RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2019

Section Contracts and Grants with Industry

Edition: 2020-03-21

Algorithmics, Computer Algebra and Cryptology

Architecture, Languages and Compilation

Embedded and Real-time Systems

Proofs and Verification

SECURITY AND CONFIDENTIALITY

ARIC Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Bosch (Germany) ordered from us some support for implementing complex numerical algorithms (participants: Claude-Pierre Jeannerod and Jean-Michel Muller).

8.2. Bilateral Grants with Industry

- Miruna Rosca and Radu Titiu are employees of BitDefender. Their PhD's are supervised by Damien Stehlé and Benoît Libert, respectively. Miruna Rosca works on the foundations of lattice-based cryptography, and Radu Titiu works on pseudo-random functions and functional encryption.
- Adel Hamdi is doing is PhD with Orange Labs and is supervised by Fabien Laguillaumie. He is working on advanced encryption protocols for the cloud.

AROMATH Project-Team

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Contracts with Industry

- **NURBSFIX: Repairing the topology of a NURBS model in view of its approximation.** We have a research contract with the industrial partner GeometryFactory, in collaboration with the project-team Titane (Pierre Alliez). The post-doc of Xiao Xiao is funded by this research contract together with a PEPS from the labex AMIES.

Because of their flexibility and accuracy, NURBS (Non-Uniform Rational Basis Spline) models have become a standard in the modeling community for generating and representing complex shapes. They are made of several surface patches and a collection of curves that are used for trimming. As a direct consequence of software quirks, designer errors, and representation flaws, these NURBS models have inconsistencies that introduce small gaps and overlaps between surface patches. They are mainly located on the singularity graph of a NURBS model, near the trimming curves, especially near singularities such as sharp edges or corners. Building a correct approximation of a NURBS model in the presence of inconsistencies is a challenging problem. Most of the current approaches are based on the repairing of the geometry of the surface patches. This requires an interactive process which is difficult to control and rarely completely successful. In this project, we develop another approach which consists in repairing the topology of the singularity graph within a tolerance volume. This tolerance volume will be considered as a protected region that will not receive any query of geometric computations. Based on that, three types of approximations will be treated: triangular isotropic surface meshing of NURBS models, volume approximation of multi-domains delimited by NURBS surfaces, and NURBS models approximation within a given tolerance volume.

CARAMBA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- Together with the PESTO team, we had a contract with the Docapost company, the purpose of which is to improve their e-voting solution by adding some verifiability properties and switching to elliptic curve cryptography.
- Together with the PESTO team, we have a contract with the Idemia company about e-voting.

8.2. Bilateral Grants with Industry

- A contract with Orange Gardens at Chatillon-Montrouge is dedicated to the supervision of Sandra Rasoamiaramanana's PhD thesis about security in the white box context. The co-supervisor for Orange Gardens is Gilles Macario-rat.
- A contract with Thales (Thales Communication & Security, Gennevilliers, subsidiary of Thales Group) is dedicated to the supervision of Simon Masson's PhD thesis about elliptic curves for bilinear and post-quantum cryptography. The co-supervisor for Thales is Olivier Bernard.

CASCADE Project-Team (section vide)

DATASHAPE Project-Team

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Contracts with Industry

- Collaboration with Sysnav, a French SME with world leading expertise in navigation and geopositioning in extreme environments, on TDA, geometric approaches and machine learning for the analysis of movements of pedestrians and patients equipped with inetial sensors (CIFRE PhD of Bertrand Beaufils).
- Research collaboration with Fujitsu on the development of new TDA methods and tools for Machine learning and Artificial Intelligence (started in Dec 2017).
- Research collaboration with MetaFora on the development of new TDA-based and statistical methods for the analysis of cytometric data (started in Nov. 2019).

6.2. Bilateral Grants with Industry

- DATASHAPE and Sysnav have been selected for the ANR/DGA Challenge MALIN (funding: 700 kEuros) on pedestrian motion reconstruction in severe environments (without GPS access).

GAMBLE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- Company: WATERLOO MAPLE INC
  Duration: 2 years
  Participants: GAMBLE and OURAGAN Inria teams
  Abstract: A two-years licence and cooperation agreement was signed on April 1st, 2018 between WATERLOO MAPLE INC., Ontario, Canada (represented by Laurent Bernardin, its Executive Vice President Products and Solutions) and Inria. On the Inria side, this contract involves the teams GAMBLE and OURAGAN (Paris), and it is coordinated by Fabrice Rouillier (OURAGAN).

  F. Rouillier and GAMBLE are the developers of the ISOTOP software for the computation of topology of curves. One objective of the contract is to transfer a version of ISOTOP to WATERLOO MAPLE INC.
- Company: GEOMETRYFACTORY
  Duration: permanent
  Participants: Inria and GEOMETRYFACTORY
  Abstract: CGAL packages developed in GAMBLE are commercialized by GEOMETRYFACTORY.

GRACE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Participants: Daniel Augot, Alain Couvreur, Guénaël Renault, François Morain.

- Through École polytechnique, Daniel Augot is leader of a teaching and research chair on Blockchains for business, funded by CapGemini.
- IRT System-X funds a PhD student for Secure Multiparty Computation in blockchains
- Ernst & Young funds a contract for providing PhD guidance to one of its employee, on the topic of blockchains
- Idemia funds a CIFRE PhD student on the secure implementation in constrained environement of post-quantum cryptosystems.
- Quarkslab funds a CIFRE PhD student on the analysis of malware code
- French Min. Arm. funds a PhD student on the analysis of the ToR network
- Grant with Nokia with the Privacy “Action de recherche”.

LFANT Project-Team (section vide)

OURAGAN Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- The objective of our Agrement with WATERLOO MAPLE INC. is to promote software developments to which we actively contribute.

  On the one hand, WMI provides man power, software licenses, technical support (development, documentation and testing) for an inclusion of our developments in their commercial products. On the other hand, OURAGAN offers perpetual licenses for the use of the concerned source code.

  As past results of this agreement one can cite our C-Library *RS* for the computations of the real solutions zero-dimensional systems or also our collaborative development around the Maple package *DV* for solving parametric systems of equations.

  For this term, the agreement covers algorithms developed in areas including but not limited to: 1) solving of systems of polynomial equations, 2) validated numerical polynomial root finding, 3) computational geometry, 4) curves and surfaces topology, 5) parametric algebraic systems, 6) cylindrical algebraic decompositions, 7) robotics applications.

  In particular, it covers our collaborative work with some of our partners, especially the Gamble Project-Team - Inria Nancy Grand Est.

- In 2019, a contract was signed with the company *Safran Tech*. Its goal is to bring our scientific expertise on mathematical and algorithmic aspects on certain problems studied in gearbox vibration analysis. Gear fault diagnosis is an important issue in aeronautics industry since a damage in a gearbox, which is not detected in time, can have dramatic effects on the safety of a plane. Since the vibrations of a spur gear can be modeled as a product of two periodic functions related to the gearbox kinematic, [92] has proposed to recover each function from the global signal by means of an optimal reconstruction problem which, by means of Fourier analysis, yields a Frobenius norm minimization problem for structured matrices. The goal of the collaboration is to use symbolic-numeric to study this problem.

POLSYS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Technological Transfer

The group have had a continuous commitment into industrial transfer as well as a strong involvement into standardization bodies.

Industrial transfer. This activity is related to our long-standing activity in post-quantum cryptography. The transfer started at the beginning of the current evaluation period and culminated this year with the creation of a new spin-off, called CRYPTONEXT SECURITY[0], from Inria Paris and Sorbonne Université. The goal of CRYPTONEXT SECURITY is to propose security products that are resistant against the quantum computers. Its business model is based on B2B and targeted customers are Fortune 500 companies.

The activity has been partially founded and supervised by SATT-LUTECH who is specialized in the processing and transfer of technologies from research laboratories of its shareholders: Inria, CNRS, University of Technology of Compiègne, National Museum of Natural History, Institute Curie, University Panthéon-Assas, Paris Sorbonne University and National School of Industrial Creation). Typically, SATT-LUTECH has funded the post-quantum experiment described in the dedicated Section. The impact of such experiment can be partially measured by the press released covering out the test [0] (La Recherche, l'Usine Nouvelle, L'Informaticien).

As a preliminary step for launching the spin-off, two members of the team (J.-C. Faugère and L. Perret) followed two entrepreneurship programs for creating innovative companies : HEC Challenge plus [0] (1 week of courses by month, 9 months) and Deep Tech Founders [0] (3 months, 2 sessions by weeks). This was a necessary, but significant effort, before launching CRYPTONEXT in which the two members will work full-time from now on.

Post-quantum standardization. Besides the NIST PQC standardization process, we are involved in the on-going world effort for standardizing post-quantum cryptography. More precisely, the European Telecommunications Standards Institute (ETSI) has a strong standardization activity on post-quantum cryptography. ETSI is a EU standardization body with a worldwide scope. We are an active member of ETSI regarding post-quantum cryptography. In particular, we are the rapporteur of a technical document on post-quantum cryptosystems. The goal of our involvement is to bring our scientific expertise to define trustworthy post-quantum public-key standards; that are going to be the basis of our digital economy within $10/15$ years.

We are also involved in the Cloud Security Alliance (CSA). This is a large non-profit organization (80.000 member worldwide) whose main goal is to promote the best practices with the secure usage of cloud computing. CSA has a group dedicated to quantum-safe security. The group is ideation catalyzer for promoting the transition of companies to a quantum-safe security. In particular, the group has a significant educational activity in order to increase awareness regarding the quantum risk and the techniques to mitigate this risk. We are co-chairing this group and participated to several white papers. The group is probably now the main channel for promoting quantum-safe security. Standardization is a long-term effort.

[0] https://cryptonext-security.com/

[0] https://www-polsys.lip6.fr/Links/index.html

[0] http://entrepreneurship-center.hec.edu/learn-program/hec-challenge-plus/

[0] https://deeptechfounders.com/

SECRET Project-Team (section vide)

SPECFUN Project-Team (section vide)

CAIRN Project-Team (section vide)

CAMUS Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Caldera

Participants: Cédric Bastoul, Vincent Loechner.

Duration : 2016 - 2019

Caldera (www.caldera.com) is a company specialized in software development for wide image processing. The goal of this collaboration is the development of a parallel and scalable image processing pipeline for industrial printing. The project started in September 2016 and it includes the industrial thesis (CIFRE) of Paul Godard, defended in Dec. 2019.

CASH Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

CIFRE Ph.D of Julien Emmanuel with Bull/Atos, hosted by Inria. 2020-2023.

CORSE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Atos/Bull

- Title: Static and dynamic approaches for the optimization of the energy consumption associated with applications of the High Performance Computing (HPC) field
- CORSE participants: François Broquedis, Frédéric Desprez, Mathieu Stoffel
- Partner: Atos/Bull
- Duration: February 2018 - February 2021
- Abstract: The purpose of this project is to dynamically improve the energy consumption of HPC applications on large-scale platforms. It relies on an adaptation of the CPU frequency at runtime, based on the analysis of hardware-related metrics to determine an *application profile*. This profile is then split into different *phases*, each of which being associated to a best CPU frequency, depending on its nature (CPU bound, memory bound, ...). This project is funding the PhD of Mathieu Stoffel, and the corresponding development is to be integrated into *Bull Dynamic Power Optimizer*, a software suite developed by Atos/Bull.

7.2. Bilateral Grants with Industry

7.2.1. ES3CAP

- Title: Embedded Smart Safe Secure Computing Autonomous Platform
- CORSE participants: Fabrice Rastello, Nicolas Tolenaere
- Duration: July 2018 - August 2021
- INRIA Partners: AOSTE, PARKAS, CHROMA
- Other Partners: Renault-Nissan, EasyMile, Safran E&D, MBDA, ANSYS/ESterel Technologies, Kronno-Safe, Prove & Run, Kalray, Prophesee, CEA
- Abstract: The objective of ES3CAP is to develop a tool-chain that targets multi- and many-core architectures for critical systems. In particular it should address the different challenges related to making existing critical systems solutions (heterogeneous, decentralized, single-core, single-task) match the industrial constraints targeted by Kalray's MPPA (MPPA, high-performance, real-time, safety, security). Considered applications are autonmous driving, drones, avionics, and defense. CORSE is involved in the optimization of machine learning algorithms for many-core architectures.

PACAP Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. Intel research grant INTEL2016-11174

Participants: Niloofar Charmchi, Kleovoulos Kalaitzidis, Anis Peysieux, André Seznec.

Intel is supporting the research of the PACAP project-team on “Design tradeoffs for extreme cores”.

HYCOMES Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Glose: Globalisation for Systems Engineering

Participants: Benoît Caillaud, Benoît Vernay.

Glose is a bilateral collaboration between Inria and Safran Tech., the corporate research entity of Safran Group. It started late 2017 for a duration of 44 months. Three Inria teams are involved in this collaboration: Diverse (Inria Rennes), Hycomes and Kairos (Inria Sophia-Antipolis). The scope of the collaboration is systems engineering and co-simulation.

The simulation of system-level models requires synchronizing, at simulation-time, physical models with software models. These models are developed and maintained by different stakeholders: physics engineers, control engineers and software engineers. Models designed by physics engineers are either detailed 3D finite-elements models, with partial differential equations (PDEs), or finite-dimension 0D models (obtained by model reduction techniques, or by empirical knowledge) expressed in modeling languages such as Simulink (with ordinary differential equations, or ODEs), Modelica (with differential algebraic equations, or DAEs), or directly as a C code embedding both the differential equations and its discretization scheme. Coupling together heterogeneous models and programs, so that they can be co-simulated, is not only a technological challenge, but more importantly raises several deep and difficult questions: Can we trust simulations? What about their reproducibility? Will it be possible to simulate large systems with hundreds to thousands of component models?

Co-simulation requires that models are provided with interfaces, specifying static and dynamic properties about the model and its expected environments. Interfaces are required to define how each model may synchronize and communicate, and how the model should be used. For instance, an interface should define (i) which variables are inputs, which are outputs, (ii) their data types, physical units, and sampling periods, but also (iii) the environmental assumptions under which the model is valid, and (iv) the causal dependencies between input and output variables and for continuous-time models, (v) the stiffness of the model, often expressed as a time-varying Jacobian matrix.

Formally, an interface is an abstraction of a model's behavior. A typical example of interface formalism for 0D continuous-time models is the FMI standard. Co-simulation also requires that a model of the system architecture is provided. This architectural model specifies how components are interconnected, how they communicate and how computations are scheduled. This is not limited to the topology of the architecture, and should also specify how components interact. For instance, variables in continuous-time models may have different data-types and physical units. Conversion may be required when continuous-time models are plugged together. Another fine example is the coupling of a 3D finite-element model to a 0D model: effort and flow fields computed in the 3D model must be averaged in a scalar value, before it can be sent to the 0D model, and conversely, scalar values computed by the 0D model must be distributed as a (vector) field along a boundary manifold of the 3D model. For discrete-time models (eg., software), components may communicate in many ways (shared variables, message passing, ...), and computations can be time- or event-triggered. All these features are captured as data-/behavior-coordination patterns, as exemplified by the GEMOC initiative [0].

In the Glose project, we propose to formalize the behavioral semantics of several modeling languages used at system-level. These semantics will be used to extract behavioral language interfaces supporting the definition of coordination patterns. These patterns, in turn, can systematically be used to drive the coordination of any model conforming to these languages. The co-simulation of a system-level architecture consists in an orchestration of hundreds to thousands of components. This orchestration is achieved by a master algorithm, in charge of triggering the communication and computation steps of each component. It takes into account the

[0] http://gemoc.org

components' interfaces, and the data-/behavior-coordination patterns found in the system architecture model. Because simulation scalability is a major issue, the scheduling policy computed by the master algorithm should be optimal. Parallel or distributed simulations may even be required. This implies that the master algorithm should be hierarchical and possibly distributed.

In 2019, the Hycomes team has been working on the use of Quantized State System (QSS) nethods for the cosimulation of aeronautics system models. The aim is to design new distributed simulation protocols, capable of simulating large, but heterogeneous system models. The investigation is on the trade-offs between pessimistic simulation techniques, where no roll-back is required, and speculative methods, where roll-back may be required. The latter method can be beneficial to the performance and scalability of the simulation, provided roll-backs do not happen too often. The models under consideration are cyberphysical systems consisting in both Modelica models (for the physics) and discrete-time models expressed in a dedicated language (for the control).

In 2019, the Hycones team has delivered one report, detailing the state-of-the-art techniques for continuous systems cosimulation.

Kairos Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Safran : Desir/Glose We participate to the bilateral collaborative program Desir, put up by Safran to work with selected academic partners. We share the Glose project started in this program with two other Inria teams : HyComes, and DiverSE. The aim of the project is to improve early stages of system engineering by allowing early execution and co-simulation of heterogeneous models. The technical content of our contributions is described in section 7.13 . A CIFRE PhD is funded by Renault on related topics.

IRT Saint-Exupery ATIPPIC This cooperative project aims at building a computing digital electronic structure of micro-satellites on ordinary, "COTS" processors. The project was accepted for 30 months and will reach completion by the end of 2019. It funds two temporary research engineers working under our own supervision, while exchanging extensively with the rest of the ATIPPIC project, which is actually physically hosted by Inria. The technical content of our contributions is described in section 7.2 .

Airbus In the continuation of the ITEA3 ASSUME project, Airbus has provided funding for the extension of the Real-Time Systems Compilation method to allow parallelization onto multi-cores with classical ARM or POWER architecture. The technical content of our contributions is described in section 7.16 . The technical content of our contributions is described in section 7.2 .

IRT Saint-Exupery The CAPHCA project of IRT Saint-Exupéry has provided funding for the extension of the Real-Time Systems compilation method to allow parallelization onto timing predictable multi-cores different from the Kalray MPPA 256. The targets of this work are Infineon TC27x and FlexPRET.

Renault Software Lab We have started, at the end of 2018, a collaboration with Renault Software Labs on the definition of rules for ensuring safe maneuvers in autonomous vehicles. The rules express conditions from the environments, safety rules to preserve the integrity of the vehicles, driving legislation rules, local rules from the authorities. The rules must be updated dynamically when the vehicle evolves and are used to monitor at run-time the behavior of the ADAS. While the ADAS contains several algorithms relying on machine learning, the monitoring system must be predictive and rules must guarantee formally that the system does not cause any accident. So it can be seen as a way to build trustworthy monitoring of learning algorithms. A CIFRE PhD is funded by Renault on this topic and has started in April 2019.

Accenture Labs We have continued discussions with Accenture Labs, started in 2018, on Smart Contract languages for permissioned blockchains. A CIFRE funding is under way.

In recent years, various platform developments focused on so-called *private* (or *permissioned*) blockchain(s) and digital ledgers. Almost all private blockchains present their own implementation of Smart Contract. Between public and private blockchains we are observing a wide variety of different languages with different capabilities and limitations. Inspired by our researches in object-oriented languages [40], we aim at designing a language which might extend an object instance upon receiving a message, an ability referred to by Cardelli as *self-inflicted* operation. Public and private blockchains would take advantage of this novel capability in building safe and flexible intelligent smart contracts.

KOPERNIC Team (section vide)

PARKAS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Collaboration with Airbus

Our work on multi-clock Lustre programs is funded by a contract with Airbus.

7.2. Bilateral Grants with Industry

7.2.1. Google Research Fellowship: DWARF unwinding

Francesco Zappa Nardelli benefits from a Google Research Fellowship to pursue the work on DWARF unwinding, about 50k euros.

SPADES Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- Inria and Orange Labs have established in 2015 a joint virtual research laboratory, called I/O LAB. We have been heavily involved in the creation of the laboratory and are actively involved in its operation (Jean-Bernard Stefani is one of the two co-directors of the lab). I/O LAB focuses on the network virtualization and cloudification. As part of the work of I/O LAB, we have cooperated with Orange Lab, as part of a cooperative research contract funded by Orange, on defining architectural principles and frameworks for network cloud infrastructures encompassing control and management of computing, storage and network resources.

7.2. Bilateral Grants with Industry

With Orange:

- Fault Management in Multi-Tenant Programmable Networks. This CIFRE grant funds the PhD of Sihem Cherrared.
- Dynamic dataflow models of computation. This CIFRE grant funds the PhD of Arash Shafiei.

TEA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Inria – Mitsubishi Electric framework program (2018+)

Title: Inria – Mitsubishi Electric framework program

Inria principal investigator: Jean-Pierre Talpin

International Partner: Mitsubishi Electric R&D Europe (MERCE)

Duration: 2018+

Abstract: Following up the fruitful collaboration of TEA with the formal methods group at MERCE, Inria and Mitsubishi Electric signed a center-wide collaboration agreement, which currently hosts projects with project-teams Sumo and Tea, as well as Tocata.

8.1.2. Mitsubishi Electric R&D Europe (2019-2022)

Title: A logical framework to verify requirements of hybrid system models

Inria principal investigator: Jean-Pierre Talpin, Stéphane Kastenbaum

International Partner: Mitsubishi Electric R&D Europe

Duration: 2015 - 2018

Abstract: The goal of this doctoral project is to verify and build cyber-physical systems (CPSs) with a correct-by-construction approach in order to validate system requirements against the two facets of the cyber and physical aspects of such designs. Our approach is based on components augmented with formal contracts that can be composed, abstracted or refined. It fosters the proof of system-level requirements by composing individual properties proved at component level. While semantically grounded, the tooling of this methodology should be usable by regular engineers (i.e. not proof theory specialists).

8.1.3. Mitsubishi Electric R&D Europe (2015-2019)

Title: Parallelism and modular proof in differential dynamic logic [1]

Inria principal investigator: Jean-Pierre Talpin, Simon Lunel

International Partner: Mitsubishi Electric R&D Europe

Duration: 2015 - 2018

Abstract: The primary goal of this Ph.D. project is to ensure correctness-by-design in cyber-physical systems, i.e., systems that mix software and hardware in a physical environment, e.g., Mitsubishi factory automation lines. We develop a component-based approach in Differential Dynamic Logic allowing to reason about a wide variety of heterogeneous cyber-physical systems. Our work provides tools and methodology to design and prove a system modularly.

ANTIQUE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Follow up to the AnaStaSec project

Title: Analyse de propriété de sécurité

Type: Research contracts funded by AirBus France

Duration: March 2019 - August 2018 and November 2019 - March 2020

Inria contact: Jérôme Feret

Abstract: An emerging structure in our information processing-based society is the notion of trusted complex systems interacting via heterogeneous networks with an open, mostly untrusted world. This view characterises a wide variety of systems ranging from the information system of a company to the connected components of a private house, all of which have to be connected with the outside.

The goal of these constracts is to analyse an application that is used to filter messages from higher-level security regions to lower-level ones in trusted complex systems. This application shall check that messages are well-formed and that they match with existing requests. Moreover, so as to limit potential flows of information, one shall prove that the internal state of buffers are reset between the processing of each packet.

To certify these properties, the front-end of ASTRÉE has been upgraded with new directives to specify the properties of interest, and the analysis has been tuned to improve the analysis : 1) ghost variables are used to record the value of buffers between each packet processing so that already existing relational domains can prove that they are restored to the correct value, and 2) data-partitioning strategies have been implemented to separate the different modes of usage.

CAMBIUM Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. The Caml Consortium

Participant: Damien Doligez.

The Caml Consortium, is a formal structure where industrial and academic users of OCaml can support the development of the language and associated tools, express their specific needs, and contribute to the long-term stability of OCaml. Membership fees are used to fund specific developments targeted towards industrial users. Members of the Consortium automatically benefit from very liberal licensing conditions on the OCaml system, allowing for instance the OCaml compiler to be embedded within proprietary applications.

Damien Doligez chairs the Caml Consortium.

The Consortium currently has 9 member companies:

- Aesthetic Integration
- Citrix
- Docker
- Esterel Technologies
- Facebook
- Jane Street
- LexiFi
- Microsoft
- SimCorp

The Caml Consortium is being gradually phased out. In the future, we would like to replace it entirely with the OCaml Software Foundation, discussed below.

7.2. Bilateral Grants with Industry

7.2.1. The OCaml Software Foundation

Participants: Damien Doligez, Xavier Leroy.

The OCaml Software Foundation (OCSF),[0] established in 2018 under the umbrella of the Inria Foundation, aims to promote, protect, and advance the OCaml programming language and its ecosystem, and to support and facilitate the growth of a diverse and international community of OCaml users.

Damien Doligez and Xavier Leroy serve as advisors on the foundation's Executive Committee.

We receive substantial basic funding from the OCaml Software Foundation in order to support research activity related to OCaml.

[0] http://ocaml-sf.org/

7.2.2. Funding from Nomadic Labs

Nomadic Labs, a Paris-based company, has implemented the Tezos blockchain and cryptocurrency entirely in OCaml. This year, Nomadic Labs and Inria have signed a framework agreement ("contrat-cadre") that allows Nomadic Labs to fund multiple research efforts carried out by Inria groups. Within this framework, we have received three 3-year grants:

- "Évolution d'OCaml". This grant is intended to fund a number of improvements to OCaml, including the addition of new features and a possible re-design of the OCaml type-checker. This grant has allowed us to fund Jacques Garrigue's visit (10 months) and to hire Gabriel Radanne on a Starting Research Position (3 years).
- "Maintenance d'OCaml". This grant is intended to fund the day-to-day maintenance of OCaml as well as the considerable work involved in managing the release cycle. This grant has allowed us to hire Florian Angeletti as an engineer for 3 years.
- "Multicore OCaml". This grant is intended to encourage research work on Multicore OCaml within our team. This grant has allowed us to fund Glen Mével's PhD thesis (3 years).

7.2.3. Funding from the Microsoft-Inria joint lab

Funding from the Microsoft-Inria joint lab has allowed us to hire Ioannis Filippidis on a Starting Research Position (until March 2020) to work on the TLAPS system.

CELTIQUE Project-Team (section vide)

CONVECS Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. Orange Labs

Participants: Umar Ozeer, Gwen Salaün.

Umar Ozeer is supported by a PhD grant (from November 2016 to November 2019) from Orange Labs (Grenoble) on detecting and repairing failures of data-centric applications distributed in the cloud and the IoT (see § 7.5.1), under the supervision of Loïc Letondeur (Orange Labs), Gwen Salaün (CONVECS), François Gaël Ottogalli (Orange Labs), and Jean-Marc Vincent (POLARIS project-team).

8.1.2. Nokia Bell Labs

Participants: Radu Mateescu, Ajay Muroor Nadumane, Gwen Salaün.

Ajay Muroor Nadumane is supported by a PhD grant (from October 2017 to October 2020) from Nokia Bell Labs (Nozay) on IoT service composition (see § 7.5.2) supported by formal methods, under the supervision of Gwen Salaün (CONVECS), Radu Mateescu (CONVECS), Ludovic Noirie, and Michel Le Pallec (Nokia Bell Labs).

DEDUCTEAM Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Valentin Blot obtained with Chantal Keller funding for a 4-year project involving a PhD student, a research engineer (2 years) and a post-doctoral researcher (2 years). This funding is part of the Inria - Nomadic labs partnership for Tezos blockchain.

GALLINETTE Project-Team (section vide)

MEXICO Project-Team (section vide)

MOCQUA Team (section vide)

PARSIFAL Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. OCaml Software Foundation

Participant: Gabriel Scherer.

The OCaml Software Foundation (OCSF), [0] established in 2018 under the umbrella of the Inria Foundation, aims to promote, protect, and advance the OCaml programming language and its ecosystem, and to support and facilitate the growth of a diverse and international community of OCaml users.

Gabriel Scherer serves as the director of the foundation.

8.1.2. Funding from Nomadic Labs

Participant: Gabriel Scherer.

Nomadic Labs, a Paris-based company, has implemented the Tezos blockchain and cryptocurrency entirely in OCaml. This year, Nomadic Labs and Inria have signed a framework agreement ("contrat-cadre") that allows Nomadic Labs to fund multiple research efforts carried out by Inria groups. Within this framework, we participate to two 3-year grants, in collaboration with the Cambium team at Inria Paris:

- "Évolution d'OCaml". This grant is intended to fund a number of improvements to OCaml, including the addition of new features and a possible re-design of the OCaml type-checker.
- "Maintenance d'OCaml". This grant is intended to fund the day-to-day maintenance of OCaml as well as the considerable work involved in managing the release cycle.

[0] http://ocaml-sf.org/

PI.R2 Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Theo Zimmermann will start a research engineer position in January 2020 to continue his research and development work about improving the Software Engineering practices of the development of Coq, especially to continue the improvement of the collaborative development processes and of its ecosystem. This position is funded by the Inria-NomadicLabs grant.

STAMP Project-Team (section vide)

SUMO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Nokia Bell Labs - ADR SAPIENS

Several researchers of SUMO are involved in the joint research lab of Nokia Bell Labs France and Inria. We participate in the common research team SAPIENS (Smart Automated and Programmable Infrastructures for End-to-end Networks and Services), previously named “Softwarization of Everything.” This team involves several other Inria teams: Convecs, Diverse and Spades. SUMO focuses on the management of reconfigurable systems, both at the edge (IoT based applications) and in the core (*e.g.* virtualized IMS systems). In particular, we study control and diagnosis issues for such systems.

Two PhD students are involved in the project. Erij Elmajed (3rd year), on the topic of Diagnosis of virtualized and reconfigurable systems supervised by Éric Fabre and Armen Aghasaryan (Nokia Bell Labs). Abdul Majith (started in January 2019) on Controller Synthesis of Adaptive Systems, supervised by Hervé Marchand, Ocan Sankur and Dinh Thai Bui (Nokia Bell Labs).

8.1.2. Orange Labs

SUMO takes part in IOLab, the common lab of Orange Labs and Inria, dedicated to the design and management of Software Defined Networks. Our activities concern the diagnosis of malfunctions in virtualized multi-tenant networks.

This collaboration supports one Cifre PhD student, Sihem Cherrared (2nd year), supervised by Éric Fabre, Gregor Goessler (Inria Spades, Grenoble) and Sofiane Imadali (Orange Labs).

8.1.3. Alstom Transport - P22

Several researchers of SUMO are involved in the joint research lab of Alstom and Inria, in a common research team called P22. On Alstom side, this joint research team involves researchers of the ATS division (Automatic Train Supervision). The objective of this joint team is to evaluate regulation policies of urban train systems, to assess their robustness to perturbations and failures, to design more efficient regulation policies and finally to provide decision support for human regulators. The P22 project between Alstom and Inria ended in 2018. However, our collaboration with Alstom Transport continues. One of the outcomes of this collaboration is the PhD defense of Karim Kecir in July 2019 [2].

8.1.4. Mitsubishi Electric Research Center Europe (MERCE)

Several researchers of SUMO are involved in a collaboration on the verification of real-time systems with the "Information and Network Systems (INS)" Team led by David Mentré of the "Communication & Information Systems (CIS)" Division of MERCE Rennes. The members of the team at MERCE work on different aspects of formal verification. Currently the SUMO team and MERCE jointly supervise a Cifre PhD student (Emily Clément) funded by MERCE since fall 2018; the thesis is about robustness of reachability in timed automata. Moreover Reiya Noguchi, a young engineer, member of MERCE, on leave of a Japanese operational division of Mitsubishi is also hosted and co-supervised by the SUMO team since the beginning of 2019, one day per week; we collaborate with him on the consistency of timed requirements.

TOCCATA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

We have two bilateral contracts which are closely related to a joint effort called the ProofInUse joint Laboratory. The objective of ProofInUse is to provide verification tools, based on mathematical proof, to industry users. These tools are aimed at replacing or complementing the existing test activities, whilst reducing costs.

This joint laboratory is a follow-up of the former "LabCom ProofInUse" between Toccata and the SME AdaCore, funded by the ANR programme "Laboratoires communs", from April 2014 to March 2017 http://www.spark-2014.org/proofinuse.

8.1.1. ProofInUse-AdaCore Collaboration

Participants: Claude Marché [contact], Jean-Christophe Filliâtre, Andrei Paskevich, Guillaume Melquiond, Sylvain Dailler.

This collaboration is a joint effort of the Inria project-team Toccata and the AdaCore company which provides development tools for the Ada programming language. It is funded by a 5-year bilateral contract from Jan 2019 to Dec 2023.

The SME AdaCore is a software publisher specializing in providing software development tools for critical systems. A previous successful collaboration between Toccata and AdaCore enabled Why3 technology to be put into the heart of the AdaCore-developed SPARK technology.

The objective of ProofInUse-AdaCore is to significantly increase the capabilities and performances of the Spark/Ada verification environment proposed by AdaCore. It aims at integration of verification techniques at the state-of-the-art of academic research, via the generic environment Why3 for deductive program verification developed by Toccata.

8.1.2. ProofInUse-MERCE Collaboration

Participants: Claude Marché [contact], Jean-Christophe Filliâtre, Andrei Paskevich, Guillaume Melquiond, Sylvain Dailler.

This bilateral contract is part of the ProofInUse effort. This collaboration joins efforts of the Inria project-team Toccata and the company Mitsubishi Electric R&D (MERCE) in Rennes. It is funded by a bilateral contract of 18 months from Nov 2019 to April 2021.

MERCE has strong and recognized skills in the field of formal methods. In the industrial context of the Mitsubishi Electric Group, MERCE has acquired knowledge of the specific needs of the development processes and meets the needs of the group in different areas of application by providing automatic verification and demonstration tools adapted to the problems encountered.

The objective of ProofInUse-MERCE is to significantly improve on-going MERCE tools regarding the verification of Programmable Logic Controllers and also regarding the verification of numerical C codes.

8.2. Bilateral Grants with Industry

8.2.1. CIFRE contract with TrustInSoft company

Participants: Guillaume Melquiond [contact], Raphaël Rieu-Helft.

Jointly with the thesis of R. Rieu-Helft, supervised in collaboration with the TrustInSoft company, we established a 3-year bilateral collaboration contract, that started in October 2017. The aim is to design methods that make it possible to design an arbitrary-precision integer library that, while competitive with the state-of-the-art library GMP, is formally verified. Not only are GMP's algorithm especially intricate from an arithmetic point of view, but numerous tricks were also used to optimize them. We are using the Why3 programming language to implement the algorithms, we are developing reflection-based procedures to verify them, and we finally extract them as a C library that is binary-compatible with GMP [9] [67] [33].

VERIDIS Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Logic4Business

The Max Planck Institute for Informatics (MPI-INF) and Logic 4 Business GmbH (L4B) have signed a cooperation contract. Its subject is the application of automated reasoning methods to product complexity management, in particular in the car industry. MPI-INF is providing software and know-how, L4B is providing real-world challenges.

CIDRE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **HP (2013-2019): Embedded Systems Security** One of the main activities of HP Inc. is to develop and manufacture computing platforms (such as laptops, printers, etc). These platforms consist of hardware and embedded software (usually referred to as firmware). Such embedded software is typically required for the proper functioning of the hardware and relied upon by high level operating system, application or solution software. One of the research tracks of this collaboration consists in enhancing the security level of low-level software components (firmware and OS) in future computing platforms. The final objective is to provide a more resilient and trustworthy platform to the end-user. This work is carried out in the context of the PhD of Ronny Chevalier.
- **DGA (2018-2020)** Traditionally, IDSes are evaluated based on their detection ability against a labeled dataset that contains normal and abnormal network traffic. Upon inspection, it is clear that datasets publicly available are usually obsolete in the span of a couple years in both anomaly types and background, benign Internet traffic. They also suffer from a lack of volume and diversity in traffic, and ultimately, lack of representativeness and realism. In this context, the goal of this project is to come up with an evolutive platform for IDS evaluation that solves many of the issues that exist in the state of the art methods. In order to create such an evolutive platform, there is a need for dynamic infrastructure that allows continuous and automatic change. Here are a number of design principles that we followed for our platform: reproducibility (it is possible to rebuild the infrastructure of the platform or any element of it); repeatability (any action carried out on the infrastructure tested in the platform is repeatable); live evaluation (while traditional IDS evaluation is carried out using a static benchmark dataset, we propose an environment that resembles what IDS does in real life); realism (in terms of traffic generation, real world attack representativeness, and system setup. This will surely be a continuous and evolutive effort to try to approach real world conditions as best as can be); automatization (scripts allow a complete description of the system in which an IDS is tested, and of normal/malicious activity generation inside this system).

  This work is carried out in the context of the postdoc of Mouad Lemoudden.
- **DGA (2019-2021)** DGA and its industrial partners have to regularly implement filters applied to standard or proprietary protocols on communication interfaces or directly in products. In order to allow administrators to easily adapt these filters to the specific context of the various devices, filtering languages specific to the different filtering policies applicable to the different devices should be developed. Even for simple static filters, the definition of such languages is a complex task. A methodological approach that would simplify this task for higher level abstraction filtering languages (and therefore simpler to use) would be to allow the definition of higher level abstraction filtering languages by relying on a single language of lower level of abstraction. This would make it possible to define high-level abstraction and easy-to-use languages in a recursive way by progressively increasing the levels of abstraction (and specificity). In addition, this approach would improve reusability. Indeed, it would be possible to rely on a filtering language, previously developed for another project, in order to more easily develop a more specific (and easy to use) language for another project.

  This work is carried out in the context of the postdoc of Ludovic Claudepierre

7.2. Bilateral Grants with Industry

- **DGA: Intrusion Detection in Distributed Applications** David Lanoé has started his PhD thesis in October 2016 in the context of a cooperation with DGA-MI. His work is focussing on the construction of behavioral models (during a learning phase) and their use to detect intrusions during an execution of the modelled distributed application.
- **Idemia: Hardware Security for Embeded Devices** Kevin Bukasa has started his PhD in January 2016 in a bilateral contract between Inria and Idemia. He explored fault injection attacks using EM probes on two different kind of devices: microcontroller (representing IoT) and SoC (representing Smart phone). He demonstrated the vulnerability of both architectures on this kind of attack. On IoT device he has developped an attack allowing to take a full control on the device. He discovered also new fault attacks never described in the litterature.
- **Idemia: Protection against fuzzing attack** Leopold Ouairy has started his PhD in October 2017 in a bilateral contract between Inria and Idemia. The context is related with security testing of Java applications to avoid fuzzing attack. The approach is based on AI to design automatically a model use for the oracle. He used machine learning to serach in a corpus of applicatons methods having the same semantics. Then in a second step, after convertir the source code into a vector he compute a similarity value which is related with absence of conditions evaluation.
- **Ministry of Defence: Visualisation for the characterization of security events** Laetitia Leichtnam has started his PhD thesis in November 2016 in the context of a contract between CentraleSupelec and the French Ministry of Defence. His work consists in presenting events appearing in heterogeneous logs as a dependency graph between the lines of logs. This permits to the administrator to investigate easily the logs to discover the different steps that has performed an attack in the supervised system.
- **Ministry of Defence: Characterization of an attacker** Aïmad Berady has started his PhD thesis in November 2018 in the context of a contract between CentraleSupelec and the French Ministry of Defence. His work is to highlight the characteristics of an attacker performing a targeted and long-term attack on an information system.
- **Nokia: Risk-aware security policies adaptation in modern communication infrastructures** Pernelle Mensah was hired in January 2016 on this CIFRE funding in order to work on unexplored aspects of information security, and in particular response strategies to complex attacks, in the context of cloud computing architectures. The use case proposed by our industrial partner is a multi-tenant cloud computing platform involving software-defined networking in order to provide further flexibility and responsiveness in architecture management. The topic of the thesis is to adapt and improve the current risk-aware reactive response tools, based on attack graphs and adaptive security policies, to this specific environment, taking into account the heterogeneity of actors, platforms, policies and remediation options.
- **Orange LAb's: Storage and query in a massive distributed graph for the web of things** Cyprien Gottstein has started his PhD thesis in October 2018 in the context of a collaboration between Inria and Orange (I/O Lab). In this thesis, we consider storage and query problems that arise when massive distributed graphs are used to represent the web of things. In particular, access to the data and partitioning of the graph are studied to propose efficient geographical services.
- **Thales: Privacy and Secure Multi-party Computation** Aurélien Dupin has started his PhD thesis in January 2016 within the context of a CIFRE contract with Thales. His PhD subject concerns secure multi-party computation. Secure two-party computation provides a way for two parties to compute a function, that depends on the two parties' inputs, while keeping them private. Known since the 1980s, Yao's garbled circuits appear to be a general solution to this problem, in the semi-honest model. Decades of optimizations have made this tool a very practical solution. However, it is well known that a malicious adversary could modify a garbled circuit before submitting it. Many protocols, mostly based on cut-&-choose, have been proposed to secure Yao's garbled circuits in the presence of malicious adversaries. Nevertheless, how much an adversary can modify a circuit and make it still executable have not been studied. In the context of his PhD, Aurélien Dupin is interested by such a question.

- **Thales: Combining Attack Specification and Dynamic Learning from traces for correlation rule generation** Charles Xosanavongsa has started his PhD thesis in December 2016 in the context of a CIFRE with Thales. His work will focus on the construction of correlation rules. In previous work on correlation rule generation, the usual approach is static. It always relies on the description of the supervised system using a knowledge base of the system. The use of correlation trees is an appealing solution because it allows to have a precise description of the attacks and can handle any kind of IDS. But in practice, the behavior of each IDS is quite difficult to predict, in particular for anomaly based IDS. To manage automatically the correlation rules (and adapt them if necessary), we plan to analyze synthetic traces containing both anomaly based and misused based IDS alerts resulting from an attack.

COMETE Project-Team (section vide)

DATASPHERE Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

The PhD Thesis of Colin Gerard is funded through a contract with DGA (Ministry of Defense).

PESTO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

We have several contracts with industrial partners interested in the design of electronic voting systems:

- Since 2014, a collaboration agreement has been signed between Pesto and Scytl, a Spanish company which proposes solutions for the organization of on-line elections, including legally binding elections, in several countries. In this context, a first contract has been signed in 2016 to design a formal proof of both verifiability and privacy of the protocol developed by Scytl, for deployment in Switzerland. In 2018, a new contract has been signed to adapt the previous security proof to the new protocol proposed by Scytl, in order to achieve universal verifiability.
- Docapost signed a 18-month contract in September 2017, with Pesto and Caramba, to enhance the voting solution of Docapost, in particular with respect to verifiability.
- IDEMIA signed a 2-year contract in January 2019, with Pesto and Caramba. The goal is to design a voting protocol adapted to the elections they plan to organize, in various countries. This includes the use of smartcard, yet without having to trust them. Once designed, the protocol will be formally analysed with the tools developed in the team such as ProVerif or Tamarin.

8.2. Bilateral Grants with Industry

A CIFRE contract with Numeryx has started with the Resist research group at Inria Nancy and Pesto, to develop algorithms for optimizing sets of filtering rules in Software Defined Networks.

PRIVATICS Project-Team (section vide)

PROSECCO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. Evolution, Semantics, and Engineering of the F Verification System*

Grant from Nomadic Labs - Inria

PIs: Catalin Hritcu and Exequiel Rivas

Duration: March 2019 - April 2023

Abstract: While the F* verification system shows great promise in practice, many challenging conceptual problems remain to be solved, many of which can directly inform the further evolution and design of the language. Moreover, many engineering challenges remain in order to build a truly usable verification system. This proposal promises to help address this by focusing on the following 5 main topics: (1) *Generalizing Dijkstra monads*, i.e., a program verification technique for arbitrary monadic effects; (2) *Relational reasoning in F**: devising scalable verification techniques for properties of multiple program executions (e.g., confidentiality, noninterference) or of multiple programs (e.g., program equivalence); (3) *Making F*'s effect system more flexible*, by supporting tractable forms of effect polymorphism and allowing some of the effects of a computation to be hidden if they do not impact the observable behavior; (4) Working out more of the *F* semantics and metatheory*; (5) Solving the *engineering challenges* of building a usable verification system.

TAMIS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- CISCO (http://www.cisco.com) contract (2017–2019) to work on graph analysis of malware

7.2. Bilateral Grants with Industry

- CISCO (http://www.cisco.com) one grant (2016–2019) to work on semantical analysis of malware
- Thales (https://www.thalesgroup.com) one CIFRE (2016–2019) to work on verification of communication protocols, one grant (2018–2019) to work on learning algorithms
- Oberthur Technologies (http://www.oberthur.com/) one grant (2016–2020) to work on fuzzing and fault injection