RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2015

Section Contracts and Grants with Industry

Edition: 2016-03-21

ARIC Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

- Marie Paindavoine is supported by an Orange Labs PhD Grant (from October 2013 to November 2016). She works on privacy-preserving encryption mechanisms.
- Within the program Nano 2017, we collaborate with the Compilation Expertise Center of STMicroelectronics on the theme of floating-point arithmetic for embedded processors.

CARAMEL Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Training and Consulting with HTCS

The training and consulting activities begun in 2012 with the HTCS company have been pursued, and the existing contract has been renewed in identical form for 2013, 2014 and 2015.

8.2. Consulting with Docapost

In the context of our activities on electronic voting, in collaboration with the Cassis team, we had a consulting contract with the Docapost company. The goal was to evaluate their e-voting product and to propose various directions for future improvements.

CASCADE Project-Team (section vide)

CRYPT Team (section vide)

GALAAD2 Team (section vide)

GEOMETRICA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Cifre Contract with Geometry Factory

Mael Rouxel-Labbé's PhD thesis is supported by a Cifre contract with GEOMETRY FACTORY (http://www.geometryfactory.com). The subject is the generation of anisotropic meshes.

8.1.2. Commercialization of cgal packages through Geometry Factory

In 2015, GEOMETRY FACTORY (http://www.geometryfactory.com) had the following new customers for CGAL packages developed by GEOMETRICA:

CSM3D (UK, Cad chaussures): surface parametrization

Silvaco (USA, simulation) : 3d mesh generation

Cimmi (Canada): Approximation of Ridges and Umbilics on Triangulated Surface Meshes, Estimation of Local Differential Properties, AABB Tree, Principal Compoment Analysis, Point Set Processing

Varel (France, forage): 2D triangulations

Powel (Norway, GIS): point set processing, surface reconstruction

ExxonMobil (USA) : 2D triangulations, surface parametrization

Metrologic (France, metrology): point set processing

Geomage (Israel, oil&gas): 2D and 3D triangulations

Corvid (USA, simulation) : 3D triangulations

Medicim (Belgium, medical imaging): 3D mesh generation

Huntsman (Belgium), Pasco (Japan), Qualcomm (USA), Facebook (USA): industrial research licenses

GRACE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. Alcatel-Lucent

Within the framework of the joint lab Inria-ALU, Grace and Alcatel-Lucent collaborate on the topic of Private Information Retrieval: that is, enabling a user to retrieve data from a remote database while revealing neither the query nor the retrieved data. (This is not the same as data confidentiality, which refers to the need for users to ensure secrecy of their data; this is classically obtained through encryption, which prevents access to data in the clear.)

A typical application would be a centralized database of medical records, which can be accessed by doctors, nurses, and so on. A desirable privacy goal would be that the central system does not know which patient is queried for when a query is made, and this goal is precisely achieved by a Private Information Retrieval protocol. Note also that in this scenario the database is not encrypted, since many users are allowed to access it.

We are exploring applications of Locally Decodable Codes to Private Information Retrieval in the multi-cloud (multi-host) setting, to ensure both secure, reliable storage, and privacy of database queries.

Our progress on information sets of multiplicity codes was presented at the ISIT 2015 conference [18]

LFANT Project-Team (section vide)

POLSYS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Gemalto. Gemalto is an international IT security company providing software applications, secure personal devices such as smart cards and token, POLSYS is currently working with Gemalto – thanks to a CIFRE PhD grant – on the security analysis of code-based cryptosystems (Participants: J.-C. Faugère, L. Perret, F. Urvoy de Portzamparc).

7.2. Industrial Transfer

Until the mid 2000's, multivariate cryptography was developing very rapidly, producing many interesting and versatile public-key schemes. However, many of them were soon successfully cryptanalysed (a lot have been done in this group). As a consequence, the confidence in multivariate cryptography cryptosystems declined. It seems that there have emerged new important reasons for renewal of the interest in a new generation of multivariate schemes. In the past two years, the algorithms for solving the Discrete Logarithm Problem over small characteristic fields underwent an extraordinary development. This clearly illustrates the risk to not consider alternatives to classical assumptions based on number theory. In parallel, two of the most important standardization bodies in the world, NIST and ETSI have recently started initiatives for developing cryptographic standards not based on number theory, with a particular focus on primitives resistant to quantum algorithms. An objective here is then to focus on the design of multivariate schemes.

The team is now involved in the industrial transfer of post-quantum cryptography. The project is supervised by SATT-LUTECH. SATT Lutech specializes 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, Université Panthéon-Assas, Paris Sorbonne University and National School of Industrial Creation).

The team has recently developed, in partnership with a mobile application development company (WASSA), an Android app for smartphones (Samsung G5 type) that uses multivariate cryptography. The application has been tested mid-November in a series of experiments supervised by DGA and French Minsitry of Defense. The experiment gathered a total of hundred participants from various operational units. This is a first milestone in the maturation project whose goal is to create a start-up.

SECRET Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

- **Thales** ($02/14 \rightarrow 01/17$)
  Funding for the supervision of Julia Chaulet's PhD.
  30 kEuros.

SPECFUN Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- *Mathematical Components* (project of the MSR–INRIA Joint Centre).
  Goal: Investigate the design of large-scale, modular and reusable libraries of formalized mathematics, using the Coq proof assistant. This project successfully formalized the proof of the Odd Order Theorem, resulting in a corpus of libraries related to various areas of algebra.
  Leader: G. Gonthier (MSR Cambridge). Participants: F. Chyzak, A. Mahboubi.
  Website: http://www.msr-inria.fr/projects/mathematical-components/.

VEGAS Project-Team (section vide)

ALF Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Intel research grant ALF-INTEL2014-8957

Participants: André Seznec, Fernando Endo.

Intel is supporting the research of the ALF project-team on "Mixing branch and value prediction to enable high sequential performance".

8.2. Bilateral Grants with Industry

8.2.1. Nano 2017 PSAIC

Participants: Arif Ali Ana-Pparakkal, Erven Rohou, Emmanuel Riou.

Nano 2017 PSAIC is a collaborative R&D program involving Inria and STMicroelectronics. The PSAIC (Performance and Size Auto-tuning through Iterative Compilation) project concerns the automation of program optimization through the combination of several tools and techniques such as: compiler optimization, profiling, trace analysis, iterative optimization and binary analysis/rewriting. For any given application, the objective is to devise through a fully automated process a compiler profile optimized for performance and code size. For this purpose, we are developing instrumentation techniques that can be focused and specialized to a specific part of the application aimed to be monitored.

The project involves the Inria teams ALF, AriC, CAMUS and CORSE. ALF contributes program analyses at the binary level, as well as binary transformations. We will also study the synergy between static (compiler-level) and dynamic (run-time) analyses.

ATEAMS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

With the **ING bank** we a running a four-year project on advising and research in functional and non-functional properties of a part of the ING IT-infrastructure. The project involves modelling a large part of the product portfolio and using state-of-the-art MDE technology to simulate, verify and generate part of its IT infrastructure. The funding of this project is approximately 50% industry, 50% grants from CWI & NWO.

CAIRN Project-Team (section vide)

CAMUS Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

The CAMUS team is taking part of the NANO 2017 national research program and its sub-project PSAIC (Performance and Size Auto-tuning thru Iterative Compilation) with the company STMicroelectronics, starting January 2015. Luis Esteban Campostrini has been recruited as PhD student in this project. His work is focusing in extending advanced loop optimization techniques to nonlinear loops using a linear virtual data layout remapping. Artiom Baloian has been recruited in October 2015 as research engineer, in order to make the Apollo framework applicable to ARM Cortex platforms and to merge all the last extensions inside the framework.

COMPSYS Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. ManycoreLabs Project with Kalray

Compsys was part of 3-years a bilateral contract with Kalray called ManycoreLabs, funded by "Investissements d'avenir pour le développement de l'économie numérique". The goal of this project was to allow the company Kalray, based on a collaboration with several partners, to become the European leader of the market of many-core chips for embedded systems. Industrial partners of this project included Bull, CAPS Entreprise, Digigram, Thales, Renault. Academic partners are CEA, Inria (Parkas, Compsys, and Corse), VERIMAG.

Compsys role was to explore analysis and compilation techniques linked to streaming languages, with the Kalray MPPA platform as long-term target. The research on OpenStream described in Section 7.8 corresponds to extensions of the work package WP 2.5.3. This study showed the need for extending polyhedral techniques to polynomials, which is one of the motivation of the work described in Section 7.11 . The work on parametric tiling (Section 7.7), first in the context of FPGA, then of GPUs, was also a first step towards the automatic generation of blocking algorithms for multicores such as the Kalray MPPA.

This project ended in June 2015.

8.2. Technological Transfer: XtremLogic Start-Up

The XTREMLOGIC start-up (http://xtremlogic.com/) was initiated, initially with the name Zettice, at the end of 2010 by Alexandru Plesco and Christophe Alias, after the PhD thesis of Alexandru Plesco under the guidance of Christophe Alias, Alain Darte and Tanguy Risset. The goal of XTREMLOGIC is to build on the disruptive technologies emerging from the polyhedral compilation community, and particularly the results obtained in Compsys, to provide the HPC market with efficient and communication-optimal circuit blocks (IP) for FPGA.

The compiler technology transferred to XTREMLOGIC (see Sections 6.2 and 7.5) is the result of a tight collaboration between Christophe Alias and Alexandru Plesco. XTREMLOGIC is one way to spread the polyhedral technology to industry. In 2015, XTREMLOGIC was supported by the Rhône Développement Initiative 2015 (loan).

CORSE Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contract with Industry

- Tirex is a bilateral contract with Kalray. The subject is a prototyping of hybrid alias analysis. The collaboration led to a recent publication which corresponding work is described in 6.4 .

7.2. Bilateral Grants with Industry

- ManyCoreLabs is a bilateral Grant (BGLE) with Kalray. CORSE is involved in the development of generalized register tiling.
- PSAIC Nano2017 is a bilateral Grant with STMicroelectronics. CORSE is involved in the development of trace analysis and hybrid compilation.
- DEMA Nano2017 is a bilateral Grant with STMicroelectronics. CORSE is involved in the development of debugging of multithreaded applications.

7.3. CIFRE contracts

- CORSE is involved in another contract with Kalray associated with the CIFRE PhD of Duco van Amstel. The subject of the collaboration is related to fine grain scheduling. Corresponding work is described in 6.3 .
- CORSE is involved in a contract with Aselta for the CIFRE thesis of Nassim Halli.
- CORSE is also involved in two contracts with STMicroelectronics for the CIFRE theses of Serge Emteu and Oleg Iegorov.

DREAMPAL Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Collaboration contract with Nolam Embedded Systems: In conjunction with the CIFRE grant of Venkatasubramanian Viswanathan, a collaboration contract is established with Nolam ES. The objective is to design an innovative embedded computing platform supporting massively parallel dynamically reconfigurable execution model. The use-cases of this platform cover several application domains such as medical, transportation and aerospace.

Collaboration contract with NAVYA: In conjunction with the doctoral grant of Karim Ali, a collaboration contract is established with NAVYA. The objective is to design an innovative embedded system dedicated for dynamic obstacle detection and tracking for autonomous vehicle navigation.

POSTALE Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- EDF R&D: this is a collaboration with the department SINETICS of EDF in the area of high-performance computing.
  Participants: Marc Baboulin, Amal Khabou.

  It concerns two differents topics:
  - Enhancing performance of numerical solvers using accelerators (postdoc started in October 2014).
  - Studying numerical quality and reproducibility in HPC exascale applications (ongoing ANR submission).
- NumScale: Collaboration with the small size company NumScale (PME, 10 people) NumScale on C++ parallel code generation technology. NumScale is a start-up created in 2012 as the result of a Digiteo/University Paris Sud technological transfer program (Digiteo OMTE). NumScale exploits scientific results and tools based around code generation for parallel programs as well as advanced code optimization techniques developed by members of the team.

TASC Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Labcom TransOp

Participants: Charles Prud'Homme, Xavier Lorca.

Title: TransOp.

Duration: 2014-2016.

Type: **new project**.

Budget: 300000 Euros.

Others partners: Eurodécision.

The goal of the project is to handle robustness in the context of industrial timetabling problems with constraint programming using CHOCO. The project is managed by Xavier Lorca.

8.2. Bilateral Grants with Industry

8.2.1. Gaspard Monge

Participants: Nicolas Beldiceanu, Helmut Simonis.

Title: Gaspard Monge 2.

Duration: 2014.

Type: **continuation of 2012,2013 project**.

Budget: 6000 Euros.

Others partners: EDF.

Within the context of the Gaspard Monge call program for Optimisation and Operation Research we work with EDF on the research initiative on *Optimization and Energy*. The goal of the project (continuation of last years projects) is to provide a systematic reformulation of time-series constraints in term of linear constraints that can be used in a MIP solver.

AOSTE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Kontron CIFRE

This contract, ended in April 2015, provided partial support for the PhD thesis of Mohamed Bergach. It was extended until the end of September with a direct collaborative contrat funded by Kontron until the PhD defense [16]
The topic is to study how to efficiently implement various sizes of the FFT (Fast Fourier Transform) algorithm on multicore and GP-GPU architectures from the range of processors used at Kontron, in order to understand in a second phase how to best allocate several such algorithms in parallel, as part of a single application, in the most efficient way (regarding performance but also power consumption and thermal constraints).

8.1.2. Airbus CIFRE

This contract, started on March 2014, provides full support for the PhD thesis of Cristian Maxim. The thesis concerns the statistical timing analysis while different variability factors are taken into account. This method is built on top of existing statistical approaches while proving appropriate programs for training these methods and thus learning from the history of the execution.

8.1.3. CNES/Airbus DS

Financing comes here through the CNES R&T programme, which has partly funded the post-doctorate of Raul Gorcitz (Sep 2013-Aug 2015) and the acquisition of an industry-grade evaluation platform based on TTEthernet and VxWorks 653.

The objective of our collaboration with Airbus Defence and Space and the CNES is to determine how the design and implementation of embedded software and system/network configuration can be largely automated in an aerospace context, while preserving an assurance level superior to that of the Ariane 5 flight program. We are exploring the novel algorithms developed and implemented in the Lopht tool.

CONVECS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

Participants: Hubert Garavel, Abderahman Kriouile, Radu Mateescu, Wendelin Serwe.

Abderahman Kriouile is supported by a CIFRE PhD grant (from March 2012 to March 2015) from STMicroelectronics (Grenoble) on the verification of cache coherency in systems on chip (see § 6.5.1), under the supervision of Guilhem Barthes (STMicroelectronics), Christophe Chevallaz (STMicroelectronics), Grégory Faux (STMicroelectronics), Radu Mateescu (CONVECS), Wendelin Serwe (CONVECS), and Massimo Zendri (STMicroelectronics).

HYCOMES Team (section vide)

MUTANT Project-Team (section vide)

PARKAS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Technology Transfer Project, partly funded by the TETRACOM grant and by Kalray.

7.2. Bilateral Grants with Industry

Polly Labs initiative. Fully funded by ARM.

POSET Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- PhD Grant CIFFRE, 2015-2018, for Jean-Michael Célérier, in partnership with Blue Yeti (Royan),

SPADES Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- INRIA and Orange Labs have established this year 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.
- With Daimler (subcontracting via iUTBS): We have applied our recent improvements regarding the analysis of deadline miss models for real-time systems to the specific needs of Daimler in the context of CAN buses.

7.2. Bilateral Grants with Industry

With Thales: Early Performance assessment for evolving and variable Cyber-Physical Systems. This CIFRE grant funds the PhD of Christophe Prévot.

TEA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Toyota Info-Technology Centre (2014+)

Title: Co-Modeling of Safety-Critical Multi-threaded Embedded Software for Multi-Core Embedded Platforms

Inria principal investigator: Jean-Pierre Talpin

International Partner (Institution - Laboratory - Researcher):

Toyota Info-Technology Centre, Mountain View, California

Virginia Tech Research Laboratories, Arlington

Duration: renewed yearly since 2014

Abstract: We started a new project in April 2014 funded by Toyota ITC, California, to work with Huafeng Yu (a former post-doctorate of team ESPRESSO) and with VTRL as US partner. The main topic of our project is the semantic-based model integration of automotive architectures, virtual integration, toward formal verification and automated code synthesis. This year, Toyota ITC is sponsoring our submission for the standardisation of a time annex in the SAE standard AADL.

In a second work-package, we aim at elaborating a standardised solution to virtually integrate and simulate a car based on heterogeneous models of its components. This year, it will be exemplified by the elaboration of a case study in collaboration with Virginia Tech. The second phase of the project will consist of delivering an open-source, reference implementation, of the proposed AADL standard and validate it with a real-scale model of the initial case-study.

8.2. Bilateral Grants with Industry

8.2.1. Mitsubishi Electric R&D Europe (2015-2018)

Title: Analysis and verification for correct by construction orchestration in automated factories

Inria principal investigator: Jean-Pierre Talpin, Simon Lunel

International Partner: Mitsubishi Electric R&D Europe

Duration: 2015 - 2018

Abstract: The primary goal of our 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 plan to explore a multi-sorted algebraic framework for static analysis and formal verification starting from a simple use case extracted from Mitsubishi factory automation documentations. This will serve as a basis to more ambitious research where we intend to leverage recent advance in type theory, SMT solvers for nonlinear real arithmetic (dReal and δ-decidability) and contracts theory (meta-theory of Benveniste et al., Ruchkin's contracts) to provide a general framework of reasoning about heterogeneous factory components.

ANTIQUE Project-Team (section vide)

CELTIQUE Project-Team (section vide)

DEDUCTEAM Team (section vide)

ESTASYS Team (section vide)

GALLIUM Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. The Caml Consortium

Participants: Xavier Leroy [**contact**], Damien Doligez, Didier Rémy.

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 Caml. 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.

The Consortium currently has 12 member companies:

- Aesthetic Integration
- Bloomberg
- CEA
- Citrix
- Dassault Aviation
- Dassault Systèmes
- Esterel Technologies
- Jane Street
- LexiFi
- Microsoft
- OCamlPro
- SimCorp

For a complete description of this structure, refer to http://caml.inria.fr/consortium/. Xavier Leroy chairs the scientific committee of the Consortium.

8.1.2. Scientific Advisory for OCamlPro

Participant: Fabrice Le Fessant.

OCamlPro is a startup company founded in 2011 by Fabrice Le Fessant to promote the use of OCaml in the industry, by providing support, services and tools for OCaml to software companies. OCamlPro performs a lot of research and development, in close partnership with academic institutions such as IRILL, Inria and Univ. Paris Sud, and is involved in several collaborative projects with Gallium, such as the Bware ANR, the Vocal ANR and the Secur-OCaml FUI.

Since 2011, Fabrice Le Fessant is a scientific advisor at OCamlPro, as part of a collaboration contract for Inria, to transfer his knowledge on the internals of the OCaml runtime and the OCaml compilers.

MARELLE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

In 2015, we discussed a contract with a potential industrial partner, but these discussions are currently covered by a non-disclosure agreement. We expect this discussion to become visible in 2016.

MEXICO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

At present, our industrial cooperations are centered in the IRT SystemX, see below; there are currently no *bilateral* agreements.

PARSIFAL Project-Team (section vide)

PI.R2 Project-Team (section vide)

SUMO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Joint Alstom-Inria research lab: 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 project started in march 2014. Alstom agreed to start a second phase of the project in 2016, for a duration of three years. This covers in particular the CIFRE PhD of Karim Kecir.

TOCCATA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. ProofInUse Joint Laboratory

Participants: Claude Marché [contact], Jean-Christophe Filliâtre, Andrei Paskevich.

ProofInUse is a joint project between the Toccata team and the SME AdaCore. It was selected and funded by the ANR programme "Laboratoires communs", starting from April 2014, for 3 years http://www.spark-2014.org/proofinuse.

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 goal is now to promote and transfer the use of deduction-based verification tools to industry users, who develop critical software using the programming language Ada. The proof tools are aimed at replacing or complementing the existing test activities, whilst reducing costs.

VERIDIS Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. ADN4SE Project

Participants: Stephan Merz, Martin Riener.

Joint work with Damien Doligez of Inria Paris Rocquencourt.

The ADN4SE project started in 2013 within *Programme d'Investissements d'Avenir: Briques Génériques du Logiciel Embarqué* and is coordinated for Inria by the Gallium team in Rocquencourt. The objective of this project is to develop and commercialize the PharOS real-time micro-kernel operating system. In cooperation with researchers at CEA List, we are contributing to the project by verifying key properties (in particular, determinism) of a high-level model of the system written in TLA$^+$. The proof was completed in the summer of 2015, and the project ended in December 2015.

8.2. Proving formulas over streams

Participants: Pascal Fontaine, Stephan Merz.

In an exploratory project with *Atelier de Qualification Logicielle* of RATP, we studied the use of SAT solving techniques for proving certain formulas expressed over infinite Boolean streams. Such formulas arise as proof obligations generated from SCADE models used by RATP, and they are currently proved using proprietary tools. We showed that in the absence of recursive definitions, checking a small number of instances of a proof obligation ensures its validity for all instances. For models that contain recursive definitions, the bound on the number of instances that must be checked becomes much bigger, making it unwieldy to apply the same technique, and inductive reasoning should be used. We implemented our proposal in a prototype checker and validated it using several benchmarks provided by RATP.

CARTE Project-Team (section vide)

CASSIS Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Electronic Voting Systems

Participant: Véronique Cortier.

A collaboration agreement has been signed between Loria and Scytl, a Spanish company who is proposing solutions for the organization of on-line elections, including legally binding elections, in several countries. We have a collaboration with David Galindo (who joined Scytl in July 2014) on defining security properties for e-voting (privacy as well as verifiability properties) and designing e-voting schemes that meet all these properties. Further contracts may cover the analysis of the solutions developed at Scytl.

8.2. Electronic Voting Systems

Participants: Véronique Cortier, Stéphane Glondu.

Docapost has signed a 6 months contract with Cassis for defining potential colaborations around the voting protocol used by Docapost. We have examined their source code and proposed a list of enhancements, delivered at the end of the contract. Based on this list, further collaborations should take place in the following years.

COMETE Project-Team (section vide)

DECENTRALISE Team (section vide)

DICE Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

Worldline Wordline is a leader in B2B applications development, and is in the front line to provide new technical solution in the Web 2.0 era. We have a CIFRE partnership contract on the study of flow based architectures both at the data centers and at the Web browser level.

PRIVATICS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. IPSec with pre-shared key for MISTIC security

Title: IPSec with pre-shared key for MISTIC security.

Type: CIFRE.

Duration: Juillet 2014 - Juillet 2017.

Coordinator: Inria

Others partners: Privatics, Moais and Incas-ITSec.

PROSECCO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

The miTLS project received a grant from Mozilla for work on TLS 1.3. Catalin Hritcu received a PhD grant from Microsoft Research.