Activity Report 2011

Section Contracts and Grants with Industry
ALGORITHMS, CERTIFICATION, AND CRYPTOGRAPHY
1. ALGORITHMS Project-Team ................................................. 5
2. ARENAIRE Project-Team ..................................................... 6
3. CARMEL Project-Team (section vide) .................................. 7
4. CASCADE Project-Team ...................................................... 8
5. GALAAD Project-Team (section vide) .................................. 10
6. GEOMETRICA Project-Team ............................................... 11
7. LFANT Project-Team .......................................................... 12
8. SALSA Project-Team .......................................................... 14
9. SECRET Project-Team ....................................................... 15
10. TANC Project-Team ......................................................... 16
11. VEGAS Project-Team (section vide) ................................... 17

ARCHITECTURE AND COMPILING
12. ALF Project-Team ............................................................ 18
13. CAIRN Project-Team ........................................................ 19
14. CAMUS Team (section vide) ............................................. 23
15. COMPSYS Project-Team ................................................... 24

EMBEDDED AND REAL TIME SYSTEMS
16. AOSTE Project-Team ....................................................... 25
17. DART Project-Team ........................................................ 26
18. ESPRESSO Project-Team .................................................. 30
19. LICIT Exploratory Action .................................................. 32
20. PARKAS Team ............................................................... 33
21. POP ART Project-Team ..................................................... 34
22. S4 Project-Team (section vide) ........................................ 35
23. TRIO Project-Team (section vide) ..................................... 36
24. VASY Project-Team ........................................................ 37
25. VERTECS Project-Team (section vide) ............................. 38

PROGRAMS, VERIFICATION AND PROOFS
26. ABSTRACTION Project-Team ............................................. 39
27. ATEAMS Project-Team .................................................... 41
28. CARTE Project-Team ....................................................... 42
29. CASSIS Project-Team ....................................................... 43
30. CELTIQUE Project-Team .................................................. 44
31. COMETE Project-Team (section vide) ............................... 46
32. CONTRAINTES Project-Team .......................................... 47
33. FORMES Team .............................................................. 48
34. GALLIUM Project-Team ................................................... 49
35. MARELLE Project-Team (section vide) ............................. 50
36. MEXICO Project-Team .................................................... 51
37. MOSCOVA Project-Team .................................................. 52
38. PAREO Project-Team (section vide) ................................................. 53
39. PARSIFAL Project-Team (section vide) ......................................... 54
40. PLR2 Project-Team ................................................................. 55
41. PROVAL Project-Team ............................................................. 56
42. SECSI Project-Team (section vide) ............................................. 57
43. TASC Project-Team ................................................................. 58
44. TYPICAL Project-Team (section vide) ........................................ 61
45. VERIDIS Team .................................................................... 62
6. Contracts and Grants with Industry

6.1. Contracts with Industry

The Algorithms Project and Waterloo Maple Inc. (WMI) have collaborated for many years based on reciprocal interests. Thanks to this collaboration, the company WMI considers Inria as a special partner and grants it a free license for all of its research units.

Our work on automating the derivation of formulæ for special functions is hosted and funded for 6 years (2007–2012) by the Microsoft Research - INRIA Joint Centre as one of its projects, called “Dynamic Dictionary of Mathematical Functions”.
7. Contracts and Grants with Industry

7.1. Contracts with Industry

One contract with STMicroelectronics and one contract with Kalray, in the context of two PhD CIFRE grants; see § 7.2.

7.2. Grants with Industry

7.2.1. STMicroelectronics CIFRE PhD Grant

Participants: Claude-Pierre Jeannerod, Jingyan Jourdan-Lu, Jean-Michel Muller.

Jingyan Jourdan-Lu is supported by a CIFRE PhD grant (from March 2009 to September 2012) from STMicroelectronics (Compilation Expertise Center, Grenoble) on the theme of floating-point arithmetic code generation and specialization for embedded processors. Advisors: Claude-Pierre Jeannerod and Jean-Michel Muller (Arénaire), Christophe Monat (STMicroelectronics). A contract between STMicroelectronics and INRIA (duration: 36 months; amount: 36,000 euros; signature: fall 2010) aims at supporting the developments done in the context of this PhD.

7.2.2. Mediacom Project with STMicroelectronics

Participants: Florent de Dinechin, Claude-Pierre Jeannerod, Jingyan Jourdan-Lu, Jean-Michel Muller, David Pfannholzer, Nathalie Revol.

We have been involved in Mediacom since September 1, 2009. Mediacom is a 40-month joint project with the Compiler Expertise Center (STMicroelectronics Grenoble) and INRIA project-teams Alchemy, Alf, and Compsys, and a Nano 2012 partner project. For Arénaire, it funds in particular the 3-year MEFI PhD grant of David Pfannholzer. The development this year is the generation of some elementary functions, focusing on the pre-processing (argument reduction, exception handling) and post-processing (argument reconstruction). Our long-term goal with this project is the design and implementation of a dynamic code generation tool, for numerical kernels typical of intensive mediaprocessing, and that could be integrated into production compilers.

7.2.3. STMicroelectronics CIFRE PhD Grant

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

7.2.4. Altera hardware donation

Altera donated to the team an FPGA-based acceleration card (Altera DK-DEV-4SGX530N) worth 8000 euros for the Table-Maker’s Dilemma acceleration project.
CARAMEL Project-Team (section vide)
6. Contracts and Grants with Industry

6.1. ANR Projects with Industrials

- **SAPHIR-II (Sécurité et Analyse des Primitives de Hachage Innovantes et Récents)**
  Security and analysis of innovating and recent hashing primitives.
  **Participants:** Charles Bouillaguet, Pierre-Alain Fouque, Jiqiang Lu, Christian Rechberger.
  From April 2009 to March 2013.

- **PACE: Pairings and Advances in Cryptology for E-cash.**
  **Participants:** Olivier Blazy, Pierre-Alain Fouque, David Pointcheval, Mehdi Tibouchi, Damien Vergnaud.
  From December 2007 to February 2012.
  Partners: France Telecom R&D, NXP, Gemalto, CNRS/LIX (INRIA/TANC), Univ. Caen, Cryptolog.
  This project aims at studying new properties of groups (similar to pairings, or variants), and then to exploit them in order to achieve more practical e-cash systems.

- **PAMPA: Password Authentication and Methods for Privacy and Anonymity.**
  **Participants:** Michel Ferreira Abdalla, Dario Fiore, David Pointcheval.
  From December 2007 to December 2011.
  Partners: EADS, Cryptolog.
  One of the goals of this project is to improve existing password-based techniques, not only by using a stronger security model but also by integrating one-time passwords (OTP). This could avoid for example having to trust the client machine, which seems hard to guarantee in practice due to the existence of numerous viruses, worms, and Trojan horses. Another extension of existing techniques is related to group applications, where we want to allow the establishment of secure multicast networks via password authentication. Several problems are specific to this scenario, such as dynamicity, robustness, and the random property of the session key, even in the presence of dishonest participants.
  Finally, the need for authentication is often a concern of service providers and not of users, who are usually more interested in anonymity, in order to protect their privacy. Thus, the second goal of this project is to combine authentication methods with techniques for anonymity in order to address the different concerns of each party. However, anonymity is frequently associated with fraud, without any possible pursuit. Fortunately, cryptography makes it possible to provide conditional anonymity, which can be revoked by a judge whenever necessary. This is the type of anonymity that we will privilege.

- **BEST: Broadcast Encryption for Secure Telecommunications.**
  **Participants:** Duong Hieu Phan, David Pointcheval, Mario Strefler.
  From December 2009 to November 2013.
  This project aims at studying broadcast encryption and traitor tracing, with applications to the Pay-TV and geolocalisation services.
- **PRINCE: Proven Resilience against Information leakage in Cryptographic Engineering.**
  
  **Participants:** Michel Ferreira Abdalla, Bruno Blanchet, Dario Fiore, David Pointcheval.
  
  From December 2010 to November 2014.
  
  Partners: UVSQ, Oberthur Technologies, Ingenico, Gemalto, Tranef.
  
  We aim to undertake research in the field of leakage-resilient cryptography with a practical point of view. Our goal is to design efficient leakage-resistant cryptographic algorithms and invent new countermeasures for non-leakage-resistant cryptographic standards. These outcomes shall realize a provable level of security against side-channel attacks and come with a formally verified implementation. For this every practical aspect of the secure implementation of cryptographic schemes must be taken into account, ranging from the high-level security protocols to the cryptographic algorithms and from these algorithms to their implementation on specific devices which hardware design may feature different leakage models.

6.2. ANR Projects within Academics

- **ProSe: Security protocols : formal model, computational model, and implementations.**
  
  **Participants:** Bruno Blanchet, David Cadé, Miriam Paiola, David Pointcheval.
  
  From December 2010 to November 2014.
  
  Partners: ENS Cachan-INRIA/Secsi, LORIA-INRIA/Cassis, Verimag.
  
  The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the symbolic level, in which messages are terms; the computational level, in which messages are bitstrings; the implementation level: the program itself.
GALAAD Project-Team (section vide)
7. Contracts and Grants with Industry

7.1. Geometry Factory

The initial development phase of the CGAL library has been made by a European consortium. In order to achieve the transfer and diffusion of CGAL in the industry, a company called GEOMETRY FACTORY has been founded in January 2003 by Andreas Fabri (http://www.geometryfactory.com).

The goal of this company is to pursue the development of the library and to offer services in connection with CGAL (maintenance, support, teaching, advice). GEOMETRY FACTORY is a link between the researchers from the computational geometry community and the industrial users.

It offers licenses to interested companies, and provides support. There are contracts in various domains such as CAD/CAM, medical applications, GIS, computer vision...

GEOMETRY FACTORY is keeping close contacts with the original consortium members, and in particular with GEOMETRICA.

In 2011, GEOMETRY FACTORY had the following new customers for CGAL packages developed by GEOMETRICA: Acute3D (3D Delaunay, France), Ansys (2D Circular Kernel, CAD, USA), Autodesk (Poisson Surface reconstruction, CAD, USA), Esri (AABB Tree, GIS, USA), ExxonMobil (3D Delaunay, oil, USA), Halliburton (Poisson Surface reconstruction, oil, USA), Metria (2D Delaunay, GIS, Spain), Petrobras (2D Mesh, Surface mesher, Segment Voronoi diagram, oil, Brasil), Petroglyphgames (2D Constrained Delaunay, games, USA), Zimmer (Poisson Surface reconstruction, medical, Canada).

Moreover, research licenses (in-house research usage for all of CGAL) have been purchased by: Geovariances (petrol, France), Siemens Corporate Research (medical, USA), Spot Image (GIS, France), IGN (GIS, France), Kappa Engineering (oil, Germany), MPI Metal Research (Germany).
7. Contracts and Grants with Industry

7.1. Industrial ANR PACE

Participants: Andreas Enge, Jérôme Milan.

https://pace.rd.francetelecom.com/

The PACE project unites researchers of France Télécom, Gemalto, NXP, Cryptolog International, the INRIA project teams CASCADE and LFANT and University of Caen. It deals with electronic commerce and more precisely with electronic cash systems. Electronic cash refers to money exchanged electronically, with the aim of emulating paper money and its traditional properties and use cases, such as the anonymity of users during spending. The goal of PACE is to use the new and powerful tool of bilinear pairings on algebraic curves to solve remaining open problems in electronic cash, such as the strong unforgeability of money and the strong unlinkability of transactions, which would allow users to conveniently be anonymous and untraceable. It also studies some cryptographic tools that are useful in the design of e-cash systems.

7.2. DGA

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

- Duration: two years, 2011–2012
- Scientific coordinator: K. Balabas
- Topics covered: index calculus and discrete logarithms, fast arithmetic for polynomials, pairings and cryptography, algorithmics of the Langlands programme

7.3. Thèse cifre

Participants: Karim Belabas, Vincent Verneuil.

Vincent Verneuil, co-directed with B. Feix (Inside Contactless) and C. Clavier (Université de Limoges), works at Inside Contactless on elliptic curve cryptography, with an emphasis on embedded systems and side-channel attacks.

7.4. National Initiatives

7.4.1. ANR AlgoL: Algorithmics of $L$-functions

Participants: Bill Allombert, Karim Belabas, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Pascal Molin.

http://www.math.u-bordeaux1.fr/~belabas/algol/index.html

The ALGO-L project comprises research teams in Bordeaux, Montpellier, Lyon, Toulouse and Besançon. It studies the so-called $L$-functions in number theory from an algorithmic and experimental point of view. $L$-functions encode delicate arithmetic information, and crucial arithmetic conjectures revolve around them: Riemann Hypotheses, Birch and Swinnerton-Dyer conjecture, Stark conjectures, Bloch-Kato conjectures, etc.

Most of current number theory conjectures originate from (usually mechanised) computations, and have been thoroughly checked numerically. $L$-functions and their special values are no exception, but available tools and actual computations become increasingly scarce as one goes further away from Dirichlet $L$-functions. We develop theoretical algorithms and practical tools to study and experiment with (suitable classes of) complex or $p$-adic $L$-functions, their coefficients, special or general values, and zeroes. For instance, it is not known whether $K$-theoretic invariants conjecturally attached to special values are computable in any reasonable complexity model. On the other hand, special values are often readily computed and sometimes provide, albeit conjecturally, the only concrete handle on said invariants.
New theoretical results are translated into new or more efficient functions in the PARI/GP system.

7.5. European Initiatives

7.5.1. Collaborations in European Programs, except FP7

Program: Erasmus Mundus
Project acronym: ALGANT
Project title: ALgebra, Geometry and Number Theory
Duration: 09/2004–
Coordinator: University Bordeaux 1
Other partners: University Leiden (Netherlands), University Milano (Italy), University Padova (Italy), University Paris-Sud (France), Chennai Mathematical Institute (India), Concordia University (Canada), Stellenbosch University (South Africa)
Abstract: Joint master and doctoral programme; the PhD theses of Athanasios Angelakis and Julio Brau are co-supervised by P. Stevenhagen (Leiden) and K. Belabas

7.6. International Initiatives

7.6.1. Visits of International Scientists

The following researchers have visited the LFANT team:

- Christophe Ritzenthaler, Luminy, Marseille, February 23–25
- Bernadette Perrin-Riou, Université d’Orsay, March 4–18 and June 10–17
- Vanessa Vitse, Université de Versailles–St.-Quentin-en-Yvelines, April 13–14
- Jérémy Le Borgne, University of Rennes, April 27–28
- Andy Novocin, ÉNS Lyon and INRIA project-team ARÉNAIRE, May 4–5
- Lassina Dembelé, University of Warwick, May 18–19
- Jean-François Biasse, University of Calgary, May 25–26
- David Lubicz, Université de Rennes, July 18–22
- Eduardo Friedman, Universidad de Chile, October 3–21
- Michael Rubinstein, University of Waterloo, October 3–7
- Tony Ezone, Université de Franceville, Gabon, December 2011–January 2012
7. Contracts and Grants with Industry

7.1. Contract with Thalès

Participants: J.-C. Faugère [contact], G. Renault, C. Goyet.

The goal of this contract (including a CIFRE PhD grant) is to mix side channel attacks (DPA) and algebraic cryptanalysis.
6. Contracts and Grants with Industry

6.1. Grants with Industry

- **Gemalto** (01/10 → 12/12)
  
  *CIFRE grant for Christina Boura.*
7. Contracts and Grants with Industry

7.1. Contracts with Industry

- A GEMPLUS contract corresponds to É. Brier’s thesis on the use of (hyper-)elliptic curves in cryptology.
- D. Augot, with Christine Eisenbess, is in discussion with MassiveRand, an SME providing random bits at high rate, in order to provide Rabin’s HyperEncryption, which is provably secure.
VEGAS Project-Team (section vide)
7. Contracts and Grants with Industry

7.1. IBM Faculty award

Participant: André Seznec.

The research on Phase Change Memory and security has been partially funded by a 2010 IBM faculty award attributed to André Seznec.

7.2. Nano2012 Mediacom

Participants: Erven Rohou, David Yuste.

Mediacom is a Nano2012 project (Ministry of Industry, INRIA, STMicroelectronics). This project proposes to extend the application domain of virtualization and to combine it with split-compilation, in the context of homogeneous and heterogeneous multicore processors. The goal is to move the compilation complexity from the JIT compiler to the static compilation pass. This would enable very aggressive compilation techniques on embedded systems, such as iterative compilation, polyhedral analysis, or auto-vectorization and auto-parallelization.
7. Contracts and Grants with Industry


Participants: Sébastien Pillement, Arnaud Tisserand, Philippe Quémerais.

ARDyT (in french: Architecture Reconfigurable Dynamiquement Tolérante aux fautes) is a project on a Reliable and Reconfigurable Dynamic Architecture. It involves IRISA-Cairn (Lannion), Lab-STICC (Lorient), LIEN (Nancy) and ATMEL. The purpose of the ARDyT project is to provide a complete environment for the design of a fault tolerant and self-adaptable platform. Then, a platform architecture, its programming environment and management methodologies for diagnosis, testability and reliability have to be defined and implemented. The considered techniques are exempt from the use of hardened components for terrestrial and aeronautics applications for the design of low-cost solutions. The ARDyT platform will provide a European alternative to import ITAR constraints for fault-tolerant reconfigurable architectures. For more details see http://ardyt.irisa.fr.


Participants: Emmanuel Casseau, Steven Derrien, Sébastien Pillement.

COMPA (model oriented design of embedded and adaptive multiprocessor) is a project which involves Cairn, IETR (Institut d'Electronique et de Télécommunications de Rennes), Lab-STICC (University of Bretagne Sud), CAPS Entreprise, Modae Technologies and Texas Instruments. The goal of the project is to design adaptive multiprocessor embedded systems from dataflow models. Reconfigurable video coding (RVC) standard will be targeted as application use case. We will then more specifically focus on the use of the portable and platform-independent RVC-CAL language to describe the applications. We will propose transformations in order to refine, optimize and translate the application model into software and hardware components. Task mapping, instructions and processor allocation, and constrained scheduling will also be investigated for runtime execution and reconfiguration.

7.3. ANR Ingénierie Numérique et Sécurité - DEFIS (2011-2015)

Participants: Olivier Sentieys, Daniel Menard, Romuald Rocher, Nicolas Simon.

DEFIS (Design of fixed-point embedded systems) is a project which involves Cairn, LIP6 (University of Paris VI), LIRMM (University of Perpignan), CEA LIST, Thales, Inpixal. The main objectives of the project are to propose new approaches to improve the efficiency of the floating-point to fixed-point conversion process and to provide a complete design flow for fixed-point refinement of complex applications. This infrastructure will reduce the time-to-market by automating the fixed-point conversion and by mastering the trade-off between application quality and implementation cost. Moreover, this flow will guarantee and validate the numerical behavior of the resulting implementation. The proposed infrastructure will be validated on two real applications provided by the industrial partners. For more details see http://defis.lip6.fr.

7.4. ANR ARPEGE - GRECO (2010-2013)

Participants: Olivier Sentieys, Olivier Berder, Arnaud Carer, Romain Fontaine, Trong-Nhan Le.
Sensor network technologies and the increase efficiency of photovoltaic cells show that it is possible to reach communicating objects solutions with low enough power consumption to foresee the possibility of developing autonomous objects. Greco (GREen wireless Communicating Objects) is a project on the design of autonomous communicating object platforms (i.e. self-powered sensor networks). The aim is to optimize the power consumption based on (i) a modeling of the performances and power of the required blocks (RF front-end, converters, modem, peripherals, digital architecture, OS, software, power generator, battery, etc.) (ii) heterogeneous simulation models and tools, and (iii) the use of a real-time global “Power Manager”. The final validation will be performed on various case studies: a monitoring system and an audio communication between firemen. A HW/SW prototyping (based on an CAIRN’s PowWow platform with energy harvesting) and a simulation associating a precise modeling (virtual platform) of an object inserted in a network simulator-like environment will be developed as demonstrators. Greco involves Thales, INRIA/CAIRN, CEA List, CEA Leti, Im2nP, LEAT, Insight-SiP. For more details see http://greco.irisa.fr.

7.5. Images and Networks competitiveness cluster - 100GFlex project (2010-2013)

Participants: Olivier Sentieys, Arnaud Carer, Remi Pallas, Pascal Scalart.

Speed and flexibility are quickly increasing in the metropolitan networks. In this context, 100GFLEX studies the relevance of a new transmission scheme: the multiband optical OFDM at very-high rates (up to 100 Gbits/s). In this project we will study efficient algorithms (e.g. synchronization) and high-speed architectures for the digital signal processing of the optical transceivers. Due to the high rate of analog signals (sampling at more than 10Gsample/s), synchronizing and processing is real challenge. 100Gflex involves Mitsubishi Electric R&D Center Europe, Institut Télécom, Ekinops, France Télécom, Yenista Optics, Foton and Cairn.

7.6. NANO2012 Program - S2S4HLS (2008-2012)

Participants: Emmanuel Casseau, Steven Derrien, Daniel Menard, Olivier Sentieys, Loic Cloatre, Amit Kumar, Antoine Morvan, Chenglong Xiao, Jean-Charles Naud.

High-level synthesis (HLS) tools start to be used for industrial designs. HLS is analogous to software compilation transposed to the hardware domain. From an algorithmic behavior of the specification, HLS tools automate the design process and generate a register transfer level RTL architecture taking account of user-specified constraints. However, design performance still depends on designer’s skill to write the appropriate source code. The S2S4HLS (Source-to-Source for High-Level Synthesis) project intends to process source code transformations to guide synthesis hence leading to more efficient designs, and aims at providing a toolbox for automatic C code source-to-source transformations. The project is focused on three complementary goals to push the limits of existing HLS tools: loop transformations for performance optimization and a better resource usage, automatic floating-point to fixed-point conversion and synthesis of multi-mode architectures. S2S4HLS is organized into three sub-projects targeting these three objectives. The project is in close collaboration with ST Microelectronics and Compys team at Inria Rhône-Alpes, within the overall INRIA-ST partnership agreement. It is financed by the Ministry of Industry in the Nano2012 program. Cairn is responsible of the project and involved in the three workpackages.

7.7. NANO2012 Program - RecMotifs (2008-2012)

Participants: François Charot, Antoine Floch, Christophe Wolinski.

The RecMotifs project aims at the generation of application specific extensions targeting the STxP70 processor from STMicroelectronics. Cairn will study advanced technologies algorithms for graph matching and graph merging together with constraints programming methods. The project is in close collaboration with ST Microelectronics within the overall INRIA-ST partnership agreement. It is financed by the Ministry of Industry in the Nano2012 program.
7.8. ANR Architectures du Futur Open-People (2009-2012)

Participants: Daniel Chillet, Robin Bonamy, Olivier Sentieys.

The Open-People (Open Power and Energy Optimization PLatform and Estimator) project aims at defining a complete platform for power estimation and optimization. The platform will be composed of hardware boards to support measurements for the applications. End-users will be able to upload their applications through a web portal, and to control the power measurements of the execution of their applications on a specific electronic board. The Open-People project will also propose a complete power component model library which allows end-users to estimate the power consumption of some parts of the applications without making measurements. This will allow to quickly evaluate the different design choices regarding the power consumption. Finally, through the web portal http://www.open-people.fr , Open-People will propose software tools to apply power optimizations. In this project, CAIRN team will develop power model for FPGA components using dynamic reconfiguration. Open-People involves LabSticc (Lorient), Trio (Nancy), CAIRN (Rennes/Lannion) and Dart (Lille/Valenciennes) teams from Inria, Leat at Nice, Thales (Colombes) and InPixal (Rennes). Cairn is in charge of power models and optimization for reconfigurable architectures.

7.9. ANR BioWiC (2009-2011)

Participants: Steven Derrien, Naeem Abbas, Patrice Quinton.

The increasing flow of genomic data provided by the steadily improvement of new biotechnologies cannot be now efficiently exploited without a systematic in silico analysis. Data need to be filtered, curated, classified, annotated, validated, etc., to be actively used in a discovery process. The design of such complex pipeline of processing stages is known to be an extremely tedious task as their designers have to deal with both specification and implementation issues. Indeed, the execution time of such workflows is very often a bottleneck as huge amount of data has to be processed. Therefore, the goal of the BioWiC (Bioinformatics Workflows for Intensive Computation) project is twofold:

- Reducing the design time of complex bioinformatics pipelines by providing a domain specific workflow environment;
- Reducing the execution time of these workflows through the use of parallel execution on GPU, FGPA and clusters of PC whenever possible.

The ANR BioWic project is funded for 3 years, and involves several institutions (INRA-MIG, Ouest Genopole, CAIRN and Symbiose project-teams at INRIA) and Universities (Eliaus Laboratory at Université de Perpignan). For more details see http://biowic.inria.fr . CAIRN will provide a framework for helping semi-automatic generation of flexible IP cores, by widening the scope typical design constraints so as to integrate communication and data reuse optimizations between the host and the hardware accelerator.

7.10. ANR Architectures du Futur - CIFAER (2008-2011)

Participants: Sébastien Pillement, Manh Pham, Olivier Sentieys.

In various application domains, emerging requirements lead to the definition of new architectures for electronic embedded systems. In the automotive context, investigated solutions correspond to network of processing elements, distributed in the vehicle. In this context, the research activity considered in the CIFAER (Flexible Intra-Vehicule Communications and Embedded Reconfigurable Architectures) project is the definition of an innovative embedded architecture, based on general purpose processor with reconfigurable processing areas and on the use of adaptable interfaces (radio and powerline communications). Efficient software layers in the associated operating system will be investigated to enable new services as dynamic reconfiguration and task migration for error tolerance. CIFAER involves Irisa, IETR Rennes, Ireeva Nantes, Atmel and Geensys. CAIRN will propose and develop the dynamically reconfigurable platform used a the test vehicle of the project. This platform will include fault-tolerant mechanisms for error mitigation.
7.11. ANR Architectures du Futur - FOSFOR (2008-2011)

Participants: Daniel Chillet, Sébastien Pillement, Manh Pham, Ludovic Devaux, Didier Demigny.

The Fosfor (Flexible Operating System FOr Reconfigurable platform) project aims at reconsidering the structure of the RTOS which is generally implemented in software, centralized, and static, by proposing a distributed RTOS with homogeneous interface from the application point of view. We propose to exploit dynamic and partial reconfiguration of the reconfigurable SoC. In this context, the tasks are statically or dynamically deployed (i.e. instantiated) on software units (general processors) or hardware units (reconfigurable areas). Flexibility of the OS will be achieved thanks to virtualization mechanisms of OS services, such that the tasks of the application are executed and communicate without prior knowledge of their assignment to software or hardware. FOSFOR involves Irisa, LEAT Nice, ETIS Cergy, Xilinx and Thales. CAIRN will propose and include in the FOSFOR OS a flexible communication infrastructure and its control management.
CAMUS Team (section vide)
7. Contracts and Grants with Industry

7.1. MEDIACOM: Nano2012 Project with STMicroelectronics on SSA, Register Allocation, and JIT Compilation

**Participants:** Benoît Boissinot, Florian Brandner, Quentin Colombet, Alain Darte, Fabrice Rastello.

This contract has started in September 2009 as part of the funding mechanism Nano2012. This is the continuation of the successful previous project Sceptre with STMicroelectronics, which ended in December 2009. This new project concerns both aggressive optimizations and the application of the previously-developed techniques to JIT compilation. Related activities are described in Sections 6.2 to 6.7.

Unfortunately, due to a unilateral decision of the government, all fundings related to Nano2012 have been cancelled, or at least frozen, in 2011. The salary of PhD students (such as Quentin Colombet) was guaranteed by contract but neither the salary of engineers and post-docs, nor the regular budget. Thanks to Inria who covered his salary, we succeeded to keep Florian Brandner until October 2011. However, the whole travelling budget was cut. Mediacom survived and will continue, as planned, until the end of 2012, but in a less ambitious format.

7.2. S2S4HLS: Nano2012 Project with STMicroelectronics on Source-to-Source Transformations for High-Level Synthesis

**Participants:** Christophe Alias, Alain Darte, Paul Feautrier, Alexandru Plesco.

This contract has started in January 2009 as part of the funding mechanism Nano2012. This is a joint project with the Cairn Inria project-team and STMicroelectronics, whose goal is the study and development of source-to-source program transformations, in particular loop transformations, that are worth applying on top of HLS tools. This includes restructuring transformations, program analysis, memory optimizations and array reshaping, etc. Some of the work presented in Section 6.9 is part of this project.

The fact that Nano2012 was cancelled or only frozen (depending on the day) forced us to quit the project. We were indeed about to hire a post-doc on this topic and could not do it due to this unexpected governmental decision. This contract was therefore closed in 2011.

7.3. Creation of the Start-Up Zettice

Following his PhD, Alexandru Plesco initiated a start-up on high-level synthesis for FPGAs, named Zettice, and the use and extension of tools/techniques developed in Compsys (for high-level code transformations) and Arénaire (for the development of pipelined operators). The results described in Sections 5.7, 6.9, 6.10, and 6.11 are directly linked to this effort.

The incubation of Zettice is supported by Crealys, the “Région Rhône-Alpes”, and Inria: Alexandru Plesco is “ingénieur technologie et innovation” (ITI) since October 2011. Christophe Alias is in charge of the collaboration between Compsys and Zettice.
7. Contracts and Grants with Industry

7.1. ID/TL-M project with ST Microelectronics

Participants: Charles André, Robert de Simone, Benoît Ferrero, Jean-François Le Tallec.

ID/TL-M is a project launched as part of the larger NANO 2012 programme conducted by ST Microelectronics in Rhône-Alpes. Its main goal is to study the potential use of model-driven engineering techniques (MDE) for Electronic System-Level Design (ESL) of Systems-on-Chip (SoC).

In particular we focused this year on the relations and connexions between UML MARTE profile and the other standard IP-XACT, itself introduced as dedicated Architecture Description Language (ADL) for easy assembly of IP hardware components. One advantage here of MARTE in our view is that it is meant to be extendable to comprise Non-Functional Property annotations, such as consumption for low-power, in a much more open and larger setting as the extensions under way at Accelera (the IP-XACT standardisation body which recently merged with OSCI, the Open SystemC Initiative).

The direct collaboration in ID/TL-M allows implementations of tools and methods whose general descriptions are somehow shared with the neighboring ANR project HeLP (see below). Nevertheless, due to external reasons of political nature, funding of the general nano2012 programme was halted in 2011, and this project was consequently put on stand-by.

7.2. Thales ARCADIA/Melody

Participants: Frédéric Mallet, Robert de Simone.

During the course of the ARTEMIS CESAR project, we exchanged views with partners at Thales on potential methodologies based on Model-Driven Engineering for Embedded Systems. These considerations were mostly aimed at the support with tools of the various allocation and refinement steps in a V-cycle process, considering joint software and hardware design. Subsequently we were invited to conduct an evaluation survey and expert consulting on their internal MDE development project, the ARCADIA methodology (supported by the Melody tool environment).

The work included identification of potential ambiguous points in the representation models, followed by the definition of a relevant set of questions regarding possible interpretations. This form was then submitted to a panel of development engineers inside the company. Their return answers were analyzed by us, jointly with the promoters of the methodology inside Thales. Recommendations for improvements followed.

This job was conducted under Non-Disclosure Agreement (as the methodology remains proprietary, and is not part of CESAR tool deliverables). It led to a Grant agreement from this company to our team.
6. Contracts and Grants with Industry

6.1. ANR Famous

Collaboration with INRIA Rhône Aplies, Université de Bretagne Sud, Université de Bourgogne, SME SODIUS

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 is a basic research project. In fact, most of partners are academic, and its main objective is to explore novel design methodologies and target modern embedded systems architectures. FAMOUS project is funded by french Agence Nationale de la Recherche (ANR). It has also been labeled by Media & Network cluster in 2009. The involved resources reach 408 person-month, from five partners: the public research labs LIFL INRIA (Lille), LabSTICC (Lorient), INRIA Rhône-Alpes (Grenoble), LE2I University of Bourgogne (Dijon) and the SME company Sodius SAS (Nantes). It has started on December 2009, and it will last 48 months.

6.2. The ANR Open-People project

**Partners:** Université de Bretagne Sud (UBS) Lab-STICC, INRIA Nancy Grand Est, INRIA Lille Nord Europe, Université de Rennes 1 (UR1), Université de Nice Sophia Antipolis (UNSA), THALES Communications (Comolmes), InPixal (Rennes)

The Open-PEOPLE (Open Power and Energy Optimization PLatform and Estimator project is a national project funded by the ANR (Agence Nationale de la Recherche), the French National Research Agency. The objective of Open-PEOPLE is to provide a platform for estimating and optimizing the power and energy consumptions. Users will be able to estimate the consumption of an application deployed on a hardware architecture chosen in a set of parametric reference architectures. The components used in the targeted architecture will be chosen in a library of hardware and software components. Some of these components will be parametric (such as reconfigurable processors or ASIP) to further enlarge the design space for exploration. The library will be extensible; users will have the possibility to add new components, according to the evolution of both applications and technology. Open-PEOPLE is definitely an open project. The software platform for conducting estimation and optimization, will be accessible through an Internet portal. This software platform will be coupled to an automated hardware platform for physical measurements. The measurements needed to build models for new components to be added in the library will be remotely controlled through the software platform. A library of benchmarks will be proposed, to help building models for new components and architectures.

6.3. INRIA Euromed 3+3

This project, involves the DaRT team of Inria Lille Nord-Europe, Ecole Supérieur d’Informatique d’Alger, Université de Monastir and University of Las Palmas. It aims at studying efficient architectures for modern embedded system. Thus, we defined, modeled and designed NoC based systems using MDE approaches. Image processing applications (H264) modeling and their efficient mapping on the developed architectures, constitute also a key issue in this project.
6.4. STIC INRIA - Tunisia program

We have been co-advising two PhD students and several Master students in collaboration with the team of Pr. Mohamed Abid at CES-ENIS in Sfax and Pr. Abderrazak JEMAI at INSAT in Tunis. This collaboration is supported by the STIC Inria-Tunisia program, which aims at promoting the design of metamodels, transformation tools and techniques for the implementation of reconfigurable systems-on-chip. The resulting co-design environment will be validated on embedded systems dedicated to security in automobile, and more specifically in the design of cruise control systems integrating anti-collision radars.

Several successful student exchanges have been realized since 2006 between DaRT, INSAT and CES-ENIS.

6.5. Contrat STIC INRIA - Algérie

This project, involving the DaRT and Dolphin team of Inria Lille Nord-Europe, and the Laboratoire d’Informatique d’Oran of the university of Oran, Algeria aims at studying the architecture exploration phase of embedded system design. It has started in 2011 and should end in 2012. It funds exchanges between the two countries. A first “magistère” has been defended in 2011 (Abdelkader Aroui).

6.6. Nano 2012 ID-TLM

This project, involves the DaRT team of Inria Lille Nord-Europe, the Aoste team of Inria Sophia-Antipolis Méditerranée and ST Microelectronics studies formal models of computation and model driven engineering to help design embedded systems. It has started in 2009 for four years.

6.7. Collaboration with CEA List

A PhD thesis (Asma Charfi) is co-advised between our team and the CEA List on optimized code generation from MARTE models. The idea is that some information is lost when the code is generated from a high level model to code. The compiler then tries to find back this lost information to optimize the code. If these optimizations were taken care of at model level, the compiler would have a simplified task to do and we could expect improved performance. This thesis has been defended on December 2011.

A new PhD thesis (Amine El Kouhen) is co-advised between our team and the CEA List on the adaptation of UML Tools to the domain and to the design process. The idea is to provide customers with a UML tool adapted to its work, here, the design of embedded system. The tool customization is done with the help of models or profiles.

DaRT and the CEA List also collaborate on the Papyrus UML project.

6.8. Collaboration with SME Ecreall

The transformation chain used in the DaRT Embedded System modeling approach involves several models automatically generated. This work aims to be able to modify directly ones of the generated model, and let the modification be propagated in both direction to other models of the chain. Not all changes can be propagated, a part of this work will be to identify changes that can be propagated. This work is done in collaboration with Ecreall (http://www.ecreall.com/), a small company involved in developing web collaborative portals. The first step of the work was to align MDE practice of the company to the DaRT practice. A first transformation chain has been developed. It allows to model collaborative portals, transform it in intermediate models, and then generate the code for a targeted technology (dolmen). This work will reuse results from the Traceability.
6.9. Collaboration EADS IW, and Eurocopter

The subject deals with dynamic reconfigurable system design for avionic test applications. It is motivated by the need of methodologies and tools for the design of high-performance applications on dynamic reconfigurable computing systems. A complete methodology takes the reconfigurability of the hardware as an essential design concept and proposes the necessary mechanisms to fully exploit those capabilities at runtime. A set of tools must provide high-quality designs with improved designer productivity, which guarantees consistency with the initial requirements for adaptability and for the final implementation. This methodology allows designers to easily implement a system specification on a platform that includes general purpose processors dynamically combined with multiple accelerators running on an FPGA.

6.10. International Initiatives

6.10.1. Collaboration with Colombia

The collaboration with the Universidad de los Andes in Bogota and more precisely the team of software engineering directed by Rubby Casallas is still running. Anne Etien is co-supervising the master thesis of David Mendez. Furthermore, common works also with the University of York about the themes of model driven engineering and evolution are in course.

6.10.2. Collaboration with Romania

We collaborate with the university of Iași (Romania) on the formal definition of DSMLs in the K framework.

6.10.3. Visits of International Scientists

BADRI NARAYANAN RAVI (from Jan 2011 until Jun 2011)
Subject: Environnement unifié en vue de l’estimation et l’optimisation de la consommation de puissance des systèmes embarqués mobiles
Institution: Chalmers University of Technology (Sweden)

6.11. European Initiatives

6.11.1. Collaboration with Belgium

The collaboration with the Université Libre de Bruxelles, (flemish part (VUB)) and more specifically the Software Languages Lab is still running. It concerns the chaining of localized transformations.

6.11.2. Collaboration with England

The collaboration initiate the previous year with the Sosym team of the University of York in England is continuing. We are working together on model driven engineering, evolution and genericity. Some papers have been conjointly written and are under submission.

6.11.3. Participation In European Programs

Pierre Boulet is a member of the HiPEAC network of excellence.


6.12.1. Within Inria

We collaborate with colleagues within Inria with:

- the Triskell team at Inria Rennes-Bretagne Atlantique) on the analysis of DSMLs and on the formal definition of Kermeta.
- the Compsys team at Inria Grenoble Rhône-Alpes /Lyon on termination, and more generally on analysis of general C programs.
6.12.2. Other National Collaborations

We collaborate with David Monniaux (Verimag, Grenoble) on improving the global precision of fixpoint computations, via the use of SMT solving.

We also collaborate with the L2EP (Université de Lille1) inside the research pole MEDEE, especially in the first action: industrialization of Code_CARMEL. Code_CARMEL is a software for electromagnetic fields simulations.

We collaborate with Xavier Blanc (LaBri) on the definition of constraints for chaining model transformations.
6. Contracts and Grants with Industry

6.1. Artemisia project CESAR

Participants: Huafeng Yu, An Phung-Khac, Yue Ma, Loïc Besnard, Thierry Gautier, Jean-Pierre Talpin.

In the context of CESAR, we have participated to the sub-project 3 demonstrator in order to demonstrate the usability of Polychrony as a co-simulation tool within the reference technology platform of the project, to which its open-source release has been integrated. The case-study, implemented in collaboration with Airbus and IRIT, consists of co-modeling the doors management system of an Airbus A350 by merging its architecture description, specified with AADL, with its behavioral description, specified with Simulink.

In this case-study, we demonstrate that the Polychrony toolset can effectively serve as a modeling infrastructure to compositionally assemble, compile and verify heterogeneous specifications (AADL and Simulink). Our case study will cover code generation for real-time simulation and test as well as formal verification both at system-level and in a GALS framework. Based on that case study, we aim at developing further modular code-generation services, real-time simulation, test and performance evaluation, formal verification as well as the validation of the generated concurrent and distributed code.

6.2. ITEA2 project OPEES

Participants: Thierry Gautier, Yue Ma, Jean-Pierre Talpin.

The ITEA2 project OPEES is the continuation of the ANR project OPENEMBEDD to provide an open-source platform for embedded software design. Its outcome will outlive the duration of the project as it is in the process of becoming an Industrial Working Group of the Eclipse consortium, Polarsys, whose goal will be to host and maintain the proposed open-source platform and guarantee its long-term availability.

The mission of Opees is to build a community able to ensure durability of innovative engineering technologies in the domain of critical software-intensive embedded systems. Its main objectives are to secure the industrial strategy, improve their competitiveness and develop the European software industry.

Our goal in the OPEES project is to deliver the Polychrony toolset on the Polarsys platform as an infrastructure for the co-simulation and co-verification of embedded architectures. To this end, Polychrony is currently under a quality assessment performed in collaboration with CS.

6.3. ANR project VERISYNC

Participants: Loïc Besnard, Chan Ngo, Jean-Pierre Talpin.

The Verisync project aims at improving the safety and reliability assessment of code produced for embedded software using synchronous programming environments developed under the paradigm of Model Driven Engineering. This is achieved by formally proving the correctness of essential transformations that a source model undergoes during its compilation into executable code.

Our contribution to Verisync consists of revisiting the seminal work of Pnueli et al. on translation validation and equip the Polychrony environment with updated verification techniques to scale it to possibly large, sequential or distributed, C programs generated from the Signal compiler. Our study covers the definition of simulation and bisimulation equivalence relations capable of assessing the correspondence between a source Signal specification and the sequential or concurrent code generated from it, as well as both specific abstract model-checking techniques allowing to accelerate verification and counter-example search techniques, to filter spurious verification failures obtained from excessive abstracted exploration.
6.4. FUI project P

**Participants:** Loïc Besnard, Thierry Gautier, Paul Le Guernic, Christophe Junke, Jean-Pierre T. Talpin.

The aim of project P is 1/ to aid industrials to deploy model-driven engineering technology for the development of safety-critical embedded applications 2/ to contribute on initiatives such as OPEES and CESAR to develop support for tools inter-operability and 3/ provide state-of-the-art automated code generation techniques from multiple, heterogeneous, system-levels models. The focus of project P is the development of a code generation toolchain starting from domain-specific modeling languages for embedded software design and to deliver the outcome of this development as an open-source distribution, in the aim of gaining an impact similar to GCC for general-purpose programming, as well as a kit to aid with the qualification of that code generation toolchain.

The contribution of team ESPRESSO in project P is to bring the necessary open-source technology of the Polychrony environment to allow for the synthesis of symbolic schedulers for software architectures modeled with P in a manner ensuring global asynchronous deterministic execution.
LICIT Exploratory Action

6. Contracts and Grants with Industry

6.1. Contracts with Industry

The European project FI-WARE involves various industrial actors in the areas of security and internet services. The main interactions of LICIT within the project are with Nokia Siemens, SAP and Thales.
7. Contracts and Grants with Industry

7.1. Grants with Industry

- Google European Doctoral Fellowship for Tobias Grosser, 120k €.
7. Contracts and Grants with Industry

7.1. Grants with Industry

S4 Project-Team (section vide)
TRIO Project-Team (section vide)
7. Contracts and Grants with Industry

7.1. The Multival Project

Participants: Hubert Garavel, Rémi Hérilier, Frédéric Lang, Radu Mateescu, Christine McKinty, Vincent Poważny, Wendelin Serwe.

MULTIVAL (Validation of Multiprocessor Multithreaded Architectures) is a project of MINALOGIC, the pôle de compétitivité mondial dedicated to micro-nano technologies and embedded software for systems on chip (EMSoC cluster of MINALOGIC). It is funded by the French government (Fonds Unique Interministériel) and the Conseil Général de l’Isère. MULTIVAL addresses verification and performance evaluation issues for three innovative asynchronous architectures developed by BULL, CEA/LETI, and STMICROELECTRONICS.

MULTIVAL started in December 2006 and was extended until May 2011. In 2011, we focused our activities on the enhancement of CADP (see § 6.2.2 and § 6.2.3 ) and, in collaboration with our partners, on the verification of the DTD (see § 6.3.2 ).

7.2. The Topcased Project

Participants: Hubert Garavel, Frédéric Lang, Wendelin Serwe, Damien Thivolle.

TOPCASED (Toolkit in OPen-source for Critical Application and SystEms Development) is a project of AESE, the French pôle de compétitivité mondial dedicated to aeronautics, space, and embedded systems. This project gathers 23 partners, including companies developing safety-critical systems such as AIRBUS (leader), ASTRIUM, ATOS ORIGIN, CS, SIEMENS VDO, and THALES AEROSPACE.

TOPCASED develops a modular, open-source, generic CASE (Computer-Aided Software Engineering) environment providing methods and tools for embedded system development, ranging from system and architecture specifications to software and hardware implementation through equipment definition. VASY contributes to the combination of model-driven engineering and formal methods for asynchronous systems.

TOPCASED started in August 2006 and completed in December 2010. In 2011, we enhanced the FLAC translator from FIACRE to LOTOS (see § 6.2.3 ). We participated in the final review of TOPCASED and gave three lectures during the TOPCASED Days (see § 9.3 ).

During the International Paris Air Show (salon international du Bourget), the TOPCASED project received the AESE trophy of the best R&D project (category Systèmes, équipements et logiciels pour l’aéronautique et l’espace).
VERTECS Project-Team (section vide)
7. Contracts and Grants with Industry

7.1. Contracts with Industry

7.1.1. Contracts

7.1.1.1. Anastasy

Title: ANASTASY
Type: Industrial contract
Duration: September 2009 - December 2011
Others partners: Airbus France
Abstract: ANASTASY (ANAlyse STAique aSYnchone) is an industrial project with Airbus France on the static program analysis of asynchronous programs by abstract interpretation which objective is determined annually. Patrick Cousot is the principal investigator for this action.

7.1.2. License agreement

7.1.2.1. 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.

7.2. Grants with Industry

7.2.1. FNRAE projects

7.2.1.1. Ascert

Title: Analyses Statiques CERTifiés
Type: 6th call: Verification methods for software and systems
Instrument: FNRAE grant
Duration: April 2009 - March 2012
Coordinator: INRIA (France)
Others partners: INRIA-Bretagne Atlantique, the INRIA Rhône-Alpes, the INRIA Paris-Rocquencourt, and the ENS.
See also: http://ascert.gforge.inria.fr/
Abstract: Although static analyzers have demonstrated their ability to prove the absence of large classes of errors in critical software, they are themselves large and complex software, so it is natural to question their implementation correctness and the validity of their output. The focus of the ASCERT project is the use of formal methods to ensure the correctness of an analyzer with respect to the abstraction interpretation theory. Methods to be investigated include the direct proof of the analyzer, the proof of a verifier for the analyzer result, and the validation of the inductive invariants generated by the analyzer, using the Coq proof assistant. These methods will be applied to the certification of several numerical abstract domains, of an abstract interpreter for imperative programs and its possible extensions to one of the formal semantics of the CompCert verified C compiler.
7.2.1.2. Sardanes

Title: Sémantique, Analyse et Transformation Des Applications Numériques Embarqués Synchrones

Type: 6th call: Verification methods for software and systems

Instrument: FNRAE grant

Duration: February 2009 - September 2013

Coordinator: Université de Perpignan

Others partners: Université de Perpignan and the ENS.

See also: http://perso.univ-perp.fr/mmartel/sardanes.html

Abstract: SCADE is widely used to write critical embedded software, as a specification and verification language. The semantics of SCADE uses real arithmetics whereas it is compiled into a language that uses floating-point arithmetics. The goal of the SARDANES project is to use expression transformation so as to ensure that the numerical properties of the programs is preserved during the compilation. Patrick Cousot and Radhia Cousot are the principal investigators for this action.
ATEAMS Project-Team

7. Contracts and Grants with Industry

7.1. UvA

- Paul Klint is employed by Universiteit van Amsterdam for 0.4fte for directing the Master Software Engineering.
- Jan van Eijck is contracted by Universiteit van Amsterdam for 0.2fte, for teaching the course Software Testing.
- Tijs van der Storm is contracted by Universiteit van Amsterdam for 0.2fte, for teaching the courses Software Evolution and Software Construction.
- Jurgen Vinju is contracted by Universiteit van Amsterdam for 0.2fte, for teaching the courses Software Evolution and Software Construction.
- ATEAMS was contracted by Open Universiteit for the course material and support in teaching the Software Evolution course.
7. Contracts and Grants with Industry

7.1. Contracts with Industry

We have no contract with industry. However, we have several relationships with industrial partners like Thales and Netasq and established a lot of others contacts. See the Fi-Ware project.
CASSIS Project-Team

7. 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. European Projects

- AVANTSSAR — Automated validation of trust and security of service-oriented architectures. STREP Project funded under 7th FP (Seventh Framework Program) Research area: ICT-2007.1.4 Secure, dependable and trusted infrastructures. The coordinator is the University of Verona (Italy) and Cassis is one of the 10 partners. AVANTSSAR aims to propose a rigorous technology for the formal specification and "Automated VALidation of Trust and Security of Service-oriented ARChitectures". This technology will be automated into an integrated toolset, the AVANTSSAR Validation Platform, tuned on relevant industrial case studies.

- Nessos is a Network of Excellence on Engineering Secure Future Internet Software Services and Systems in FP7-ICT (starting in October 2010 for a period of 42 months). Nessos has 12 partners and aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. Partner INRIA is involved through project-teams Arles, Triskell and Cassis. Cassis will focus on developing tools for service security verification and testing tasks.

- ProSecure (2011-2016) — ERC Starting Grant Project on Provably secure systems: foundations, design, and modularity. This long-term project aims at developing provably secure systems such as security protocols. The goal is to propose foundations for a careful analysis and design of large classes of up-to-date protocols. To achieve this goal, we foresee three main tasks. First, we plan to develop general verification techniques for new classes of protocols that are of primary interest in nowadays life like e-voting protocols, routing protocols or security APIs. Second, we will consider the cryptographic part of the primitives that are used in such protocols (encryption, signatures, ...), obtaining higher security guarantees. Third, we aim at proposing modular results both for the analysis and design of protocols. Véronique Cortier is the leader of the project.

- SecureChange is funded under the 7th FP (Seventh Framework Program) Research area: ICT-2007.8.6: ICT forever yours. The project will develop processes and tools that support design techniques for evolution, testing, verification, re-configuration and local analysis of evolving software. Our focus is on mobile devices and homes, which offer both great research challenges and long-term business opportunities. The project is lead by Fabio Massacci (University of Trento, Italy) and it has started in February 2009 for a period of 36 months. Cassis is leader of the 7th workpackage (Testing). The local coordinator is Fabrice Bouquet.

---

4 http://www.loria.fr/~cortier/ProSecure.html
5 http://www.securechange.eu
6. Contracts and Grants with Industry

6.1. ANR DECERT project

Participants: Frédéric Besson, Thomas Jensen, David Pichardie, Pierre-Emmanuel Cornilleau, Florent Kirchner.

The DECERT project (2009–2011) is funded by the call Domaines Emergents 2008, a program of the Agence Nationale de la Recherche.

The objective of the DECERT project is to design an architecture for cooperating decision procedures, with a particular emphasis on fragments of arithmetic, including bounded and unbounded arithmetic over the integers and the reals, and on their combination with other theories for data structures such as lists, arrays or sets. To ensure trust in the architecture, the decision procedures will either be proved correct inside a proof assistant or produce proof witnesses allowing external checkers to verify the validity of their answers.

This is a joint project with Systerel, CEA List and INRIA teams Mosel, Cassis, Marelle, Proval and Celtique (coordinator).

6.2. ANR CAVERN project

Participants: Arnaud Gotlieb, Matthieu Carlier.

The CAVERN project (ANR, 2007-2011) gathers national research teams to study the capabilities of Constraint Programming for Program Verification (http://cavern.inria.fr/). This year, we focussed on WP4 on floating-point computations and got new results with the CeP team of University of Nice Sophia-Antipolis. The overall results of the project will be presented at the annual 2012 ANR meeting in Lyon.

6.3. ANR PiCoq project

Participant: Alan Schmitt.

The goal of the PiCoq project is to develop an environment for the formal verification of properties of distributed, component-based programs. The project’s approach approach lies at the interface between two research areas: concurrency theory and proof assistants. Achieving this goal relies on three scientific advances, which the project intends to address:

- Finding mathematical frameworks that ease modular reasoning about concurrent and distributed systems: due to their large size and complex interactions, distributed systems cannot be analysed in a global way. They have to be decomposed into modular components, whose individual behaviour can be understood.
- Improving existing proof techniques for distributed/modular systems: while behavioural theories of first-order concurrent languages are well understood, this is not the case for higher-order ones. We also need to generalise well-known modular techniques that have been developed for first-order languages to facilitate formalisation in a proof assistant, where source code redundancies should be avoided.
- Defining core calculi that both reflect concrete practice in distributed component programming and enjoy nice properties w.r.t. behavioural equivalences.

The project partners include INRIA, LIP, and Université de Savoie. The project runs from November 2010 to October 2014.
6.4. ANR U3CAT project

Participants: Sandrine Blazy, Matthieu Carlier, Arnaud Gotlieb, David Pichardie.

The ANR U3CAT project (2009–2012) is built upon the results of the RNTL CAT project, which delivered the Frama-C platform for the analysis of C programs and the ACSL assertion language. The ANR U3CAT project focuses on providing a unified interface that would allow to perform several analyses on a same code and to study how these analyses can cooperate in order to prove properties that could not have been established by one single technique. The other members of the project are the CEA LIST laboratory (project leader), Proval (Inria Futurs), Gallium (Inria Paris-Rocquencourt), Cedric (CNAM), Atos Origin, CS, Dassault-Aviation, Sagem Defense and Airbus Industries.

6.5. The FRAE ASCERT project

Participants: Frédéric Besson, Sandrine Blazy, David Cachera, Thomas Jensen, David Pichardie, Pierre-Emmanuel Cornilleau.

The ASCERT project (2009–2012) is founded by the Fondation de Recherche pour l’Aéronautique et l’Espace. It aims at studying the formal certification of static analysis using and comparing various approaches like certified programming of static analysers, checking of static analysis result and deductive verification of analysis results. It is a joint project with the INRIA teams ABSTRACTION, GALLIUM and POP-ART.

6.6. Regional Initiatives

6.6.1. The CERTLOGS project

Participants: Thomas Genet, Thomas Jensen, David Pichardie, Vincent Monfort, Florent Kirchner.

The CERTLOGS project (2009–2012) is funded by the CREATE action of the Région Bretagne. The objective of this project is to develop new kinds of program certificates and innovating certifying verification techniques using static analysis as the fundamental tool and combine this with techniques coming from probabilistic algorithms and cryptography.

6.7. European Initiatives

6.7.1. The COST Action IC0701

Participants: Thomas Jensen, David Pichardie.

COST Action IC0701 is a European scientific cooperation. The Action aims at developing verification technology with the power to ensure dependability of object-oriented programs on industrial scale. The action is composed of 15 countries. The COST action has been a forum for presenting our results concerning the data race analysis and our proposal for an intermediate language into which Java byte code can be transformed in order to facilitate the static analysis of byte code programs.

6.7.2. The Valves consortium

This year, we built the VALVES (Variability Testing of Highly-Variable Systems) European proposal gathering University of Sevilla, University of Namur, University of Uppsala, Isotrol, Thales and INRIA Rennes (Arnaud Gotlieb being the coordinator of the proposal). The proposal was submitted to the FP7 program (Call 7, challenge 3.3) and got well evaluated but not enough to be funded this year. From this, we got a support of the Brittany Region to organize a physical meeting during Fall 2011 and prepare a new submission. This meeting was held in the Paris INRIA’s offices, the 18th November 2011.
COMETE Project-Team (section vide)
7. Contracts and Grants with Industry

7.1. Biointelligence

- OSEO BioIntelligence project (2009-2014) coordinated by Patrick Johnson, Dassault-Systèmes, with EPI ORPAILLEUR, SOBIOS, Aureus pharma, IPSEN, Pierre Fabre, Sanofi-Aventis, Servier, Bayer CropScience, INSERM, Genopole Evry.

7.2. Rules2Optim

- DTI ITI support for the industrialization of Rules2CP software with SME KLS-Optim.

7.3. General Electric Transportation

- Pre-study on urban railway time tabling optimization (2011), General Electric Transportation.
- Cifre PhD accompanying contract on urban railway time tabling optimization (2011-2014), General Electric Transportation.
7. Contracts and Grants with Industry

7.1. Schneider Electric

The goal of this project contracted with Schneider Electric China is to develop a full system simulator for a System-on-Chip used by Schneider Electric in their automation product line.

7.2. Orange IT Labs

The goal of this project is to complete the PowerPC simulator and compare its performance with another simulator used internally by Orange IT Labs.
7. Contracts and Grants with Industry

7.1. The Caml Consortium

Participants: Xavier Leroy [correspondant], Xavier Clerc, 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 13 member companies:

- CEA
- Citrix
- Dassault Aviation
- Dassault Systèmes
- Esterel Technologies
- Jane Street
- LexiFi
- Microsoft
- MLstate
- Mylife.com
- OCamlCore
- 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.
MARELLE Project-Team (section vide)
7. Contracts and Grants with Industry

7.1. Contracts and Grants with Industry

So far, several contacts with industry have been established, but no bilateral contracts have materialized yet. Cooperations with France Télécom, Alcatel-Lucent and NEC are currently being developed within the EU IP UNIVERSELF, which has started in October 2010.
MOSCOVA Project-Team

7. Contracts and Grants with Industry

7.1. Grants with Industry

In 2006, we started to work at the Microsoft Research-INRIA Joint Centre in a common project with Cédric Fournet (MSR Cambridge), Gilles Barthe (now at IMDEA), Nataliya Guts (who defended her PhD in January 2011) and Jérémy Planul (who will defend on February 2012). The project is named Secure Distributed Computations and their Proofs and deals with security, programming languages theory and formal proofs. This work is still under active collaboration within all year 2011.

7.2. European Initiatives

7.2.1. FP7 Projet

7.2.1.1. CRYSP

Title: CRYSP: A Novel Framework for Collaboratively Building Cryptographically Secure Programs and their Proofs

Type: IDEAS

Instrument: ERC Starting Grant (Starting)

Duration: November 2010 - October 2015

Coordinator: Karthikeyan Bhargavan, INRIA (France)

Abstract: The goal of this grant proposal is to develop a collaborative specification framework and to build incremental, modular, scalable verification techniques that enable a group of collaborating programmers to build an application and its security proof side-by-side. We propose to validate this framework by developing the first large-scale web application and full-featured cryptographic protocol libraries with formal proofs of security.

7.3. International Initiatives

We are Équipe Associée with Computer lab at University of Cambridge (P. Sewell et al).
PARSIFAL Project-Team (section vide)
7. Contracts and Grants with Industry

7.1. National Initiatives

Matthieu Sozeau is member of the ANR Typex project (Types and certification for XML) and is coordinator of one of the tasks of the project on formalization and certification of XML tools. The project will kick-off on January 8th, 2012 and is a joint project with LRI, PPS and INRIA Grenoble.

Matthieu Sozeau, Hugo Herbelin and Yann Régis-Gianas are members of the ANR Paral-ITP started November 2011. Paral-ITP is about preparing the Coq and Isabelle interactive theorem provers to a new generation of user interfaces thanks to massive parallelism and incremental type-checking.

Hugo Herbelin is the coordinator of the PPS site for the ANR Récré accepted in 2011 and starting January 2012. Pierre Letouzey is member of the ANR Récré. Récré is about realisability and rewriting, with applications to proving with side-effects and concurrency.

7.2. European Initiatives

Yann Régis-Gianas is a participant of the EU-FP7 Certified Complexity project (CerCo). This European project started in February 2010 as a collaboration between Bologna university (Asperti, Coen), Edinburgh university (Pollack) and Paris Diderot university (Amadio, Régis-Gianas). The CerCo project aims at the construction of a formally verified complexity preserving compiler from a large subset of the C programming language to some typical micro-controller assembly language, of the kind traditionally used in embedded systems. Nicolas Ayache’s postdoc is funded by this project.

Hugo Herbelin, Pierre Letouzey and Matthieu Sozeau submitted a proposal for a PHC Van Gogh with the university of Nijmegen in the Netherlands. This proposal is about the mathematical libraries of Coq, type classes, and the homotopic interpretation of equality in the Calculus of Inductive Constructions.

Hugo Herbelin is the participant of a submitted proposal for a PHC Pavle Savić with the university of Novi Sad in Serbia, the mathematical institute of Belgrade, ENS Lyon and the university of Turin. This proposal is on a general thematic logic and types. Hugo Herbelin is also the participant of a submitted proposal for another PHC Pavle Savić with the university of Belgrade and the university of Strasbourg. This proposal is about automated deduction and formal geometry.
7. Contracts and Grants with Industry

7.1. Systematic: Hi-Lite

Participants: Claude Marché [contact], Jean-Christophe Filliâtre, Sylvain Conchon, Evelyne Contejean, Andrei Paskevich, Alain Mebsout, Mohamed Iguernelala, Denis Cousineau.

The Hi-Lite project (http://www.open-do.org/projects/hi-lite/) is a project in the SYSTEMATIC Paris Region French cluster in complex systems design and management http://www.systematic-paris-region.org. Hi-Lite is a project aiming at popularizing formal methods for the development of high-integrity software. It targets ease of adoption through a loose integration of formal proofs with testing and static analysis, that allows combining techniques around a common expression of specifications. Its technical focus is on modularity, that allows a divide-and-conquer approach to large software systems, as well as an early adoption by all programmers in the software life cycle.

Our involvements in that project include the use of the Alt-Ergo prover as back-end to already existing tools for SPARK/ADA, and the design of a verification chain for an extended SPARK/ADA language to verification conditions, via the Why VC generator.

This project is funded by the french ministry of industry (FUI), the Île-de-France region and the Essonne general council for 36 months from September 2010.

7.2. CEA-Airbus contract

Participants: Sylvain Conchon [contact], Évelyne Contejean, Claude Marché.

In conjunction with the INRIA funding of ADT Alt-Ergo, a specific support contract has started in Sep 09, between INRIA, CEA Saclay and Airbus France at Toulouse. This is to support our efforts for the maintainance and to feature updates of Alt-Ergo, for its use at Airbus software development and certification of avionics critical code.

7.3. Airbus contract

Participant: Sylvain Conchon [contact].

This 2 years support contract has started in Sep 10, between INRIA and Airbus France at Toulouse. This is to support our efforts for the DO-178B qualification of Alt-Ergo.
SECSI Project-Team (section vide)
TASC Project-Team

7. Contracts and Grants with Industry

7.1. Contracts

7.1.1. Ligéro

Participants: Sophie Demassey.
Title: Ligéro.
Duration: 2009-2012.
Type: Regional research group
Budget: PhD founded by the project.
Others partners: LISA, IRCCyN (team SLP), LERIA (team MOA), LINA (team OPTI).

The goal of the project is to create an internationally visible regional research group putting together the key actors in the domain of Operations Research in the Pays de la Loire region.

7.1.2. CPER

Participants: 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.

7.1.3. UNIT

Participants: Nicolas Beldiceanu.
Title: UNIT.
Duration: 2011.
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).

7.1.4. 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.

### 7.1.5. ANR BOOLE

**Participants:** Jérémie du Boisberranger, Xavier Lorca, Charlotte Truchet.

- **Title:** BOOLE.
- **Duration:** 2010-2015.
- **Type:** open research program.
- **Budget:** founding a PhD student and travels.
- **Défi:** Probabilistic method for combinatorial problems.

The work of TASC focuses on the use of probabilistic methods to avoid waking 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.

### 7.1.6. ANR SelfXL

**Participants:** Nicolas Beldiceanu, Sophie Demassey, Xavier Lorca, Arnaud Letort.

- **Title:** SelfXL.
- **Duration:** 2009-2011.
- **Type:** embedded systems and large infrastructures research program.
- **Budget:** founding for half a PhD.
- **Others partners:** ASCOLA.

Flexible and efficient tools for complex-large scale autonomic systems. TASC contributes for handling bin packing and bin repacking problems with side constraints derived from migration modes of virtual machines between servers. Constraints based models and CHOCO based solvers are developed for this purpose. The work was done with F. Hermenier and J.-M. Menaud.

### 7.1.7. ANR NetWMS2

**Participants:** Nicolas Beldiceanu, Gilles Chabert.

- **Title:** Networked Warehouse Management Systems 2: packing with complex shapes.
- **Duration:** 2011-2014.
- **Type:** cosinus research program, **new project**.
- **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 generalising 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).
7.1.8. 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.

7.2. Grants

7.2.1. Google Focused Research Awards

**Participants:** Narendra Jussien, Charles Prud’Homme.

- **Title:** Non intrusive explanations.
- **Duration:** 2011.
- **Type:** new grant.
- **Budget:** 75000 Euros.

Constraint programming, despite its numerous successes in practice, suffers from not being really user-friendly when used by software engineers. Explanations for constraint programming have addressed this issue but are not yet widely used in the CP community. The objective of our work is to specify an user-oriented explanation-module for flexible solver architectures and provide a reference implementation within the new version of our solver CHOCO. This line of work will be founded in 2012 by the CNRS (one year of engineer).
TYPICAL Project-Team (section vide)
7. Contracts and Grants with Industry

7.1. ANR project DeCert

Participants: Pascal Fontaine, Stephan Merz, Bruno Woltzenlogel Paleo.

The DeCert (Deduction and Certification) project is being funded by ANR from 2009–2012 within its “Domaines émergents” program. It is coordinated by the Celtique project team of INRIA Rennes, the other partners are academic teams from INRIA Saclay (Proval) and INRIA Sophia Antipolis (Marelle) as well as the CEA and the Systerel company. In Nancy, the project also involves members of the Cassis team, in particular Alain Giorgetti and Christophe Ringeissen.

The objective of the project is to study certified decision procedures, including the design of appropriate certificates, the development of new certifying decision procedures, their combination, their integration with skeptical proof assistants such as Coq or Isabelle, and their use in application domains such as software verification or static analysis. The main lines of research concern questions of expressiveness vs. efficiency, certificates vs. proof objects, and the integration of certificates into verification environments. Our work within the project is related to veriT (see section 5.1), its proof production, and its integration with verification environments such as Isabelle or the TLA+ proof environments (see section 5.2).

7.2. Tools and Methodologies for Formal Specifications and for Proofs

Participants: Stephan Merz, Hernán-Pablo Vanzetto.

We participate in the project on Tools and Methodologies for Formal Specifications and for Proofs at the MSR-INRIA Joint Centre. The objective of the project is to develop a proof environment for verifying distributed algorithms in TLA+ (see also sections 5.2 and 6.4). The project in particular funds the PhD thesis of Hernán Vanzetto.

7.3. Diagnosis of errors in network controlled systems

Participants: Diego Caminha Barbosa de Oliveira, Pascal Fontaine, Stephan Merz.

In an exploratory project with Westinghouse France, we studied the possibility of using formal verification technology (in particular model checking and SAT/SMT solving) for diagnosing possibly transient faults in communication networks. The diagnosis is based on logs that are generated by periodic self tests. In particular, the SAT solver of veriT has been interfaced with Matlab so that it can be used by our industrial partner for determining causes of certain permanent faults. We have also used Uppaal to model a simplified version of a protocol used by our industrial partner in order to determine timing intervals for the occurrence of faults detected in logs.