



RESEARCH CENTER

FIELD

Algorithmics, Programming, Software and Architecture

Activity Report 2013

Section Contracts and Grants with Industry

Edition: 2014-03-20

ALGORITHMICS, COMPUTER ALGEBRA AND CRYPTOLOGY

1. ARIC Project-Team	5
2. CAMEL Project-Team	6
3. CASCADE Project-Team (section vide)	7
4. CRYPT Team (section vide)	8
5. GEOMETRICA Project-Team	9
6. GRACE Project-Team	10
7. LFANT Project-Team	11
8. POLSYS Project-Team	12
9. SECRET Project-Team	13
10. Specfun Team	14
11. VEGAS Project-Team (section vide)	15

ARCHITECTURE, LANGUAGES AND COMPILATION

12. ALF Project-Team	16
13. ATEAMS Project-Team (section vide)	17
14. CAIRN Project-Team (section vide)	18
15. CAMUS Team	19
16. COMPSYS Project-Team	20
17. CONTRAINTES Project-Team	21
18. DREAMPAL Team	22
19. INDES Project-Team (section vide)	23
20. PAREO Project-Team (section vide)	24
21. TASC Project-Team	25

EMBEDDED AND REAL TIME SYSTEMS

22. ESPRESSO Project-Team (section vide)	28
23. S4 Project-Team	29
24. TRIO Team (section vide)	30

EMBEDDED AND REAL-TIME SYSTEMS

25. AOSTE Project-Team	31
26. CONVECS Project-Team	32
27. Hycomes Team (section vide)	33
28. MUTANT Project-Team	34
29. PARKAS Project-Team	35
30. SPADES Team	36

PROGRAMS, VERIFICATION AND PROOFS

31. FORMES Team (section vide)	37
32. SECSI Project-Team (section vide)	38

PROOFS AND VERIFICATION

33. ABSTRACTION Project-Team	39
34. CELTIQUE Project-Team	40
35. DEDUCTEAM Exploratory Action (section vide)	41

36. GALLIUM Project-Team	42
37. MARELLE Project-Team (section vide)	43
38. MEXICO Project-Team (section vide)	44
39. PARSIFAL Project-Team (section vide)	45
40. PI.R2 Project-Team (section vide)	46
41. SUMO Team	47
42. TOCCATA Team	48
43. VERIDIS Project-Team	49

SECURITY AND CONFIDENTIALITY

44. CARTE Project-Team	50
45. CASSIS Project-Team	51
46. COMETE Project-Team (section vide)	52
47. DICE Team	53
48. PRIVATICS Team	54
49. PROSECCO Project-Team	55

ARIC Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Contract with STMicroelectronics

A contract between STMicroelectronics and Inria supported our work on floating-point arithmetic code generation and specialization for embedded processors (duration: 36 months; amount: 36,000 euros; signature: fall 2010). This work, which was done jointly with the Compilation Expertise Center of STMicroelectronics Grenoble, was also supported by the PhD CIFRE grant of Jingyan Jourdan-Lu.

7.1.2. Collaboration with Bosch

Bosch (Stuttgart) ordered us a study on the choice of an adequate representation of numbers (fixed-point or floating-point) for some embedded systems. The study was conducted by Florent de Dinechin and Jean-Michel Muller.

7.1.3. Collaboration with Intel

INTEL made a \$20000 donation in recognition of our work on the correct rounding of functions.

7.2. Bilateral Grants with Industry

7.2.1. Kalray CIFRE PhD Grant

Nicolas Brunie is supported by a CIFRE PhD grant (from 15/04/2011 to 14/04/2014) from Kalray. The purpose is the study of a tightly coupled reconfigurable accelerator to be embedded in the Kalray multicore processor. Advisors: Florent de Dinechin and, within Kalray, Benoît de Dinechin. The support contract between Kalray and Inria amounts to 76,000 euros on three years.

7.2.2. Orange Labs PhD Grant

Marie Paindavoine is supported by an Orange Labs PhD Grant (from October 2013 to November 2016). She will work on privacy-preserving encryption mechanisms.

CAMEL Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Training and Consulting with HTCS

Participants: Pierrick Gaudry, Emmanuel Thomé [contact].

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 and 2014.

7.2. Study of the Kalray MPPA-256 Processor for Applications in Cryptology

Participants: Jérémie Detrey, Pierrick Gaudry [contact].

A 5-month contract has been signed between CAMEL (through Inria) and Kalray, a French company which has recently designed and manufactured the MPPA-256 processor, a 256-core VLIW architecture targeted at embedded applications. The objective of this contract was to study the performance of this processor in a cryptographic context. Several key arithmetic primitives, such as multi-precision modular arithmetic or polynomial multiplication in binary and ternary fields, were implemented and optimized to take advantage of the specific micro-architecture and instruction set of the VLIW cores of the MPPA-256. The results are encouraging and prompt us to explore further the possible benefits of this processor for cryptanalytic applications.

7.3. Study of the electronic voting system of Voxaly

Participants: Pierrick Gaudry, Stéphane Glondu [contact].

A 4-month contract has been signed between CAMEL, CASSIS and Voxaly, a French company who is proposing solutions for the organization of on-line elections. During several meetings, we discussed their current solution and proposed improvements to gradually add security features that get close to the academic standards.

CASCADE Project-Team (section vide)

CRYPT Team (section vide)

GEOMETRICA Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. *Contrat Cifre 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.

7.1.2. *Commercialization of cgal packages through Geometry Factory*

In 2013, GEOMETRY FACTORY (<http://www.geometryfactory.com>) had the following new customers for CGAL packages developed by GEOMETRICA:

GeoSoft (oil and gas, USA) : 2D constrained triangulation, AABB tree

British Geological Survey (oil and gas, UK) : 2D Meshes, Interpolation

Hexagon Machine Control (GIS, Sweden) 3D triangulations, point set processing

Thales (GIS, France) 2D constrained triangulation

GRACE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

- Within the framework of the joint lab Inria-ALU, Grace and Alcatel-Lucent collaborate on the topic of Private Information Retrieval: that is, retrieving 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, and is classically obtained through encryption, which prevents access to data in clear.) 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. We will hire a PhD candidate in February 2014.

LFANT Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. DGA

Contract with *DGA maîtrise de l'information* about number theory and cryptography

- Duration: two years, 2011–2013 (ended May 2013)
- Scientific coordinator: J.-M. Couveignes
- Topics covered: index calculus and discrete logarithms, fast arithmetic for polynomials, pairings and cryptography, algorithmics of the Langlands programme

POLSYS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts and Grants with Industry

- **Oberthur Technologies**
Oberthur Technologies is the World second largest provider of security and identification solutions and services based on smart card technologies for mobile, payment, transport, digital TV and convergence markets. Since 2007, SALSA co-supervised 3 internships of first year master student on cryptology in smart-cards, and one internship of a 2nd year master student. The goal of this last internship was to study the feasibility of implementing multivariate schemes in constrained environments (typically a smart card). A new jointly supervised PhD thesis (PolSys/Oberthur) has start in march 2012.
- **Gemalto**
Gemalto is an international IT security company providing software applications, secure personal devices such as smart cards and token, etc. Governments, wireless operators, banks, and enterprises use Gemalto's software and personal devices to deliver mobile services, payment security, authenticated cloud access, identity and privacy protection, eHealthcare, eGovernment, transport ticketing and machine to machine (M2M) communications applications.

SECRET Project-Team

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Contracts with Industry

- **High Tech Communications Services** (09/13 → 09/14)
Recovering a convolutional encoder followed by a block interleaver
19 kEuros

Specfun Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

The team is involved in two Common Research Agreements in the MSR–INRIA Joint Centre:

- *DDMF (Dynamic Dictionary of Mathematical Functions)*.
Goal: Automate exact computations of the mathematical formulas on the special functions of mathematical analysis and present them on an interactive mathematical dictionary online.
Leader: F. Chyzak. Participants: A. Bostan, P. Lairez.
Website: <http://ddmf.msr-inria.inria.fr/>.
- *Mathematical Components*.
Goal: Investigate the design of large-scale, modular and reusable libraries of formalized mathematics. Developed 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: A. Mahboubi, E. Tassi.
Website: <http://www.msr-inria.fr/projects/mathematical-components/>.

VEGAS Project-Team (section vide)

ALF Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Intel Research Grant

Participant: André Seznec.

Intel is supporting the research of the ALF project-team on "Alternative ways for improving uniprocessor performance".

ATEAMS Project-Team (section vide)

CAIRN Project-Team (section vide)

CAMUS Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

A contract with the French company Kalray (<http://www.kalray.eu>) was established early 2013. It provided to the team the Kalray 256-core MPPA platform and necessary funding to recruit a student for a 6-months internship: Dhruva Tirumala Bukkapatnam. A deep evaluation of the platform regarding performance and programming strategies has been accomplished. Moreover, an extension of the source-to-source compiler Pluto (<http://pluto-compiler.sourceforge.net>), allowing to automatically generate code adapted for the MPPA has been mostly implemented.

COMPSYS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Tirex Contract with Kalray

Compsys has a contract with Kalray called Tirex. The goal of this project is to prototype within the TireX toolbox (see Section 5.17) some new profiling/analysis techniques necessary to enable cloning. Because of the current financial problems encountered by Kalray, the efforts related to this project have been frozen until further notice.

7.2. ManycoreLabs Project with Kalray

Compsys is part of a bilateral grant with Kalray called ManycoreLabs, funded by “Investissements d’avenir pour le développement de l’économie numérique”. The goal of this project is 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 include Bull, CAPS Entreprise, Digigram, Thales, Renault. Academic partners are CEA, Inria (Parkas and Compsys), VERIMAG.

The cloning/specialization work summarized in Section 6.3 and the generalized register tiling work summarized in Section 6.4 have been done in the context of this grant and correspond to WP 3.3.3. The research on OpenStream described in Section 6.15 corresponds to WP 2.5.3.

7.3. Technological Transfer Towards Zettice Start-Up

Participants: Christophe Alias, Adrian Muresan [Zettice], Alexandru Plesco [Zettice].

The Zettice start-up project has been initiated by Alexandru Plesco and Christophe Alias in March 2011, with the idea of transferring some of the research concepts emerging from the polyhedral model to the context of high-level circuit synthesis. Since, an important amount of applied research has been achieved to propose an effective technology ready for industrial transfer. From an academic perspective, Zettice is a unique opportunity to cover all the aspects of high-level synthesis from the front-end aspects (polyhedral code analysis and optimization) to the back-end aspects (pipelining, retiming, FPGA mapping) providing a global knowledge of relevant industrial issues.

Zettice received in 2012 the “*lean start-up award*” of the startup weekend labs 2012, the “*most exciting start-up mention*” at SAME 2012, and the *concours Crealys Excel&Rate 2012* grant (30 Keuros). In 2013, Zettice won the *concours OSEO 2013* grant (Banque Publique d’Investissement, 40 Keuros) and the “*most promising start-up award*” at SAME 2013.

A patent is under deposit. The research results related to Zettice are presented in Section 6.9 . The software tools developed in the context of Zettice are Dcc (see Section 5.8) and IceGEN (see Section 5.9).

CONTRAINTEs Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- Cifre PhD accompanying contract with General Electric Transportation on urban railway time tabling optimization (2011-2014).

7.2. Bilateral Grants with Industry

- DTI ITI support for the industrialization of our Rules2CP modeling software and technological transfer to SME KLS-Optim (2011-2013).

DREAMPAL 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.

7.2. Bilateral Grants with Industry

The FAMOUS project aims at introducing a complete methodology that takes the reconfigurability of the hardware as an essential design concept and proposes the necessary mechanisms to fully exploit those capabilities at runtime. The project covers research in system models, compile time and run time methods, and analysis and verification techniques. These tools will provide high-quality designs with improved designer productivity, while guaranteeing consistency with the initial requirements for adaptability and the final implementation.

Thus FAMOUS is a research project with an immediate industrial impact. Actually, it will make reconfigurable systems design easier and faster. The obtained tool in this project is expected to be used by both companies designers and academic researchers, especially for modern applications system specific design as smart camera, image and video processing, FAMOUS tools will be based on well established standards in design community. In fact, modeling will start from very high abstraction level using an extended version of MARTE. Simulation and synthesizable models will be obtained by automatic model to model transformations, using MDE approach. These techniques will contribute to shorten drastically time-to-market.

FAMOUS ended in December 2013. Its main result is a complete MDE tool for modeling, transforming and generating dynamically reconfigurable systems targeting Xilinx devices. This tool has been validated on a video processing application as a demonstrator.

INDES Project-Team (section vide)

PAREO Project-Team (section vide)

TASC Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Ligéro(AGIRA)

Participants: Xavier Lorca, Thierry Petit.

Title: **Ligéro**.

Duration: 2013.

Type: Regional research group

Teaching optimization project.

7.2. CPER

Participant: Charles Prud'Homme.

Title: CPER.

Duration: 2010-2014.

Type: Regional research group.

Budget: 250000 Euros.

Others partners: **EMN** (team **ATLANMOD**), **EMN** (team **ASCOLA**), **IRCCyN** (team **SLP**).

Develop, promote and build up an eco-system around free software in the Pays de la Loire region. The **TASC** team is involved in the maintenance and development of the free constraint programming platform **CHOCO**.

7.3. UNIT

Participants: Nicolas Beldiceanu, Eliane Vacheret.

Title: **UNIT**.

Duration: 2011-2013.

Type: Developing teaching material.

Budget: 5000 Euros.

Others partners: **EMN** (**CAPE**).

Pedagogical material and software for learning constraints programming for non experts (integrated within the global constraint catalog). The course will be available on line in spring 2014.

7.4. FUI SUSTAINS

Participants: Charlotte Truchet, Bruno Belin.

Title: SUSTAINS.

Duration: 2010-2015.

Type: FUI.

Budget: 151400 Euros.

Others partners: **Artefacto**, **Artelys**, **Areva TA**, **EPAMarne**, **LIMSI**.

The **SUSTAINS** project (*Constraint-based Prototyping of Urban Environments*) aims at building decision support system for city development planning with evaluation of energy impacts. The project is focussed on spatial allocation of typical units such as industrial areas, commercial areas and leaving areas with their respective appropriate infrastructure. Its integrates sustainability, transport and energy concerns.

7.5. ANR BOOLE

Participants: Vincent Armant, Jérémie Du Boisberranger, Xavier Lorca, Charlotte Truchet.

Title: **BOOLE**.

Duration: 2010-2013.

Type: open research program.

Budget: founding a PhD student and travels.

Others partners: **Univ. de Versailles Saint-Quentin**, **Univ. Caen**, **Univ. Paris 8**, **Univ. Aix-Marseille**, **Univ. Paris Nord**, **Univ. Paris 11**, **ENS Paris**.

Défi: Probabilistic method for combinatorial problems.

The work of **TASC** focuses on the use of probabilistic methods to avoid wakening systematically global constraints for nothing. The goal is to provide probabilistic models for the consistency of global constraints such as *alldifferent* or *nvalue*. We compute the probability of a constraint to be still consistent after fixing one of its variables and provide an approximation that can be computed in constant time. The PhD of J. du Boisberranger is co-supervised with **D. Gardy** from **Univ. de Versailles Saint-Quentin**.

7.6. ANR NetWMS2

Participants: Nicolas Beldiceanu, Gilles Chabert.

Title: Networked Warehouse Management Systems 2: packing with complex shapes.

Duration: 2011-2014.

Type: cosinus research program.

Budget: 189909 Euros.

Others partners: **KLS Optim** and **CONTRAINTES** (Inria Rocquencourt).

This project builds on the former European FP6 **Net-WMS** Strep project that has shown that constraint-based optimisation techniques can considerably improve industrial practice for box packing problems, while identifying hard instances that cannot be solved optimally, especially in industrial 3D packing problems with rotations, the needs for dealing with more complex shapes (e.g. wheels, silencers) involving continuous values. This project aims at generalizing the geometric kernel *geost* for handling non-overlapping constraints for complex two and three dimensional curved shapes as well as domain specific heuristics. This will be done within the continuous solver **IBEX**, where discrete variables will be added for handling polymorphism (i.e., the fact that an object can take one shape out of a finite set of given shapes). In 2013 a filtering algorithm has been devised in the case of objects described by nonlinear inequalities and is now under testing with the **Ibex** library. This work has been presented in a workshop on interval methods & geometry in **ENSTA Bretagne**.

7.7. ANR INFRA-JVM

Participants: Xavier Lorca, Charles Prud'Homme.

Title: Towards a Java Virtual Machine for pervasive computing.

Duration: 2011-2013.

Type: **new project**.

Budget: 78000 Euros.

Others partners: Univ. Paris 6 (**REGAL** team), **LaBRI** (**LSR** team), **IRISA** (**TRISKELL**).

The **INFRA-JVM** project will investigate how to enhance the design of Java virtual machines with new functionalities to better manage resources, namely resource reservation, scheduling policies, and resource optimization at the middleware level. **TASC** is concerned with this later aspect. The performance of **CHOCO** will be improved using the memory snapshot mechanism that will be developed.

7.8. EDF

Participants: Nicolas Beldiceanu, Helmut Simonis.

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 year project) is first to extract constraints from daily energy production temporal series issued from the 350 production plants of **EDF**, second to see how to use these constraints in order to reduce the combinatorial aspect of the daily production planning solving process. The work is based on the CP 2012 model seeker.

7.9. LabCom

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.

7.10. PHC Ulysses

Participants: Charlotte Truchet, Florian Richoux, Alejandro Reyes.

Title: Development and estimation analysis of massively parallel local search approaches to the k-medoids problem.

Duration: 2014.

Type: **new project**.

Budget: 2500 Euros.

Others partners: 4C (Cork, Ireland).

The goal of this project is to develop parallel local search techniques for solving large instances of the k-medoids problem, a location problem with several applications, in particular in optical fiber networks deployment.

7.11. ECOS Sud

Participant: Eric Monfroy.

Title: Auto-Evol (Autonomous Evolutionary Algorithms).

Duration: 2011-2013.

Budget: 15 KEuros per year for the project.

Others partners: LERIA (Angers, France), Univ. Austral de Chile (Chili), UTFSM (Valparaiso, Chili).

ESPRESSO Project-Team (section vide)

S4 Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.2. Bilateral Grants with Industry

TRIO Team (section vide)

AOSTE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Kalray MPPA256 experiments

As part of a larger collaborative programme between Inria and this company, new experimental machines equipped with Kalray MPPA256 manycore processor were provided to a small number of Inria teams. The processor itself consists of 16 processing clusters, each itself a 16-core processor (hence 256 cores altogether). The clusters are connected by an on-chip network, and the whole architecture (driven by a host, out-of-chip main CPU) may be programmed according to several computation models, some quite close from the MoCCs considered in our researches.

Part of this 10-month contract was meant to fund two internships, in our case on:

- The evaluation of performance (and most of all performance variability) of the various parts of the chip (in the Sophia Antipolis branch of the team). Results are discussed in section 6.5 .
- The evaluation of the possibility of code generation for the MPPA256 platform using the Lopht tool described in sections 5.4 ,6.6 .

7.1.2. Astrium/CNES PostDoc

Astrium Space Transportation (now part of Airbus Defence and Space) asked us if we could provide automatic methods for the design and implementation of embedded software and system/network configuration in an aerospace context. The objective is to reduce the design and validation costs (especially in case of system evolutions), while preserving an assurance level superior to that of the Ariane 5 flight program. We are exploring automation of the real-time allocation, scheduling, and code generation using the novel algorithms developed and implemented in the Lopht tool.

The post-doctoral position of Raul Gorcitz was funded on this contract.

7.1.3. Kontron CIFRE

This contract provides us means to partially support the PhD thesis of Mohamed Bergach (which is physically most of the time at Kontron Toulon). 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).

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

7. Bilateral Contracts and Grants with Industry

7.1. Qwant

Together with **Qwant**, the MuTant team is in the process of defining and developing the Antescofo accompaniment engines for the entertainment industries on various mobile terminals.

PARKAS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- Kalray 20K grant including the donation of an MPPA Developer workstation (with MPPA 256 accelerator) and support for a short-term research project (2 months of postdoc).
- Google Doctoral Fellowships of Tobias Grosser and Robin Morisset.

SPADES Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- With ST Microelectronics: CIFRE contract for the PhD of Vagelis Bebelis. This work is described in Section [6.2.6](#).
- With ARGOSIM SA: “Study and transfer contract” for the development by Bertrand Jeannet and the cession to ARGOSIM of the PolyCart library. PolyCart is a library for the manipulation of cartesian products of polyhedra and intervals.

FORMES Team (section vide)

SECSI Project-Team (section vide)

ABSTRACTION Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. License agreement

7.1.1.1. Astrée

In February 2009 was signed an exploitation license agreement between CNRS, École Normale Supérieure, and **AbsInt Angewandte Informatik GmbH** for the industrialization of the **ASTRÉE** analyzer. **ASTRÉE** is **commercially available** from **AbsInt** since January 2010. Continuous work goes on to adapt the **ASTRÉE** static analyzer to industrial needs, in particular for the automotive industry. Radhia Cousot is the scientific contact.

CELTIQUE Project-Team

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Project with FIME

Participants: Thomas Jensen, Frédéric Besson, David Pichardie, Delphine Demange, Pierre Vittet.

Static program analysis, Javacard, Certification, AFSCM

- Partner : **FIME**
- Period: Starting January 2012; ending June 2013

The FIME contract consists in an industrial transfer of the Sawja platform 4.2 adapted to analyse Javacard programs according to **AFSCM** (Association Française du Sans Contact Mobile) security guidelines. The rules specify syntactic constraints but also more semantics properties such as the absence of certain runtime exceptions. FIME aims at automating the process of validating that Javacard applications are conformant to the rules. The outcome of the project is the Jacal (JAVaCard AnaLyser) (4.3 which takes a binary Javacard application; performs static analysis and output statuses for the different rules. Pierre Vittet has recently been recruited by FIME and the operational deployment of Jacal is in progress.

DEDUCTEAM Exploratory Action (section vide)

GALLIUM Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. *The Caml Consortium*

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

The Caml Consortium is a formal structure where industrial and academic users of Caml 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 11 member companies:

- CEA
- Citrix
- Dassault Aviation
- Dassault Systèmes
- Esterel Technologies
- Jane Street
- LexiFi
- Microsoft
- Mylife.com
- 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.

7.1.2. *OCamlPro*

Participant: Fabrice Le Fessant.

Fabrice Le Fessant is consulting for OCamlPro, a SME that provides services and tools to companies wanting to use OCaml as their development language.

MARELLE Project-Team (section vide)

MEXICO Project-Team (section vide)

PARSIFAL Project-Team (section vide)

PL.R2 Project-Team (section vide)

SUMO Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

HiMa. The SUMO team was involved in the common research lab between Alcatel-Lucent Bell Labs France and Inria, through the High-Manageability team, co-headed by Pierre Peloso (Alcatel) and Éric Fabre. This joint team involved other Inria teams: Madynes and Mexico. In the last years of its existence, most of the activity of this joint team was redirected to the UniverSelf FP7 integrated project. Both the joint team and the project ended in 2013 (see the UniverSelf description for more details). This joint team supported two PhD students of SUMO, who defended their thesis in 2013: Aurore Junier (network calculus for early malfunction detection) and Carole Hounkonnou (self-diagnosis for large scale services and networks). Éric Fabre is member of the scientific board of the joint lab ALBLF-Inria, which is now entering in its second round of 5 year common teams.

TOCCATA Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. CIFRE contract with Adacore

Participants: Claude Marché [contact], Andrei Paskevich, Claire Dross.

Jointly with the thesis of C. Dross, supervised in collaboration with the Adacore company, we established a bilateral collaboration contract, that started in January 2012 for 3 years.

The aim is to strengthen the usability of the *Alt-Ergo* theorem prover in the context of the GnatProve environment for the verification of safety-critical Ada programs [85]. A focus is made on programs involving Ada containers [86].

7.2. Bilateral Grants with Industry

7.2.1. Intel Grant

Participants: Sylvain Conchon [contact], Alain Mebsout.

S. Conchon has obtained an academic grant by Intel corporation on the development of the Cubicle model checker. The goal of this project was to develop a new version of Cubicle with significantly improved model-checking power. This required innovative algorithmic enhancements to be implemented and evaluated.

VERIDIS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Project funded by EADS Foundation

Participants: Jingshu Chen, Marie Dufлот-Kremer, Pascal Fontaine, Stephan Merz.

This two-year project (2013/2014) funds our work on the analysis of real-time Java programs described in section 6.2 , and in particular 12 months of the salary of Jingshu Chen as a post-doctoral researcher. It is complemented by funds granted by Région Lorraine.

CARTE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

We are currently working with the consortium “malware.lu”.

CASSIS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Research Result Transfer

The BZ-Testing-Tools technology has been transferred to LEIRIOS Technologies, at the end of 2004. LEIRIOS changed its name into 2007 and is now called Smartesting. The partnership between the Cassis project and the R&D department of Smartesting, located at the TEMIS Scientific and Industrial area at Besançon, will be continued through (national and international) projects or with a new transfer protocol. F. Bouquet is scientific consultant of Smartesting.

7.2. Study of the electronic voting system of Voxaly

Participants: Stéphane Glondu, Véronique Cortier.

A 4-month contract has been signed between Caramel, Cassis and Voxaly, a French company who is proposing solutions for the organization of on-line elections. During several meetings, we discussed their current solution and proposed improvements to gradually add security features that get close to the academic standards.

COMETE Project-Team (section vide)

DICE Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Dice has bilateral contracts with three companies.

Worldline Worldline 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.

OrangeLabs We are finishing a joint work with OrangeLab on smart buildings and the management of home equipments. The project aims to provide a digital management layer for long living equipment that do not have network connexion for historical or technical reasons. The collaboration relies on a CIFRE partnership.

BullSA BullSA is producing and designing next generation Many-Core architecture. Although most of the time these calculators are used in real-time, closed environment such as military equipments, the dynamic, adaptability, and upgradable nature of systems is a real issue. We participate in a joint project to design a management layer for handling dynamic data flow application in a soft real-time context.

PRIVATICS Team

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Contracts with Industry

6.1.1. XDATA

Title: XDATA.

Type: FUI.

Duration: April 2013 - April 2015.

Coordinator: Data Publica

Others partners: Inria, Orange, EDF, LaPoste, Hurance, Cinequant, IMT.

See also: <http://www.xdata.fr/>.

Abstract: The X-data project is a “projet investissements d’avenir” on big data with Data Publica (leader), Orange, La Poste, EDF, Cinequant, Hurence and Inria (Indes, Privatics and Zenith) . The goal of the project is to develop a big data platform with various tools and services to integrate open data and partners’s private data for analyzing the location, density and consuming of individuals and organizations in terms of energy and services. In this project, the Zenith team leads the workpackage on data protection and anonymization.

PROSECCO Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Contract with Airbus (<http://www.airbus.com/>), on the modeling and verification of avionic security protocols. Participant: Bruno Blanchet. From October to December 2013.