
Carlos Pinzon [Universidad Javeriana of Cali, Nov 2019]
Sergio Ramirez [Universidad Javeriana of Cali, from Nov 2019 until Dec 2019]
Camilo Rocha [Universidad Javeriana of Cali, Jun 2019]
Camilo Rueda [Universidad Javeriana of Cali, from May 2019 until Jun 2019]

External Collaborators

Sayan Biswas [University of Bath, from Oct 2019]
Konstantinos Chatzikokolakis [CNRS]
Noemie Fong [ENS Paris, from Apr 2019 until Aug 2019]
Federica Granese [Univ. of Rome "La Sapienza", from Jul 2019 until Oct 2019]
Juan Pablo Piantanida [Centrale-Supélec, from Oct 2019]

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. Highlights of the Year

5.1. Highlights of the Year

Catuscia Palamidessi has received an European Research Council (ERC) grant for the project HYPATIA.

6. New Software and Platforms

6.1. 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

6.2. 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

6.3. 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

6.4. 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:

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

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

7. New Results

7.1. Foundations of privacy and quantitative information flow

Privacy and information flow have the common goal of trying to protect sensitive information. Comete focuses in particular on the potential leaks due to inference from data that are public, or anyway available to the adversary. We consider the probabilistic aspects, and we use concepts and tools from information theory.

7.1.1. Black-box Leakage Estimation

In [16] we have considered the problem of measuring how much a system reveals about its secret inputs under the black-box setting. Black-box means that we assume no prior knowledge of the system's internals: the idea is to run the system for choices of secrets and measure its leakage from the respective outputs. Our goal was to estimate the Bayes risk, from which one can derive some of the most popular leakage measures (e.g., min-entropy, additive, and multiplicative leakage). The state-of-the-art method for estimating these leakage measures is the frequentist paradigm, which approximates the system's internals by looking at the frequencies of its inputs and outputs. Unfortunately, this does not scale for systems with large output spaces, where it would require too many input-output examples. Consequently, it also cannot be applied to systems with continuous outputs (e.g., time side channels, network traffic). In [16] we have exploited an analogy between Machine Learning (ML) and black-box leakage estimation to show that the Bayes risk of a system can be estimated by using a class of ML methods: the universally consistent learning rules; these rules can exploit patterns in the input-output examples to improve the estimates' convergence, while retaining formal optimality guarantees. We have focused on a set of them, the nearest neighbor rules; we show that they significantly reduce the number of black-box queries required for a precise estimation whenever nearby outputs tend to be produced by the same secret; furthermore, some of them can tackle systems with continuous outputs. We have illustrated the applicability of these techniques on both synthetic and real-world data, and we compared them with the state-of-the-art tool, leakiEst, which is based on the frequentist approach.

7.1.2. An Axiomatization of Information Flow Measures

Quantitative information flow aims to assess and control the leakage of sensitive information by computer systems. A key insight in this area is that no single leakage measure is appropriate in all operational scenarios; as a result, many leakage measures have been proposed, with many different properties. To clarify this complex situation, in [11] we have studied information leakage axiomatically, showing important dependencies among different axioms. We have also established a completeness result about the g-leakage family, showing that any leakage measure satisfying certain intuitively-reasonable properties can be expressed as a g-leakage.

7.1.3. Comparing systems: max-case refinement orders and application to differential privacy

Quantitative Information Flow (QIF) and Differential Privacy (DP) are both concerned with the protection of sensitive information, but they are rather different approaches. In particular, QIF considers the expected probability of a successful attack, while DP (in both its standard and local versions) is a max-case measure, in the sense that it is compromised by the existence of a possible attack, regardless of its probability. Comparing systems is a fundamental task in these areas: one wishes to guarantee that replacing a system A by a system B is a safe operation, that is the privacy of B is no-worse than that of A. In QIF, a refinement order provides strong such guarantees, while in DP mechanisms are typically compared (wrt privacy) based on the ε privacy parameter that they provide.

In [15] we have explored a variety of refinement orders, inspired by the one of QIF, providing precise guarantees for max-case leakage. We have studied simple structural ways of characterizing them, the relation between them, efficient methods for verifying them and their lattice properties. Moreover, we have applied these orders in the task of comparing DP mechanisms, raising the question of whether the order based on ε provides strong privacy guarantees. We have shown that, while it is often the case for mechanisms of the same "family" (geometric, randomised response, etc.), it rarely holds across different families.

7.1.4. A Logical Characterization of Differential Privacy

Differential privacy (DP) is a formal definition of privacy ensuring that sensitive information relative to individuals cannot be inferred by querying a database. In [12], we have exploited a modeling of this framework via labeled Markov Chains (LMCs) to provide a logical characterization of differential privacy: we have considered a probabilistic variant of the Hennessy-Milner logic and we have defined a syntactical distance on formulae in it measuring their syntactic disparities. Then, we have defined a trace distance on LMCs in terms of the syntactic distance between the sets of formulae satisfied by them. We have proved that such distance corresponds to the level of privacy of the LMCs. Moreover, we have used the distance on formulae to define a real-valued semantics for them, from which we have 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 have focused on bisimulation semantics on nondeterministic probabilistic processes and we have provided 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 have shown that the generalized bisimulation distance on processes is equal to the syntactic distance on their mimicking formulae. Moreover, we have used the distance on mimicking formulae to obtain bounds on differential privacy.

7.1.5. Geo-indistinguishability vs Utility in Mobility-based Geographic Datasets

In [17] we have explored the trade-offs between privacy and utility in mobility-based geographic datasets. Our aim was to find out whether it is possible to protect the privacy of the users in a dataset while, at the same time, maintaining intact the utility of the information that it contains. In particular, we have focused on geo-indistinguishability as a privacy-preserving sanitization methodology, and we have evaluated its effects on the utility of the Geolife dataset. We have tested the sanitized dataset in two real world scenarios: 1. Deploying an infrastructure of WiFi hotspots to offload the mobile traffic of users living, working, or commuting in a wide geographic area; 2. Simulating the spreading of a gossip-based epidemic as the outcome of a device-to-device communication protocol. We have shown the extent to which the current geo-indistinguishability techniques trade privacy for utility in real world applications and we focus on their effects at the levels of the population as a whole and of single individuals.

7.1.6. Utility-Preserving Privacy Mechanisms for Counting Queries

Differential privacy(DP) and local differential privacy(LPD) are frameworks to protect sensitive information in data collections. They are both based on obfuscation. In DP the noise is added to the result of queries on the dataset, whereas in LPD the noise is added directly on the individual records, before being collected. The main advantage of LPD with respect to DP is that it does not need to assume a trusted third party. 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 sanitized data it is necessary to have a huge collection of them. In [25], we focus on the problem of estimating counting queries from collections of noisy answers, and we propose a variant of LDP based on the addition of geometric noise. Our main result is that the geometric noise has a better statistical utility than other LPD mechanisms from the literature.

7.1.7. Differential Inference Testing: A Practical Approach to Evaluate Sanitizations of Datasets

In order to protect individuals' privacy, data have to be "well-sanitized" before sharing them, i.e. one has to remove any personal information before sharing data. However, it is not always clear when data shall be deemed well-sanitized. In this paper, we argue that the evaluation of sanitized data should be based on whether the data allows the inference of sensitive information that is specific to an individual, instead of being centered around the concept of re-identification. In [20] we have proposed a framework to evaluate the effectiveness of different sanitization techniques on a given dataset by measuring how much an individual's record from the sanitized dataset influences the inference of his/her own sensitive attribute. Our intent was not to accurately predict any sensitive attribute but rather to measure the impact of a single record on the inference of sensitive

information. We have demonstrated our approach by sanitizing two real datasets in different privacy models and evaluate/compare each sanitized dataset in our framework.

7.2. Foundations of Process Calculi

7.2.1. Group Distributed Knowledge.

We introduced spatial constraint systems (scs) as semantic structures for reasoning about spatial and epistemic information in concurrent systems. They have been used to reason about beliefs, lies, and group epistemic behaviour inspired by social networks. They have also been used for proving new results about modal logics and giving semantics to process calculi. In [19] we developed the theory of scs to reason about the distributed information of potentially infinite groups. We characterized the notion of distributed information of a group of agents as the infimum of the set of join-preserving functions that represent the spaces of the agents in the group. We provided an alternative characterization of this notion as the greatest family of join-preserving functions that satisfy certain basic properties. We showed compositionality results for these characterizations and conditions under which information that can be obtained by an infinite group can also be obtained by a finite group. Finally, we provided algorithms that compute the distributive group information of finite groups. Furthermore, in [14] we summarized all the main results we have obtained about scs.

7.2.2. Group Polarization.

Social networks can make their users become more radical and isolated in their own ideological circle causing dangerous splits in society in a phenomenon known as group polarization. In [22] we developed a preliminary model for social networks, and a measure of the level of polarization in these social networks, based on Esteban and Ray's classic measure of polarization for economic situations. Our model includes information about each agent's quantitative strength of belief in a proposition of interest and a representation of the strength of each agent's influence on every other agent. We considered how the model changes over time as agents interact and communicate, and included several different options for belief update, including rational belief update and update taking into account irrational responses such as confirmation bias and the backfire effect. Under various scenarios, we considered the evolution of polarization over time, and the implications of these results for real world social networks.

7.2.3. Lattice Theory.

Structures involving a lattice and join-endomorphisms on it are ubiquitous in computer science. In [28] we studied the cardinality of the set $J(L)$ of all join-endomorphisms of a given finite lattice L. We showed that the cardinality of $J(L)$ is sub-exponential, exponential and super-exponential in the size of the lattice for boolean algebras, linear-orders, and arbitrary lattices, respectively. We also studied the following problem: Given a lattice L of size n and a subset S of $J(L)$ of size m, find the greatest lower bound in $J(L)$ of S. This join-endomorphism has meaningful interpretations in epistemic logic, distributed systems, and Aumann structures. We showed that this problem can be solved with worst-case time complexity in $O(n + mlogn)$ for powerset lattices, $O(mn^2)$ for lattices of sets, and $O(mn + n^3)$ for arbitrary lattices. The complexity is expressed in terms of the basic binary lattice operations performed by the algorithm.

7.2.4. Festschrift Contribution.

In a Festschrift dedicated to Catuscia Palamidessi [26], we presented an article with original solutions to four challenging mathematical puzzles [23]. The first two are concerned with random processes. The first problem can be reduced to computing, for arbitrary large values of n, the expected number of iterations of a program that increases a variable at random between 1 and n until exceeds n. The second problem can be reduced to determining the probability of reaching a given point after visiting all the others in a circular random walk. The other two problems involve finding optimal winning group strategies in guessing games.

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. LOST2DNN

Program: DATAIA Call for Research Projects

Project title: Leakage of Sensitive Training Data from Deep Neural Networks

Duration: October 2019 - September 2022

Coordinators: Catuscia Palamidessi, Inria Saclay, EPI Comète and Pablo Piantanida, Centrale Supèlec

Other PI's and partner institutions: Georg Pichler, TU Wien, Austria

Abstract: The overall project goal is to develop a fundamental understanding with experimental validation of the information-leakage of training data from deep learning systems. More specifically, we aim at:

- Developing a compelling case study based on state-of-the-art algorithms to perform model inversion attacks, showcasing the feasibility of uncovering specified sensitive information from a trained software (model) on real data.
- Quantifying information leakage. Based on the uncovered attacks, the amount of sensitive information present in trained software will be measured or quantified. The resulting measure of leakage will serve as a basis for the analysis of attacks and for the development of robust mitigation techniques.
- Mitigating information leakage. Strategies will be explored to avoid the uncovered attacks and minimize the potential information leakage of a trained model.

8.2. National Initiatives

8.2.1. 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

8.3. European Initiatives: FP7 & H2020 Projects

8.3.1. HYPATIA

Program: European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme.

Project acronym: HYPATIA

Project title: Privacy and Utility Allied

Duration: October 2019 – September 2024

Principal Investigator: Catuscia Palamidessi

Abstract: With the ever-increasing use of internet-connected devices, such as computers, smart grids, IoT appliances and GPS-enabled equipments, personal data are collected in larger and larger amounts, and then stored and manipulated for the most diverse purposes. Undeniably, the big-data technology provides enormous benefits to industry, individuals and society, ranging from improving business strategies and boosting quality of service to enhancing scientific progress. On the other hand, however, the collection and manipulation of personal data raises alarming privacy issues. Not only the experts, but also the population at large are becoming increasingly aware of the risks, due to the repeated cases of violations and leaks that keep hitting the headlines.

The objective of this project is to develop the theoretical foundations, methods and tools to protect the privacy of the individuals while letting their data to be collected and used for statistical purposes. We aim in particular at developing mechanisms that can be applied and controlled directly by the user thus avoiding the need of a trusted party, are robust with respect to combination of information from different sources, and provide an optimal trade-off between privacy and utility.

8.4. International Initiatives

8.4.1. Inria Associate Teams Not Involved in an Inria International Labs

8.4.1.1. 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 2019 - December 2021.

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.

8.4.2. Inria 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

8.4.3. Participation in Other International Programs

8.4.3.1. 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 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..

8.4.3.2. 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.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Yusuke Kawamoto, Researcher, AIST, Japan, AIST, March 2019 and Nov-Dec 2019

Takao Murakami, Researcher, AIST, Japan, AIST, March 2019

Sophia Knight, Assistant Professor, University of Minnesota, USA, May 2019

Carlos Olarte, Assistant Professor, Universidade Federal do Rio Grande do Norte, Brazil. Nov 2019

Camilo Rueda, Professor, Universidad Javeriana de Cali, Colombia. May-July 2019

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil. Nov 2019

Sergio Ramirez, PhD student, Universidad Javeriana de Cali, Colombia. Oct-Dec 2019

Carlos Pinzon, Master student, Universidad Javeriana de Cali, Colombia. Nov 2019

8.5.2. Internships

Sayan Biswas, Master student, Univ. of Bath, UK. From Jun 2019 until Sep 2019

Noemie Fong, Master student, ENS Paris. Jan-Feb 2019

Federica Granese, Univ. Od Rome "La Sapienza", Italy. From Mar 2019 until Jun 2019

Boammani Lompo, ENS Rennes. From May 2019 until Jul 2019

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committee

Catuscia Palamidessi is member of:

The Scientific Advisory Board of ANSSI, the French National Cybersecurity Agency. Since 2019.

The Scientific Advisory Board of CISPA, the Helmholtz Center for Information Security. Since 2019.

The Executive Committee of SIGLOG, the ACM Special Interest Group on Logic and Computation. 2014-19.

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

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.

9.1.2. Scientific events selection committee

9.1.2.1. Chair of conference program committee

Konstantinos Chatzikokolakis:

is serving as PC chair (with Carmela Troncoso as co-chair) of PETS 2020: The 20th Privacy Enhancing Technologies Symposium, July 14 – 18, 2020 Montréal, Canada.

9.1.2.2. Member of conference program committees

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

CCS 2020. The ACM Conference on Computer and Communications Security. Orlando, USA, November 9-13 2020.

CSF 2020. The 33rd IEEE Computer Security Foundations Symposium. Boston, MA, USA, June 22-26, 2020.

PETS 2020. The 20th Privacy Enhancing Technologies Symposium. Montréal, Canada, July 14 – 18, 2020.

FORTE 2020. The 40th IFIP International Conference on Formal Techniques for Distributed Objects, Components, and Systems. University of Malta, Valletta, June 15-19, 2020.

FSTTCS 2019. 39th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science. Indian Institute of Technology Bombay, December 11–13, 2019

FACS 2019. The 16th International Conference on Formal Aspects of Component Software. Amsterdam, The Netherlands, 23-25 October 2019.

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

TML 2020. Towards Trustworthy ML: Rethinking Security and Privacy for ML. Addis Ababa, Ethiopia, April 26, 2020.

EXPRESS/SOS 2020. Combined 27th International Workshop on Expressiveness in Concurrency and 17th Workshop on Structural Operational Semantics. Vienna, Austria, August 31, 2020.

PPAI 2020. The rAAI Workshop on Privacy-Preserving Artificial Intelligence. New York, USA, February 7, 2020.

PPML 2019. Privacy Preserving Machine Learning (ACM CCS 2019 Workshop). London, UK, November 15, 2019.

WPES 2019. Workshop on Privacy in the Electronic Society. London, UK, November 11, 2019.

APVP 2019. Atelier sur la Protection de la Vie Privée. Cap Hornu, France, July 9-11, 2019.

WIL 2019. 3rd Women in Logic Workshop. Cap Hornu, France, Vancouver, Canada, June 23, 2019.

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

CP-DP-19: Doctoral Program of the 25th International Conference on Principles and Practice of Constraint Programming. Stamford, CT, USA, Sep 30 - Oct 4, 2019.

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

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

9.1.3. Journals

9.1.3.1. Member of the editorial board

Catuscia Palamidessi is:

(2019-) Member of the Editorial Board of the Journal of Computer Security IOS Press. Since 2019.

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.

9.1.3.2. Reviewing

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

9.1.4. 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.

9.1.5. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

External Member of the committee for the promotion to full professor of Prof. Kévin Huguenin. HEC Lausanne, Switzerland.

Member of the committee for associate professor positions in the Datalogi Dept., Aalborg Univ., Denmark. 2019.

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 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.

Member of the EAPLS PhD Award Committee. From 2010.

9.1.6. Invited talks

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

Journées Nationales du GDR Sécurité Informatique. Paris, France, June 2019.

MFPS XXXV, special session on Probabilistic Programming. London, UK, June 2019.

AI & Society: From principles to practice. CIFAR-UKRI-CNRS workshop. London, UK, June 2019.

5th France-Japan Cybersecurity workshop}. Kyoto, Japan, April 2019.

Frank Valencia has given the following invited talk:

- EXPRESS/SOS 2019. Combined 26th International Workshop on Expressiveness in Concurrency and 16th Workshop on Structural Operational Semantics. Amsterdam, Netherlands, August 26, 2019.

9.1.7. Service

Catuscia Palamidessi has served as:

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

Member of the Commission Scientifique du Centre de Recherche Inria Saclay. From 2018.

Member of the hiring committee for Maitre de Conference, Ecole Polytechnique, 2019.

Frank Valencia has served as:

Directeur adjoint de l'UMR 7161, le Laboratoire d'Informatique de l'Ecole Polytechnique (LIX). May 2016 - Nov 2019.

9.2. Teaching - Supervision - Juries

9.2.1. 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, 2019.

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, 2019

Master : Catuscia Palamidessi has been teaching the masters course on "Foundations of Privacy", 24 hours, at the MPRI, Sept-Nov 2019.

9.2.2. Supervision

PhD in progress (2019-) Federica Granese. Co-supervised Catuscia Palamidessi and Daniele Gorla. Thesis subject: Security in Machine Learning.

PhD in progress (2019-) Ganesh Del Grosso. Co-supervised by Catuscia Palamidessi and Pablo Piantanida. Thesis Subject: Privacy in Machine Learning.

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

9.2.3. Juries

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

Mohamed Maouche (INSA, Lyon). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Protection against Re-identification Attacks in Location Privacy*. Defended in November 2019.

Raphaëlle Crubrillé (IRIF, Université Paris Diderot). Member of the committee board at the PhD defense. Title of the thesis: *Distances comportementales pour les programmes probabilistes d'ordre supérieur*. Defended in June 2019.

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.

9.2.4. Other didactical duties

Catuscia Palamidessi has been:

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

9.3. Popularization

9.3.1. 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 on fairness, Interpretability, and Privacy in AI at the CIFAR-UKRI-CNRS workshop. London, June 2019.

Frank Valencia has:

- Welcomed the students of bachelor program of École Polytechnique to Inria center. Sept 12, 2019.
- Welcomed visitors from ACOFI, the Colombian Association of Faculties of Engineering to Inria center. April 8, 2019.

9.3.2. Interventions

Catuscia Palamidessi has given an invited talk at:

- Safety and AI. DATAIA Workshop. Palaiseau, France, September 2019.

10. 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. *An Axiomatization of Information Flow Measures*, in "Theoretical Computer Science", 2019, vol. 777, pp. 32-54 [*DOI :* 10.1016/J.TCS.2018.10.016], https://hal.archives-ouvertes.fr/hal-01995712

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

[7] G. CHERUBIN, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *F-BLEAU: Fast Black-Box Leakage Estimation*, in "Proceedings of the 40th IEEE Symposium on Security and Privacy (SP)", San Francisco, United States, IEEE, May 2019, pp. 835-852 [*DOI :* 10.1109/SP.2019.00073], https://hal.archives-ouvertes.fr/hal-02422945

[8] M. GUZMÁN, S. KNIGHT, S. QUINTERO, S. RAMÍREZ, C. RUEDA, F. D. VALENCIA. *Reasoning about Distributed Knowledge of Groups with Infinitely Many Agents*, in "CONCUR 2019 - 30th International Conference on Concurrency Theory", Amsterdam, Netherlands, W. FOKKINK, R. VAN GLABBEEK (editors), August 2019, vol. 140, pp. 29:1–29:15 [*DOI :* 10.4230/LIPICS.CONCUR.2019.29], https://hal.archives-ouvertes.fr/hal-02172415

[9] M. GUZMÁN, S. HAAR, S. PERCHY, C. RUEDA, F. D. 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, C. MORGAN, C. PALAMIDESSI, G. SMITH, A. MCIVER. *An Axiomatization of Information Flow Measures*, in "Theoretical Computer Science", 2019, vol. 777, pp. 32-54 [*DOI :* 10.1016/J.TCS.2018.10.016], https://hal.archives-ouvertes.fr/hal-01995712

[12] V. CASTIGLIONI, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *A Logical Characterization of Differential Privacy*, in "Science of Computer Programming", 2019, forthcoming, https://hal.archives-ouvertes.fr/hal-02423048

[13] M. FALASCHI, M. GABBRIELLI, C. OLARTE, C. PALAMIDESSI. *Dynamic slicing for Concurrent Constraint Languages*, in "Fundamenta Informaticae", 2019, forthcoming, https://hal.archives-ouvertes.fr/hal-02423973

[14] F. D. VALENCIA. *Semantic Structures for Spatially-Distributed Multi-Agent Systems*, in "Electronic Proceedings in Theoretical Computer Science", August 2019, vol. 300, pp. 39-53 [*DOI :* 10.4204/EPTCS.300.3], https://hal.archives-ouvertes.fr/hal-02410770

International Conferences with Proceedings

[15] K. CHATZIKOKOLAKIS, N. FERNANDES, C. PALAMIDESSI. *Comparing systems: max-case refinement orders and application to differential privacy*, in "Proceedings of the 32nd IEEE Computer Security Foundations Symposium", Hoboken, United States, 2019, pp. 442–457 [*DOI :* 10.1109/CSF.2019.00037], https://hal.archives-ouvertes.fr/hal-02126848

[16] G. CHERUBIN, K. CHATZIKOKOLAKIS, C. PALAMIDESSI. *F-BLEAU: Fast Black-Box Leakage Estimation*, in "Proceedings of the 40th IEEE Symposium on Security and Privacy (SP)", San Francisco, United States, IEEE, May 2019, pp. 835-852 [*DOI :* 10.1109/SP.2019.00073], https://hal.archives-ouvertes.fr/hal-02422945

[17] A. DI LUZIO, A. C. VIANA, K. CHATZIKOKOLAKIS, G. DIKOV, C. PALAMIDESSI, J. STEFA. *Catch Me If You Can: How Geo-indistinguishability Affects Utility in Mobility-based Geographic Datasets*, in "Proceedings of the 3rd ACM SIGSPATIAL International Workshop", Chicago, United States, ACM Press, 2019, pp. 1-10 [*DOI :* 10.1145/3356994.3365498], https://hal.archives-ouvertes.fr/hal-02423337

[18] D. GORLA, F. GRANESE, C. PALAMIDESSI. *Enhanced Models for Privacy and Utility in Continuous-Time Diffusion Networks*, in "Proceedings of the 16th International Colloquium on Theoretical Aspects of Computing (ICTAC)", Hammamet, Tunisia, R. M. HIERONS, M. MOSBAH (editors), Lecture Notes in Computer Science, Springer, October 2019, vol. 11884, pp. 313-331 [*DOI :* 10.1007/978-3-030-32505-3_18], https://hal.inria.fr/hal-02424329

[19] M. GUZMÁN, S. KNIGHT, S. QUINTERO, S. RAMÍREZ, C. RUEDA, F. D. VALENCIA. *Reasoning about Distributed Knowledge of Groups with Infinitely Many Agents*, in "CONCUR 2019 - 30th International Conference on Concurrency Theory", Amsterdam, Netherlands, W. FOKKINK, R. VAN GLABBEEK (editors), August 2019, vol. 29, pp. 1-29 [*DOI :* 10.4230/LIPIcs.CONCUR.2019.29], https://hal.archives-ouvertes.fr/hal-02172415

[20] A. KASSEM, G. ACS, C. CASTELLUCCIA, C. PALAMIDESSI. *Differential Inference Testing: A Practical Approach to Evaluate Sanitizations of Datasets*, in "Proceedings of the 2019 IEEE Security and Privacy Workshops (SPW)", San Francisco, United States, IEEE, May 2019, pp. 72-79 [*DOI :* 10.1109/SPW.2019.00024], https://hal.archives-ouvertes.fr/hal-02422992

Scientific Books (or Scientific Book chapters)

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

[22] M. S. ALVIM, S. KNIGHT, F. D. VALENCIA. *Toward a Formal Model for Group Polarization in Social Networks*, in "The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy - Essays Dedicated to Catuscia Palamidessi on the Occasion of Her 60th Birthday", M. S. ALVIM, K. CHATZIKOKOLAKIS, C. OLARTE, F. D. VALENCIA (editors), Lecture Notes in Computer Science, Springer, November 2019, vol. 11760, pp. 419-441 [*DOI :* 10.1007/978-3-030-31175-9_24], https://hal.archives-ouvertes.fr/hal-02410747

[23] N. ARISTIZABAL, C. PINZÓN, C. RUEDA, F. D. VALENCIA. *Make Puzzles Great Again*, in "The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy - Essays Dedicated to Catuscia Palamidessi on the Occasion of Her 60th Birthday", M. S. ALVIM, K. CHATZIKOKOLAKIS, C. OLARTE, F. D. VALENCIA (editors), Lecture Notes in Computer Science, Springer, November 2019, vol. 11760, pp. 442-459 [*DOI :* 10.1007/978-3-030-31175-9_25], https://hal.archives-ouvertes.fr/hal-02410767

[24] K. CHATZIKOKOLAKIS, G. SMITH. *Refinement Metrics for Quantitative Information Flow*, in "The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy. Essays Dedicated to Catuscia Palamidessi on the Occasion of Her 60th Birthday", M. S. ALVIM, K. CHATZIKOKOLAKIS, C. OLARTE, F. D. VALENCIA (editors), Lecture Notes in Computer Science, Springer, November 2019, vol. 11760, pp. 397-416 [*DOI :* 10.1007/978-3-030-31175-9_23], https://hal.inria.fr/hal-02350777

[25] N. FERNANDES, K. LEFKI, C. PALAMIDESSI. *Utility-Preserving Privacy Mechanisms for Counting Queries*, in "Models, Languages and Tools for Concurrent and Distributed Programming", M. BOREALE, F. COR-

RADINI, M. LORETI, R. PUGLIESE (editors), Lecture Notes in Computer Science, Springer, July 2019, vol. 11665, pp. 487-495, https://arxiv.org/abs/1906.12147 , https://hal.archives-ouvertes.fr/hal-02169218

Books or Proceedings Editing

[26] M. S. ALVIM, K. CHATZIKOKOLAKIS, C. OLARTE, F. D. VALENCIA (editors). *The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy - Essays Dedicated to Catuscia Palamidessi on the Occasion of Her 60th Birthday*, Lecture Notes in Computer Science, Springer, November 2019, vol. 11760 [*DOI :* 10.1007/978-3-030-31175-9], https://hal.archives-ouvertes.fr/hal-02411252

[27] A. DAWAR, A. MUSCHOLL, C. PALAMIDESSI (editors). *Selected Papers of the 44th International Colloquium on Automata, Languages and Programming (ICALP 2017)*, Logical Methods in Computer Science Association, 2019, forthcoming, https://hal.inria.fr/hal-01997414

Research Reports

[28] S. QUINTERO, S. RAMÍREZ, C. RUEDA, F. D. VALENCIA. *Counting and Computing Join-Endomorphisms in Lattices*, LIX, Ecole polytechnique ; Inria Saclay - Ile-de-France, December 2019, Conditionally Accepted at RAMICS 2020, https://hal.archives-ouvertes.fr/hal-02422624