Activity Report 2011

Section Partnerships and Cooperations
ALGORITHMS, CERTIFICATION, AND CRYPTOGRAPHY
1. ALGORITHMS Project-Team ................................................................. 5
2. ARENAIRE Project-Team ................................................................. 6
3. CARAMEL Project-Team ................................................................. 9
4. CASCADE Project-Team ................................................................. 10
5. GALAAD Project-Team (section vide) ............................................. 11
6. GEOMETRICA Project-Team .......................................................... 12
7. LFANT Project-Team (section vide) ................................................ 17
8. SALSA Project-Team ..................................................................... 18
9. SECRET Project-Team ................................................................. 22
10. TANC Project-Team ..................................................................... 24
11. VEGAS Project-Team (section vide) ............................................ 25

ARCHITECTURE AND COMPILING
12. ALF Project-Team ......................................................................... 26
13. CAIRN Project-Team .................................................................... 27
14. CAMUS Team ............................................................................... 32
15. COMPSYS Project-Team ............................................................... 34

EMBEDDED AND REAL TIME SYSTEMS
16. AOSTE Project-Team ..................................................................... 36
17. DART Project-Team (section vide) ............................................... 41
18. ESPRESSO Project-Team ............................................................. 42
19. LICIT Exploratory Action ............................................................ 44
20. PARKAS Team ............................................................................. 46
21. POP ART Project-Team ............................................................... 49
22. S4 Project-Team ........................................................................... 52
23. TRIO Project-Team (section vide) ................................................ 53
24. VASY Project-Team ..................................................................... 54
25. VERTECS Project-Team .............................................................. 56

PROGRAMS, VERIFICATION AND PROOFS
26. ABSTRACTION Project-Team ....................................................... 59
27. ATEAMS Project-Team ............................................................... 63
28. CARTE Project-Team ................................................................. 64
29. CASSIS Project-Team ................................................................. 66
30. CELTIQUE Project-Team ............................................................ 70
31. COMETE Project-Team ............................................................... 71
32. CONTRAINTE Project-Team ....................................................... 73
33. FORMES Team ............................................................................. 76
34. GALLIUM Project-Team ............................................................. 78
35. MARELLE Project-Team ............................................................. 79
36. MEXICO Project-Team ............................................................... 81
37. MOSCOVA Project-Team (section vide) .................................... 86
38. PAREO Project-Team ................................................................. 87
39. PARSIFAL Project-Team .......................................................... 88
40. PLR2 Project-Team ................................................................. 93
41. PROVAL Project-Team .............................................................. 95
42. SECSI Project-Team ............................................................... 98
43. TASC Project-Team ................................................................. 100
44. TYPICAL Project-Team ........................................................... 101
45. VERIDIS Team ...................................................................... 103
7. Partnerships and Cooperations

7.1. Regional Initiatives

Nicolas Broutin has obtained two years funding from Egide to support a collaboration on geometric data structures with Ralph Neininger from the University of Frankfurt.

7.2. National Initiatives

Aléa is a national working group dedicated to the analysis of algorithms and random combinatorial structures. It is a meeting place for mathematicians and computer scientists working in the area of discrete models. It is currently supported by CNRS (GDR IM) and was globally animated by Philippe Flajolet. In March 2011 the yearly meeting has gathered in Luminy over 80 participants from about 20 different research laboratories throughout France.

In September 2009, the Algorithms project has started a new participation in the programme funded by the National Research Agency (ANR) entitled BOOLE for “Quantifying Boolean Frameworks”. Four teams are involved: Algorithms from Inria Paris–Rocquencourt, the Universities of Caen, Versailles (coordinator), and Provence Aix–Marseille 1; the project is for 4 years until August 2013. The Inria Team also includes researchers at the École Normale Supérieure (ENS Ulm): Guilhem Semerjian and Jean Vuillemin.

7.3. International Initiatives

7.3.1. Visits of International Scientists

James Davenport, from the University of Bath (UK) has been invited for one month in April 2011. At this occasion, [15] was completed.

Other visitors for shorter periods were: Manuel Kauers, RISC, Linz (Austria), Ziming Li (Key Laboratory of Mathematics Mechanization of the Chinese Academy of Mathematics and System Sciences, Beijing),
8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Cible Grant from Région Rhône-Alpes


Since October 2008, we have obtained a 3-year grant from Région Rhône-Alpes. That grant has funded a PhD student, Mioara Joldeș, who defended her PhD thesis on September 26, 2011. The project consists in automating as much as possible the generation of code for approximating functions. Instead of calling functions from libraries, we wish to elaborate approximations at compile-time, in order to be able to directly approximate compound functions, or to take into account some information (typically, input range information) that might be available at that time. In this project, we collaborate with the STMicroelectronics’ Compilation Expertise Center in Grenoble (C. Bertin, H. Knochel, and C. Monat). STMicroelectronics is funding another PhD grant on these themes.

8.2. National Initiatives

8.2.1. ANR HPAC Project

Participants: Claude-Pierre Jeannerod, Nicolas Louvet, Nathalie Revol, Damien Stehlé, Philippe Théveny, Gilles Villard.

“High-performance Algebraic Computing” (HPAC) is a four year ANR project that will start in January 2012. HPAC is headed by Jean-Guillaume Dumas (CASYS team, LJK laboratory, Grenoble); it involves Arénaire as well as the INRIA project-team MOAIS (LIG, Grenoble), the INRIA project-team SALSA (LIP6 lab., Paris), the ARITH group (LIRMM laboratory, Montpellier), and the HPC Project company.

The overall ambition of HPAC is to provide international reference high-performance libraries for exact linear algebra and algebraic systems on multi-processor architecture and to influence parallel programming approaches for algebraic computing. The central goal is to extend the efficiency of the LinBox and FGb libraries to new trend parallel architectures such as clusters of multi-processor systems and graphics processing units in order to tackle a broader class of problems in lattice cryptography and algebraic cryptanalysis. HPAC will conduct researches along three axes:
- A domain specific parallel language (DSL) adapted to high-performance algebraic computations;
- Parallel linear algebra kernels and higher-level mathematical algorithms and library modules;
- Library composition and innovative high performance solutions for cryptology challenges.

8.2.2. ANR TaMaDi Project

Participants: Nicolas Brisebarre, Florent de Dinechin, Guillaume Hanrot, Vincent Lefèvre, Érik Martin-Dorel, Micaela Mayero, Jean-Michel Muller, Andrew Novocin, Ioana Pasca, Damien Stehlé, Serge Torres.

The TaMaDi project (Table Maker’s Dilemma, 2010-2013) is funded by the ANR and headed by Jean-Michel Muller. It was submitted in January 2010, accepted in June, and started in October 2010. The other French teams involved in the project are the MARELLE team-project of INRIA Sophia Antipolis-Méditerranée, and the PEQUAN team of LIP6 lab., Paris.
The aim of the project is to find “hardest to round” (HR) cases for the most common functions and floating-point formats. In floating-point (FP) arithmetic having fully-specified “atomic” operations is a key-requrement for portable, predictable and provable numerical software. Since 1985, the four arithmetic operations and the square root are IEEE specified (it is required that they should be correctly rounded: the system must always return the floating-point number nearest the exact result of the operation). This is not fully the case for the basic mathematical functions (sine, cosine, exponential, etc.). Indeed, the same function, on the same argument value, with the same format, may return significantly different results depending on the environment. As a consequence, numerical programs using these functions suffer from various problems. The lack of specification is due to a problem called the Table Maker’s Dilemma (TMD). To compute \( f(x) \) in a given format, where \( x \) is a FP number, we must first compute an approximation to \( f(x) \) with a given precision, which we round to the nearest FP number in the considered format. The problem is the following: finding what the accuracy of the approximation must be to ensure that the obtained result is always equal to the “exact” \( f(x) \) rounded to the nearest FP number. In the last years, our team-project and the CACAO team-project of INRIA Nancy-Grand Est designed algorithms for finding hardest-to-round cases. These algorithms do not allow to tackle with large formats. The TaMaDi project mainly focuses on three aspects:

- big precisions: we must get new algorithms for dealing with precisions larger than double precision. Such precisions will become more and more important (even if double precision may be thought as more than enough for a final result, it may not be sufficient for the intermediate results of long or critical calculations);
- formal proof: we must provide formal proofs of the critical parts of our methods. Another possibility is to have our programs generating certificates that show the validity of their results. We should then focus on proving the certificates;
- aggressive computing: the methods we have designed for generating HR points in double precision require weeks of computation on hundreds of PCs. Even if we design faster algorithms, we must massively parallelize our methods, and study various ways of doing that.

There was a meeting in Sophia-Antipolis in February 2011, and two other ones in Lyon in June and December 2011. The various documents can be found at http://tamadiwiki.ens-lyon.fr/tamadiwiki/index.php/Main_Page.

8.2.3. ANR TCHATER Project

Participants: Florent de Dinechin, Honoré Takeugming, Gilles Villard.

The TCHATER project (Terminal Cohérent Hétérodyne Adaptatif TEmps Réel, 2008-2010) is a collaboration between Alcatel-Lucent France, E2V Semiconductors, GET-ENST and the INRIA Arénaire and ASPI project/teams. Its purpose is to demonstrate a coherent terminal operating at 40Gb/s using real-time digital signal processing and efficient polarization division multiplexing. In Lyon, we studied the FPGA implementation of specific algorithms for polarization demultiplexing and forward error correction with soft decoding. TCHATER was extended by the ANR until 9/06/2011, which allowed us to finalize the demonstrator.

8.2.4. ANR LaRedA Project

Participants: Fabien Laguillaumie, Adeline Langlois, Ivan Morel, Xavier Pujol, Damien Stehlé.

The LaRedA project (Lattice Reduction Algorithms, 2008-2011) is funded by the ANR and headed by Brigitte Vallée (CNRS/GREYC) and Valérie Berthé (CNRS/LIRMM). The aim of the project is to finely analyze lattice reduction algorithms such as LLL, by using experiments, probabilistic tools and dynamic analysis. Among the major goals are the average-case analysis of LLL and its output distribution. In Lyon, we concentrate on the experimental side of the project (by using fpLLL and MAGMA) and the applications of lattice reduction algorithms to cryptography.
8.3. European Initiatives

8.3.1. Other European Initiatives

- Guillaume Hanrot and Damien Stehlé collaborate with Cong Ling (Imperial College London, UK) on lattices and communication theory. The collaboration is jointly funded by the CNRS and the Royal Society, from January 2011 to December 2012.

8.4. International Initiatives

8.4.1. INRIA International Partners


8.4.2. Visits of International Scientists

- San Ling (Nanyang Technological University, Singapore) visited for two months (March and April), for collaborating on lattice-based cryptography. Visit partly funded by NTU and Inria Rhône-Alpes (invited researcher).
- Xiao-Wen Chang (McGill University, Canada) visited for one month (July), for collaborating on the numerical aspects of lattice reduction algorithms. Visit funded by ENS de Lyon (invited professor).
- Ron Steinfeld (Macquarie University, Australia) visited for one month (August), for collaborating on lattice-based cryptography. Visit funded by the French Embassy in Australia.

8.4.3. Participation In International Programs

- Guillaume Hanrot and Damien Stehlé participate in the LaBaCry project (Lattice-Based Cryptography), with San Ling and Huaxiong Wang (Cryptography and Coding group of Nanyang Technological University, Singapore). Project jointly funded by NTU and the MERLION program from the French Embassy in Singapore.
- Damien Stehlé is a Partner Investigator in the Australian Research Council Discovery Grant *Lattices as a Constructive and Destructive Tool in Cryptography*, with Christophe Doche, Igor Shparlinski and Ron Steinfeld (Macquarie University).
- Florent de Dinechin was invited 4 months by Nizhniy Novgorod State University (Russia).
7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Function field sieve: implementation and hardware acceleration

Participants: Jérémie Detrey [contact], Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé.

The team has obtained for the year 2012 a financial support from the Région Lorraine and INRIA for a project focusing on the hardware implementation and acceleration of the function field sieve (FFS).

The FFS algorithm is currently the best known method to compute discrete logarithms in small-characteristic finite fields, such as may occur in pairing-based cryptosystems. Its study is therefore crucial to accurately assess the key-lengths which such cryptosystems should use. More precisely, this project aims at quantifying how much this algorithm can benefit from recent hardware technologies such as GPUs or CPU-embedded FPGAs, and how this might impact current key length recommendations.

7.2. National Initiatives

7.2.1. ANR DEMOTIS (Collaborative Analysis, Evaluation and Modelling of Health Information Technology)

Participant: Marion Videau.

The project from “programme ARPEGE” involves three INRIA project-teams as a single partner (SMIS, SECRET and CARAMEL) together with colleagues from CECOJI (CNRS) and the company Sopinspace. It has been running from January 2009 and will continue until the beginning of 2012.

The project experiments new methods for the multidisciplinary design of large information systems that have to take into account legal, social and technical constraints. Its main field of application is personal health information systems.

7.2.2. ANR CHIC (Courbes Hyperelliptiques, Isogénies, Comptage)

Participants: Gaëtan Bisson, Romain Cosset, Pierrick Gaudry, Sorina Ionica, Pascal Molin, Emmanuel Thomé [contact].

The team has obtained a financial support from the ANR (“programme blanc”) for a project, common with colleagues from IRMAR (Rennes) and IML (Marseille). The ANR CHIC grant covers the period 09/2009 to 08/2012. The purpose of this ANR project is the study of several aspects of curves in genus 2, with a very strong focus on the computation of explicit isogenies between Jacobians.

This ANR project has been an important source of motivation for both permanent researchers and PhD students, giving notably PhD students the opportunity to meet interested colleagues on a regular basis. In 2011, a server with a huge large of central memory has been bought, to help with CHIC-related experiments. Two PhD thesis were defended (Bisson and Cosset) on the topic.

7.3. European Initiatives

7.3.1. PHC application with EPFL

The team obtained a PHC Germaine de Staël grant in collaboration with the LACAL team from EPFL (Lausanne, Switzerland), in 2011. The grant has been renewed for 2012. This collaboration focuses on integer factorization and discrete logarithms.
7. Partnerships and Cooperations

7.1. European Initiatives

- **ECRYPT-II: Network of Excellence in Cryptology.**
  From August 2008 to July 2012.
  *There are three virtual labs that focus on the following core research areas: symmetric key algorithms (STVL), public key algorithms and protocols (MAYA), and secure and efficient implementations (VAMPIRE).*
  ENS/INRIA/CASCADE leads the MAYA virtual lab.

- **ERC Starting Grant: LATTICE.**
  Oded Regev (2008 – 2013)

- **SecFuNet: Security for Future Networks.**
  From July 2011 to December 2013

7.2. Grants

- **Chaire ENS – France Télécom pour la sécurité des réseaux de télécommunications.**
  From January 2006 to December 2012.

- **Fondation EADS Grant.**

- **Donation of Tilera multicore cluster (512 core, 64 bits each) by Tilera.**
  This supercomputer allows the team to experiment various cryptanalysis and simulations. The machine was installed at ENS for the team, in recognition of the team’s cryptanalytic and research achievements.

7.3. Exterior Research Visitors

- Zvika Brakerski – Weizmann Institute, Israel
- Vincent Cheval – ENS Cachan, France
- Angelo De Caro – Univ. Salerno, Italy
- Karina M. Magalhães – University of Campinas, Brazil
- Petros Mol – UC San Diego, USA
- Takashi Nishide – Kyushu University, Japan
- Chris Peikert – Georgia Tech , USA
- Adi Shamir – Weizmann Institute, Israel
GALAAD Project-Team (section vide)
8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ADT CGAL-Mesh

Participants: Pierre Alliez, Mariette Yvinec, Jean-Daniel Boissonnat.

CGAL-Mesh was a two-year INRIA technological development action started in March 2009. Building upon components from CGAL, we have implemented a generic mesh generation framework for 3D domains. We primarily target applications which involve data acquired from the physical world: geology, medicine, 3D cartography and reverse engineering. We wish to establish for the whole duration of the action a close collaboration with industrial and academic partners so as to maximize the impact of the platform for a number of applications and research experiments.

- Starting date: March 2009
- Duration: 2 years

8.1.2. ANR Triangles

Participants: Olivier Devillers, Monique Teillaud.

Web site: http://www.inria.fr/sophia/geometrica/collaborations/triangles/

We lead the TRIANGLES project funded by the ANR. The project involves:

- the «Laboratoire d’Informatique en Image et Systèmes d’Information» (LIRIS), Lyon,
- the «Département d’informatique de l’ENS»
- the GEOMETRICA team.

Triangulations are essential in many applications, in particular for meshing and shape reconstruction. We want to develop and distribute new results for academic and industrial researchers. The goal of the project is the development of robust and effective algorithms for the manipulation of large sets of points, of moving sets of points and points in non Euclidean spaces such as periodic spaces (torus, cylinder), projective, oriented projective or hyperbolic spaces. The results obtained will be implemented in the CGAL library and will be applied to computer vision (visual envelopes, camera calibration), fluid dynamics, astronomy, computer graphics and medical applications.

In the GEOMETRICA team, Triangles is co-funding the scholarship of Pedro de Castro (with «Région PACA») and funding travel expenses and computers. Several meetings have been organized between participants, details can be found on the project’s web page.

- Starting date: November 2007
- Duration: 3 years + 6 months prolongation

8.1.3. ANR GAIA

Participants: Jean-Daniel Boissonnat, Frédéric Chazal, David Cohen-Steiner, Arijit Ghosh.

The aim of this project is to formalize a collaboration between researchers from computational geometry, machine learning and computer vision to study distortions and in particular Bregman divergences, information theory, statistics, Riemannian geometry, and convex analysis.

The other partners of the project are the Université des Antilles et de la Guyane (R. Nock, coordinator), the Ecole Polytechnique (F. Nielsen) and the Lear project-team (C. Schmid).
- Starting date: November 2007
- Duration: 4 years

8.1.4. ANR GIGA

**Participants:** Pierre Alliez, Jean-Daniel Boissonnat, Frédéric Chazal, David Cohen-Steiner, Mariette Yvinec, Steve Oudot, Marc Glisse.

GIGA stands for Geometric Inference and Geometric Approximation. GIGA aims at designing mathematical models and algorithms for analyzing, representing and manipulating discretized versions of continuous shapes without losing their topological and geometric properties. By shapes, we mean sub-manifolds or compact subsets of, possibly high dimensional, Riemannian manifolds. This research project is divided into tasks which have Geometric Inference and Geometric Approximation as a common thread. Shapes can be represented in three ways: a physical representation (known only through measurements), a mathematical representation (abstract and continuous), and a computerized representation (inherently discrete). The GIGA project aims at studying the transitions from one type to the other, as well as the associated discrete data structures.

Some tasks are motivated by problems coming from data analysis, which can be found when studying data sets in high dimensional spaces. They are dedicated to the development of mathematically well-founded models and tools for the robust estimation of topological and geometric properties of data sets sampled around an unknown compact set in Euclidean spaces or around Riemannian manifolds.

Some tasks are motivated by problems coming from data generation, which can be found when studying data sets in lower dimensional spaces (Euclidean spaces of dimension 2 or 3). The proposed research activities aim at leveraging some concepts from computational geometry and harmonic forms to provide novel algorithms for generating discrete data structures either from mathematical representations (possibly deriving from an inference process) or from raw, unprocessed discrete data. We target both isotropic and anisotropic meshes, and simplicial as well as quadrangle and hexahedron meshes.

This project coordinated by GEOMETRICA also involves researchers from the INRIA team-project ABS, CNRS (Grenoble), and a representative from the industry (Dassault Systèmes).

- Starting date: October 2009.
- Duration: 4 years.

8.1.5. DIGITEO Chair C3TTA: Cell Complexes in Computational Topology: Theory and Applications

**Participants:** Claire Caillerie, Frédéric Chazal, David Cohen-Steiner, Marc Glisse, Steve Oudot, Amit Patel.

The primary purpose of this project is to bring about a close collaboration between the chair holder Dr Vin de Silva and Digiteo teams working on the development of topological and geometric methods in Computer Science. The research program is motivated by problems coming from the increasing need of studying and analyzing the (often huge) data sets that are now available in many scientific and economic domains. Indeed, due to the improvements of measurement devices and data storage tools, the available data about complex shapes or complex systems are growing very fast. These data being often represented as point clouds in high dimensional (or even infinite dimensional) spaces there is a considerable interest in analyzing and processing data in such spaces. Despite the high dimensionality of the ambient space, one often expects them to be located around an unknown, possibly non linear, low dimensional shape. It is then appealing to infer and analyze topological and geometric characteristics of that shape from the data. The hope is that this information will help to process more efficiently the data and to better understand the underlying complex systems from which the data are generated. In the last few years, topological and geometric approaches to obtain such information have encountered an increasing interest. The goal of this project is to bring together the complementary expertises in computational topology and geometry of the involved Digiteo teams and in applied geometry and algebraic topology of V. de Silva to develop new topological approaches to the previous mentioned domain. The project intends to develop both the theoretical and practical sides of this subject. The other partners of the project are the Ecole Polytechnique (L. Castelli-Aleardi and F. Nielsen) and the CEA (E. Goubault).
- Starting date: January 2009.
- Duration: 3 years.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. CG-Learning

Title: Computational Geometric Learning
Type: COOPERATION (ICT)
Defi: FET Open
Instrument: Specific Targeted Research Project (STREP)
Duration: November 2010 - October 2013
Coordinator: Friedrich-Schiller-Universität Jena (Germany)
Others partners: National and Kapodistrian University of Athens (Greece), Technische Universität Dortmund (Germany), Tel Aviv University (Israel), Eidgenössische Technische Hochschule Zürich (Switzerland), Rijksuniversiteit Groningen (Netherlands), Freie Universität Berlin (Germany)
See also: http://cgl.uni-jena.de/

Abstract: The Computational Geometric Learning project aims at extending the success story of geometric algorithms with guarantees to high-dimensions. This is not a straightforward task. For many problems, no efficient algorithms exist that compute the exact solution in high dimensions. This behavior is commonly called the curse of dimensionality. We try to address the curse of dimensionality by focusing on inherent structure in the data like sparsity or low intrinsic dimension, and by resorting to fast approximation algorithms.

8.2.1.2. ERC IRON

Title: Robust Geometry Processing
Type: IDEAS
Instrument: ERC Starting Grant (Starting)
Duration: January 2011 - December 2015
Coordinator: Pierre Alliez, INRIA (France)
See also: http://www-sop.inria.fr/geometrica/collaborations/iron/

Abstract: The purpose of this project is to bring forth the full scientific and technological potential of Digital Geometry Processing by consolidating its most foundational aspects. Our methodology will draw from and bridge the two main communities (computer graphics and computational geometry) involved in discrete geometry to derive algorithmic and theoretical contributions that provide both robustness to noisy, unprocessed inputs, and strong guarantees on the outputs. The intended impact is to make the digital geometry pipeline as generic and ironclad as its Digital Signal Processing counterpart.

8.3. International Initiatives

8.3.1. INRIA Associate Teams

8.3.1.1. COMET

Title: Computational Methods for the analysis of high-dimensional data
INRIA principal investigator: Steve Y. Oudot
International Partner:
  Institution: Stanford University (United States)
  Laboratory: Computer Science Department
  Researcher: Leonidas J. Guibas

International Partner:
  Institution: Ohio State University (United States)
  Laboratory: Computer Science and Engineering
  Researcher: Yusu Wang

Duration: 2011 - 2013
See also: http://geometrica.saclay.inria.fr/collaborations/CoMeT/index.html

CoMeT is an associate team between the Geometrica group at INRIA, the Geometric Computing group at Stanford University, and the Computational Geometry group at the Ohio State University. Its focus is on the design of computational methods for the analysis of high-dimensional data, using tools from metric geometry and algebraic topology. Our goal is to extract enough structure from the data, so we can get a higher-level informative understanding of these data and of the spaces they originate from. The main challenge is to be able to go beyond mere dimensionality reduction and topology inference, without the need for a costly explicit reconstruction. To validate our approach, we intend to set our methods against real-life data sets coming from a variety of applications, including (but not restricted to) clustering, image or shape segmentation, sensor field monitoring, shape classification and matching. The three research groups involved in this project have been active contributors in the field of Computational Topology in the recent years, and some of their members have had long-standing collaborations. We believe this associate team can help create new synergies between these groups.

8.3.1.2. DDGM

Title: Discrete Differential Geometric Modeling
INRIA principal investigator: Pierre Alliez

International Partner:
  Institution: California Institute of Technology (United States)
  Laboratory: Applied Geometry Lab

Duration: 2009 - 2011
See also: http://www-sop.inria.fr/geometrica/collaborations/ddgm/

Our initial goals were to collaborate on geometry processing and modeling. Our initial focus in 2009 was on the notion of quality of the computational models or discretizations: we carried out research on the generation of quality meshes through variational methods, on the generation of surface mesh parameterizations with low distortion, and on simplifications with guaranteed error bounds. The motivation was to meet the requirements imposed by simulations in computational engineering and computer animation. Amidst the completion of our project, we partially shifted our research goals when we realized that streamlining the geometry processing pipeline could be greatly facilitated if in addition to guaranteeing the output quality, we could provide robustness (i.e., resilience) to defect-laden inputs. This explains our recent focus on methods which are robust to heterogeneous data and to data hampered with a variety of defects. Sampling defects (such as non uniform, widely variable sampling, missing data) and uncertainty (noise, background noise, registration noise, outliers) are indeed increasingly present in datasets coming from cheaper and cheaper sensors. Our quest for ironclad robustness is best illustrated by two shape reconstruction methods we contributed, able to deal with noise and outliers.
8.3.1.3. OrbiCG

Title: Triangulations and meshes in new spaces
INRIA principal investigator: Monique Teillaud
International Partner:
Institution: University of Groningen (Netherlands)
Laboratory: Johann Bernoulli Institute of Mathematics and Computing Science
International Partner:
Institution: University of Groningen (Netherlands)
Laboratory: Kapteyn Astronomical Institute
Duration: 2009 - 2011
See also: http://www-sop.inria.fr/geometrica/collaborations/OrbiCG/

Due to the now established emergence of standardized software libraries, such as the Computational Geometry Algorithms Library CGAL, a result of concerted efforts by groups of researchers in Europe, and whose Geometrica is one of the leaders, the so-far mostly theoretical results developed in computational geometry are being used and extended for practical use like never before for the benefit of researchers in academia and of industry. To fulfill the promise of applicability of computational geometry and to expand the scope of initial efforts, extending the traditional focus on the Euclidean space Rd ("urbi") to encompass various spaces ("orbi") has become important and timely.

8.3.2. Visits of International Scientists

8.3.2.1. Exterior research visitors

Alla Sheffer, University of British Columbia, one week in March
David Bommes, RWTH Aachen, one week in June
Konstantin Mischaikow Rutgers University, 6 weeks in June-July
Vin de Silva Pomona College, one month in June
Mathieu Desbrun, Caltech, one week in July
Tetsuo Asano, Japan Advanced Institute of Science and Technology, one week in September
Jian Sun (Tsinghua University, Pekin), two weeks, September.
Gert Vegter, Institute of Mathematics and Computing Science, University of Groningen, NL, three weeks in October
Pratyush Pranav, Kapteyn Astronomical Institute, University of Groningen, NL, two weeks in October
Mathijs Wintraecken, Institute of Mathematics and Computing Science, University of Groningen, NL, two weeks in October
Rien van de Weijgaert, Kapteyn Astronomical Institute, University of Groningen, NL, two weeks in October

8.3.2.2. Visiting PhD students

Kan-Le Shi, Tsinghua University Beijing, 4 months.
LFANT Project-Team (section vide)
8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR Jeunes Chercheurs “CAC”

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

The new contract CAC “Computer Algebra and Cryptography” begins in October 2009 for a period of 4 years. This project will investigate the areas of cryptography and computer algebra, and their influence on the security and integrity of digital data. In CAC, we plan to use basic tools of computer algebra to evaluate the security of cryptographic schemes. CAC will focus on three new challenging applications of algebraic techniques in cryptography; namely block ciphers, hash functions, and factorization with known bits. To this hand, we will use Gröbner bases techniques but also lattice tools. In this proposal, we will explore non-conventional approaches in the algebraic cryptanalysis of these problems.

8.2. ANR “HPAC”

Participants: J.-C. Faugère [contact], L. Perret, G. Renault, M. Safey El Din.

The pervasive ubiquity of parallel architectures and memory hierarchy has led to a new quest for parallel mathematical algorithms and software capable of exploiting the various levels of parallelism: from hardware acceleration technologies (multi-core and multi-processor system on chip, GPGPU, FPGA) to cluster and global computing platforms. For giving a greater scope to symbolic and algebraic computing, beyond the optimization of the application itself, the effective use of a large number of resources (memory and specialized computing units) is expected to enhance the performance multi-criteria objectives: time, resource usage, reliability, even energy consumption. The design and the implementation of mathematical algorithms with provable, adaptive and sustainable performance is a major challenge. In this context, this project² is devoted to fundamental and practical research specifically in exact linear algebra and system solving that are two essential “dwarfs” (or “killer kernels”) in scientific and algebraic computing. The project should lead to progress in matrix algorithms and challenge solving in cryptology, and should provide new insights into high performance programming and library design problems.

8.3. ANR “GeoLMI”

Participants: J.-C. Faugère, M. Safey El Din [contact].

The GeoLMI project³ aims at developing an algebraic and geometric study of linear matrix inequalities (LMI) for systems control theory. It is an interdisciplinary project at the border between information sciences (systems control), pure mathematics (algebraic geometry) and applied mathematics (optimisation). The project focuses on the geometry of determinantal varieties, on decision problems involving positive polynomials, on computational algorithms for algebraic geometry, on computational algorithms for semi-definite programming, and on applications of algebraic geometry techniques in systems control theory, namely for robust control of linear systems and polynomial optimal control.

8.3.1. European Initiatives

8.3.1.1. ECRYPT II - European Network of Excellence for Cryptology

Participants: J.C. Faugère [contact], L. Perret, G. Renaul, L. Bettale.

² http://hpac.gforge.inria.fr/
³ http://homepages.laas.fr/henrion/geolmi/
ECRYPT II - European Network of Excellence for Cryptology II is a 4-year network of excellence funded within the Information & Communication Technologies (ICT) Programme of the European Commission’s Seventh Framework Programme (FP7) under contract number ICT-2007-216676. It falls under the action line Secure, dependable and trusted infrastructures. ECRYPT II started on 1 August 2008. Its objective is to continue intensifying the collaboration of European researchers in information security. The ECRYPT II research roadmap is motivated by the changing environment and threat models in which cryptology is deployed, by the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, and by the requirements of new applications and cryptographic implementations. Its main objective is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. In order to reach this goal, 11 leading players have integrated their research capabilities within three virtual labs focusing on symmetric key algorithms (SymLab), public key algorithms and protocols (MAYA), and hardware and software implementations associate (VAMPIRE). They are joined by more than 20 adjoint members to the network who will closely collaborate with the core partners. The team joins the European Network of Excellence for Cryptology ECRYPT II this academic year as associate member.

8.3.2. International Initiatives

8.3.2.1. Royal Society Project  
**Participants:** J.C. Faugère [contact], L. Perret, L. Bettale.

Royal Society Project with the Crypto team Royal Holloway, University of London, UK.

8.3.2.2. Joint LIAMA Project ECCA  
ECCA (Exact/Certified Computation with Algebraic systems) is a LIAMA project (Reliable Software Theme) focusing on polynomial system solving. The partners are INRIA, CNRS, and CAS (Chinese Academy of Sciences). The general objectives of this project are mainly the same as those of SALSA.

8.3.2.3. ANR International Grant “EXACTA”  
**Participants:** D. Wang [contact], J.-C. Faugère, D. Lazard, L. Perret, G. Renault, M. Safey El Din.

The main objective of this project is to study and compute the solutions of nonlinear algebraic systems and their structures and properties with selected target applications using exact or certified computation. The project consists of one main task of basic research on the design and implementation of fundamental algorithms and four tasks of applied research on computational geometry, algebraic cryptanalysis, global optimization, and algebraic biology. It will last for three years (2010–2012) with 300 person-months of workforce. Its consortium is composed of strong research teams from France and China (KLMM, SKLOIS, and LMIB) in the area of solving algebraic systems with applications.

8.3.3. Scientific Animation

8.3.3.1. Journals – Associate Editors and Program Committees  
J.-C. Faugère is member of the editorial board of Journal “Mathematics in Computer Science” (Birkhäuser) and Journal “Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences” (Springer); guest editor for special issues in Journal of Symbolic Computation (Elsevier) and Journal “Mathematics in Computer Science” (Birkhäuser).

M. Safey el Din is member of the editorial board of Journal of Symbolic Computation (Elsevier).

J.-C. Faugère is PC co-chair of the third SCC conference (Santander, 2012).
D. Wang is member of the editorial board of:

- Editor-in-Chief and Managing Editor for the journal “Mathematics in Computer Science” (published by Birkhäuser/Springer, Basel).
- Executive Associate Editor-in-Chief for the journal “SCIENCE CHINA Information Sciences” (published by Science China Press, Beijing and Springer, Berlin).
- Member of the Editorial Boards for the
  - Frontiers of Computer Science in China (published by Higher Education Press, Beijing and Springer, Berlin),
  - Book Series on Mathematics Mechanization (published by Science Press, Beijing),
- Editor for the Book Series in Computational Science (published by Tsinghua University Press, Beijing).

M. Safey El Din was member of the program committees of the 36-th International Symposium on Symbolic and Algebraic Computation (San Jose, USA, June 8–11 2011) and the 13-th International Workshop on Computer Algebra in Scientific Computing (Kassel, Germany, September 5 - 9, 2011) and is member of the program committee of the 13-th International Workshop on Computer Algebra in Scientific Computing (Maribor, Slovenia, September 3 - 6, 2012).

D.Wang was member of the program committee of:

- Technical Session at ICCSA 2011 on Symbolic Computing for Dynamic Geometry (Santander, Spain, June 20–23, 2011).

8.3.3.2. Scientific visits and international seminar

M. Safey El Din was invited 2 weeks in July 2011 by L. Zhi at the Key Laboratory of Mechnanization and Mathematics (Chinese Academy of Sciences, Beijing China), 1 week at the department of Computer Science at Aarhus University (Denmark), 2 weeks in October 2011 by E. Schost at the Department of Computer Science at The University of Western Ontario (London, Canada). He is a co-organizer of the next National Days of Computer Algebra in 2012.

L. Perret was invited 2 weeks in 2011 (in July and December) by D. Lin at the SKLOIS (Chinese Academy of Sciences, Beijing China), 1 week (April, 2011) at the Stevens Institute (New-York, USA) by A. Miasnikov.

J.-C. Faugère was invited 1 week in July 2011 by D. Lin at the SKLOIS (Chinese Academy of Sciences, Beijing China).

8.3.3.3. Conferences (organization) and invited talks

J.-C. Faugère was plenary invited speaker at ECC 2011, the 15th workshop on Elliptic Curve Cryptography.

J.-C. Faugère, is member of the MEGA Advisory Board.

M. Safey El Din is co-organizer (with L. Zhi) of the First International Workshop on Certified and Reliable Computing, held in July 2011 at Nanning, China, co-organizer of the mini-symposia on Algebraic Complexity (with E. Schost) and Algorithms in Real Algebraic Geometry (with H. Hong) which have been held on the occasion of the SIAM conference on Applications of Algebraic Geometry (Raleigh, Oct. 2011).
M. Safey El Din was invited speaker at the mini-symposium on Algebraic Geometry and Optimization (SIAM conference on Optimization), the MaGIX conference (LIX, Palaiseau) and gave several talks in the mini-symposia organized during the SIAM Conference on Applications of Algebraic Geometry. He was also invited to give a talk at the joint Mathematics-Computer Science seminar at the University of Western Ontario and gave a talk at the first workshop of the GeoLMI project (Rennes, Nov. 2011).

J.-C. Faugère was invited speaker at the MaGIX conference (LIX, Palaiseau) and in the mini-symposium on Linear Algebra organized during the SIAM Conference on Applications of Algebraic Geometry (Raleigh, USA). He was also invited to give a talk at the joint Mathematics-Computer Science seminar at the University of Aarhus (Danmark).

8.3.3.4. Committees
J.-C. Faugère was a member of the evaluation committee (AERES) of the institut de mathématiques de Toulon et du Var.
M. Safey El Din is a designated member of the French National Council of the Universities (CNU).
J.-C. Faugère is member of the hiring committee in computer science at the <<Université Pierre et Marie Curie>>, <<Université de Toulon>> and <<Université Joseph Fourier>>.

8.3.4. Teaching
J.C. Faugère, L. Perret give a course on Polynomial System Solving, Computer Algebra and Applications at the “Master Parisien de Recherche en Informatique” (MPRI).
G. Renault gives a course on Computational Number Theory and Cryptology at the <<Master d’Informatique de l’Université Paris 6>>.
7. Partnerships and Cooperations

7.1. National Initiatives

- **ANR RAPIDE (01/07 → 03/11)**
  *Design and analysis of stream ciphers dedicated to constraint environments*
  Partners: LORIA (project-team CACAO/CARAMEL), INRIA (project-team SECRET), INSA Lyon (team Middleware/Security), University of Limoges (XLIM).
  151 kEuros.
  This project focuses on stream ciphers and especially on stream ciphers with an internal state governed by a non-linear transition function. We particularly draw our attention to ciphers whose characteristics make them especially fit constrained environments. The results of the project are practical as well as theoretical and concern both design and analysis of such stream ciphers.

- **ANR DEMOTIS (02/09 → 02/12)**
  *Collaborative Analysis, Evaluation and Modelling of Health Information Technology*
  http://www.demotis.org/
  ANR program: ARPEGE (Systèmes Embarques et Grandes Infrastructures)
  Partners: Sopinspace, INRIA (project-teams SECRET and SMIS), CNRS/CECOJI
  55 kEuros.
  DEMOTIS brings together computer scientists and legal scholars. The project experiments new methods for the multidisciplinary design of large information systems that have to take in account legal, social and technical constraints. Its main field of application is personal health information systems. Most notably, work is conducted in priority on the infrastructure for the French personal medical file system (DMP) and secondarily on the data infrastructure for the research and public health networks associated with specific diseases (AIDS, cancer). The aim is to understand how the interconnection between the legal and technical domains affects the design of such data infrastructures.

- **ANR SAPHIR-2 (03/09 → 03/13)**
  *Security and Analysis of Primitives of Hashing Innovatory and Recent 2*
  http://www.saphir2.fr/
  ANR program: VERSO (Reseaux du Futur et Services)
  Partners: France Telecom, Gemalto, Cryptolog international, EADS SN, Sagem Securite, ENS/LIENS, UVSQ/PRISM, INRIA (project-team SECRET), ANSSI
  153 kEuros
  This industrial research project aims at participating to the NIST competition (cryptanalysis, implementations, optimizations, etc.), and in supporting the SHA-3 candidates proposed by its partners.

- **ANR COCQ (01/09 → 01/12)**
  *Codes correcteurs quantiques*
  http://www-roc.inria.fr/secret/Jean-Pierre.Tillich/COCQ.html
  ANR program: Domaines emergents
  Partners: ENSEA, INRIA (project-team SECRET), Université de Bordeaux, Telecom ParisTech
  117 kEuros
  This project deals with the development of fundamental research on error correcting codes for quantum channels. In particular, we aim to suggest suitable generalizations to the quantum setting of the best known families of quantum codes (such as LDPC or turbo-codes) and to analyze their performance.
- **ANR BLOC** (10/11 → 09/15)
  "Conception et analyse de chiffrements par blocs efficaces pour les environnements contraints"
  ANR program: Ingénierie numérique et sécurité
  Partners: INSA Lyon, INRIA (project-team SECRET), University of Limoges (XLIM), CryptoExperts
  446 kEuros
  The BLOC project aims at providing strong theoretical and practical results in the domain of cryptanalyses and design of block ciphers.

- **ANR KISS** (12/11 → 12/15)
  "Keep your personal Information Safe and Secure"
  ANR program: Ingénierie numérique et sécurité
  Partners: INRIA (project-teams SMIS and SECRET), LIRIS, Gemalto, UVSQ (Prism), Conseil Général des Yvelines
  64 kEuros
  The KISS project builds upon the emergence of new portable and secure devices known as Secure Portable Tokens (e.g., mass storage SIM cards, secure USB sticks, smart sensors) combining the security of smart cards and the storage capacity of NAND Flash chips. The idea promoted in KISS is to embed, in such devices, software components capable of acquiring, storing and managing securely personal data.

- **French Ministry of Defense** (01/11 → 12/13)
  "Funding for the supervision of Marion Bellard’s PhD."
  30 kEuros.

### 7.2. European Initiatives

Associate member of the ECRYPT II European network of excellence (08/08 → 07/12) [http://www.ecrypt.eu.org/](http://www.ecrypt.eu.org/)

#### 7.2.1. Major European Organizations with which you have followed Collaborations

- Otto-von-Guericke Universität Magdeburg, Institut für Algebra und Geometrie (Germany)
  - Study of Boolean functions for cryptographic applications
- DTU - Danmarks Tekniske Universitet, Department of Mathematics
  - Symmetric cryptography and code-based cryptography

### 7.3. International Initiatives

#### 7.3.1. Visits of International Scientists

- Gohar Kyureghyan, Otto-von-Guericke Universität Magdeburg, Germany, from October 2011 to June 2012
- Kaisa Nyberg, Aalto University, Finland, November 6-8.
- Christiane Peters, Danmarks Tekniske Universitet, Copenhagen, Denmark, November 13-18.
- Stefan Heyse, Ruhr-Universität Bochum, Germany, November 13-18.

#### 7.3.2. Visits to International Partners

- EPFL, Lausanne, Switzerland, September 1-30, invitation to the *Combinatorial, Algebraic and Algorithmic Aspects of Coding Theory* Program of the Centre interfacultaire Bernoulli, (N. Sendrier)
- EPFL, Lausanne, Switzerland, September 7-15, invitation to the *Combinatorial, Algebraic and Algorithmic Aspects of Coding Theory* Program of the Centre interfacultaire Bernoulli, (P. Charpin)
- EPFL, Lausanne, Switzerland, September 5-29, invitation to the *Combinatorial, Algebraic and Algorithmic Aspects of Coding Theory* Program of the Centre interfacultaire Bernoulli, (JP. Tillich)
8. Partnerships and Cooperations

8.1. Regional Initiatives

- DIGITEO contributed the operational funding for the project AMIGA (Advanced Methods for Isogeny Graph Analysis), with B. Smith as the scientific leader of the project. On a national level, the DGA contributed a postdoctoral salary to the project (see National Initiatives).

8.2. National Initiatives

- The DGA funded a postdoctoral researcher’s salary for Sorina Ionica, allowing her to join TANC for one year (10/2010–09/2011) as a postdoctoral researcher for the AMIGA project.
- The team received DGA funding for the project DIFMAT, joint with ENSTA, to find good MDS matrices, which are used for diffusion in block ciphers. The period is October 2011–September 2012, eventually renewable one year.

8.3. European Initiatives

8.3.1. Major European Organizations with which Tanc has followed Collaborations

Partner 1: Ulm Universität, TAIT group, Germany.
Subject 1: bridging Ulm’s unique decoding with Guruswami-Sudan list decoding. Funded by a PHC Hubert Curien.

8.4. International Initiatives

8.4.1. INRIA International Partners

- DTU, Denmark.

8.4.2. Visits of International Scientists

- Kamal Khuri–Makdisi, American University of Beirut, two weeks.
- Iwan Duursma, University of Illinois at Urbana Champaign, two weeks.
VEGAS Project-Team (section vide)
ALF Project-Team

8. Partnerships and Cooperations

8.1. HiPEAC2 NoEs

Participants: François Bodin, Pierre Michaud, Erven Rohou, André Seznec.

F. Bodin, P. Michaud, A. Seznec and E. Rohou are members of the European Network of Excellence HiPEAC2. HiPEAC2 addresses the design and implementation of high-performance commodity computing devices in the 10+ year horizon, covering both the processor design, the optimising compiler infrastructure, and the evaluation of upcoming applications made possible by the increased computing power of future devices. The collaboration with University of Cyprus (Damien Hardy’s internship) has been funded by the HiPEAC2 NoE.

8.2. Brittany region fellowship

Participants: Ricardo Andrés Velasquéz, Pierre Michaud, André Seznec.

The Brittany region is funding a Ph.D. fellowship for Ricardo Velasquez on the topic “Fast hybrid multicore architecture simulation”.

8.3. PetaQCD

Participants: Junjie Lai, André Seznec.

Simulation of Lattice QCD is a challenging computational problem that requires very high performance exceeding sustained Petaflops/s. The ANR PetaQCD project combines research groups from computer science, physics and two SMEs (CAPS Entreprise, Kerlabs) to address the challenges of the design of LQCD oriented supercomputer.

8.4. DAL: ERC AdG 2010- 267175, 04-2011/03-2016


André Seznec has received an ERC Advanced grant.

We envision that, around 2020, the processor chips will feature a few complex cores and many (may be 1000s) simpler, more silicon and power effective cores. In the DAL research project, we will explore the microarchitecture techniques that will be needed to enable high performance on such heterogeneous processor chips. Very high performance will be required on both sequential sections -legacy sequential codes, sequential sections of parallel applications- and critical threads on parallel applications -e.g. the main thread controlling the application. Our research will focus on enhancing single process performance. On the microarchitecture side, we will explore both a radically new approach, the sequential accelerator, and more conventional processor architectures. We will also study how to exploit heterogeneous multicore architectures to enhance sequential thread performance.

For more informations, see http://www.irisa.fr/alf/dal .
CAIRN Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Organisation by A. Tisserand of working group on cryptography and digital security between research teams from University of Brest, University of Lorient and University of Rennes.

The Grappas project, funded by the Equipe Projet Transversale program from Université Européenne de Bretagne (UEB) aims at evaluating (and improving) the efficiency of automatic parallelization techniques for accelerating electromagnetic FDTD simulations of antennas on GPUs (Graphical Processing Units). The project is a joint project between IETR (D. Thouroude and R. Sauleau) and IRISA (S. Derrien).

8.2. National Initiatives

The CAIRN team has currently some collaboration with the following laboratories: CEA List, SATIE ENS Cachan, LEAT Nice, Lab-Sticc (Lorient, Brest), LIRMM (Montpellier, Perpignan), ETIS Cergy, LIP6 Paris, IETR Rennes, Ireena Nantes; and with the following INRIA project-teams: Arénaire, Compsys, Swing, Symbiose, TexMex.

The team participates in the activities of the following research organization of CNRS (GdR for in French “Groupe de Recherche”):

- GdR SOC-SIP (System On Chip & System In Package), working groups on reconfigurable architectures, embedded software for SoC, low power issues. See http://www2.lirmm.fr/~w3mic/SOCSIP/index.php. CAIRN is the leader of the group on reconfigurable architectures.
- GdR ISIS (Information Signal ImageS), working group on Algorithms Architectures Adequation.
- GdR ASR (Architectures Systèmes et Réseaux)
- GdR IM (Informatique Mathématiques), C2 working group on Codes and Cryptography

8.3. European Initiatives

8.3.1. FP7 Projects

Program: FP7-ICT-2011-7
Project acronym: Flextiles
Coordinator: Thales
Other partners: Thales (FR), URI (FR), KIT (GE), TU/e (NL), CSEM (SW), CEA LETI (FR), Sundance (UK)
Project title: Self Adaptive Heterogeneous Manycore Based on Flexible Tiles
Abstract: A major challenge in computing is to leverage multi-core technology to develop energy-efficient high performance systems. This is critical for embedded systems with a very limited energy budget as well as for supercomputers in terms of sustainability. Moreover the efficient programming of multi-core architectures, as we move towards manycores with more than a thousand cores predicted by 2020, remains an unresolved issue. The FlexTiles project will define and develop an energy-efficient yet programmable heterogeneous manycore platform with self-adaptive capabilities. The manycore will be associated with an innovative virtualisation layer and a dedicated tool-flow to improve programming efficiency, reduce the impact on time to market and reduce the development cost by 20 to 50%. FlexTiles will raise the accessibility of the manycore technology to industry - from small SMEs to large companies - thanks to its programming efficiency and its ability to adapt to the targeted domain using embedded reconﬁgurable technologies.
Program: FP7-ICT-2011-7
Project acronym: Alma
Project title: Architecture oriented parallelization for high performance embedded Multicore systems using scilab
Coordinator: KIT
Other partners: KIT (GE), UR1 (FR), Recore Systems (NL), Univ. of Peloponnese (GR), TEI-MES (GR), Intracom SA (GR), Fraunhofer (GE)

Abstract: The mapping process of high performance embedded applications to today’s multiprocessor system on chip devices suffers from a complex toolchain and programming process. The problem here is the expression of parallelism with a pure imperative programming language which is commonly C. This traditional approach limits the mapping, partitioning and the generation of optimized parallel code, and consequently the achievable performance and power consumption of applications from different domains. The Architecture oriented parallelization for high performance embedded Multicore systems using scilab (ALMA) project aims to bridge these hurdles through the introduction and exploitation of a Scilab-based toolchain which enables the efficient mapping of applications on multiprocessor platforms from high level of abstraction. This holistic solution of the toolchain allows the complexity of both the application and the architecture to be hidden, which leads to a better acceptance, reduced development cost and shorter time-to-market. Driven by the technology restrictions in chip design, the end of Moore’s law and an unavoidable increasing request of computing performance, ALMA is a fundamental step forward in the necessary introduction of novel computing paradigms and methodologies. ALMA helps to strengthen the position of the EU in the world market of multiprocessor targeted software toolchains. The challenging research will be achieved by the unique ALMA consortium which brings together industry and academia. High class partners from industry such as Recore and Intracom, will contribute their expertise in reconfigurable hardware technology for multi-core systems-on-chip, software development tools and real world applications. The academic partners will contribute their outstanding expertise in reconfigurable computing and compilation tools development.

8.3.2. Collaborations in European Programs, except FP7

Program: ITEA2
Project acronym: GEODES
Project title: Global Energy Optimization for Distributed Embedded Systems
Coordinator: Thales
Other partners: Thales (FR, IT, NL), Sensaris (FR), CNRS (LEAT and IRISA) (FR), CETMEF/MARTEC (FR), Infineon (AU), Thomson (FR), TUV (AU), UAQ (IT), Phillips (NL), Organo (AU), TI-WMC (NL)

Abstract: The GEODES project will provide design techniques, embedded software and accompanying tools needed to face the challenge of allowing long power-autonomy of features rich and connected embedded systems, which are becoming pervasive and whose usage is significantly rising. It approaches this challenge by considering all system levels, and notably emphasizes the distributed system view. GEODES is an ITEA2 project which involves partners from France, Austria, Italy and the Netherlands. In GEODES Cairn will provide to partners the PowWow very power sensor platform including reconfigurable hardware accelerators. CAIRN will also contribute on link and MAC layers strategies to a global optimization of the energy, and define and optimize advanced signal processing, error detection and correction and medium access (MAC) techniques in order to reduce the transmit power as well as the useless listening of the communication media. In particular, the case of cooperative strategies like cooperative MIMO or relaying techniques will be investigated.
8.3.3. Major European Organizations with which Cairn has followed Collaborations

Imec (Belgium)
Scenario-based fixed-point data format refinement to enable energy-scalable of Software Defined Radios (SDR)

University of Erlangen-Nuremberg and Dresden University of Technology (Germany)
Massively parallel embedded reconfigurable architectures and on dynamic reconfiguration optimisation in the mesh fabric

University of Paderborn (Germany)
Spatio-temporal scheduling for reconfigurable systems

Lund University (Sweden)
Constraints programming approach application in the reconfigurable data-paths synthesis flow

Computer Vision and Robotic Group of the Institute for Informatics and Applications at the University of Girona (Spain)
Parallel architectures for vision algorithms applied to underwater robot

University of Eindhoven (Netherlands)
Reconfigurable data-path synthesis

University of Leiden (Netherlands)
Parallel architecture synthesis

Code and Cryptography group of University College Cork (Ireland)
Arithmetic operators for cryptography

Ecole Polytechnique Fédérale de Lausanne - EPFL (Switzerland)
Optimization of systems using fixed-point arithmetic

Technical University of Madrid - UPM (Spain)
Optimization of systems using fixed-point arithmetic

Technical University of Tampere, University of Oulu (Finland)
Reconfigurable Video Coding

Thomas Chabrier spent four months in the group of Prof. William P. Marnane at University College Cork, Ireland, from June.

8.4. International Initiatives

8.4.1. INRIA Associate Teams

8.4.1.1. LRS: Loop unRolling Stones

Title: Loop unRolling Stones: compiling in the polyhedral model
INRIA principal investigator: Steven Derrien
International Partner:
Institution: Colorado State University (United States)
Laboratory: Mélange Group

Duration: 2010 - 2012

Abstract: The goal of the team is twofold: (i) Propose new methodologies and algorithms to tackle some of the open problems in automatic parallelization and high level hardware synthesis from nested loop specifications. In particular, we would like to address the problem of parallelization of complex bioinformatics algorithms based of sophisticated dynamic programming algorithms, for which we would like to propose efficient parallelization schemes for both FPGAs (Field Programmable Gate Arrays) and GPUs (Graphical Processing Units). (ii) Provide a common open software infrastructure based on (modern/cutting edge) software engineering techniques (Model Driven Software Development) so as to help researchers prototyping new ideas and concept in the domain of optimizing compilers. Our goal being to be able to make our in-house software completely interoperable. As far as the second point is concerned, the CAIRN group at IRISA already has a strong commitment in using Model Driven Software Design technique and has set up a very fruitful collaboration with the Triskell EPI in Rennes. This is not yet the case of the Mélange group, however we expect to leverage on another Associate Team (the MoCaa EA) which also involves groups from CSU (Software Insurance Lab) and IRISA (Triskell group) to strengthen the connections on the CSU side.

8.4.2. INRIA International Partners

Los Alamos National Laboratory (USA)
Reconfigurable architectures for scientific processing

LRTS laboratory, Laval University in Québec (Canada)
Architectures for MIMO systems, Wireless Sensor Networks, INRIA Associate Team (2006-2008)

LSSI laboratory, Québec University in Trois-Rivières (Canada)
Design of architectures for digital filters and mobile communications

Computer Science Department, Colorado State University in Fort-Collins (USA)
Loop parallelization, development of high-level synthesis tools, INRIA Associate Team (2010-2012)

University of Adelaide (Australia)
Arithmetic operators

University of Queensland (Australia)
Reconfigurable architectures for scientific processing

University of California, Riverside (USA)
Optimized image processing applications synthesis

VLSI CAD lab, Electrical and Computer Engineering Department, University of Massachusetts at Amherst (USA)
CAD tools for arithmetic datapath synthesis and optimization

University of Douala, University of Yaoundé and University of Dschang (Cameroun)
Models and tools for parallelization, SARIMA GIS for the development of research laboratories in Mathematics and Computer Science in Africa

ENIT, Univ. Tunis (Tunisia)
Architectures for mobile communications

Steven Derrien spent two months in the group of Professor Sanjay Rajopdahye at Colorado State University, US, in May and June.

8.5. Exterior research visitors

Prof. Gabriel Caffarena (University CEU-San Pablo, Madrid) for one week in June.
PhD Student Nabil Ghanmy (University of Sfax, Tunisia) for one month in September.
Prof. Sébastien Roy for one month and a half in June.
Dr. Nicolas Veyrat-Charvillon (Crypto Group from the Université Catholique de Louvain, Belgium for 4 days in May-June.
PhD Student Tomofumi Yuki (Colorado State University, USA) for two months in November and December.
CAMUS Team

7. Partnerships and Cooperations

7.1. National Initiatives

Philippe Clauss, Alain Ketterlin and Vincent Loechner are involved in the proposition of an INRIA Large Wingspan Project (Action d’Envergure Nationale) entitled “Software for multicores and hardware accelerators” and regrouping several french teams doing researches in compilers, parallel computing and program optimization. Philippe Clauss shares the head of the project with Gilles Muller of the INRIA REGAL team. A new version of the project will be submitted to INRIA at the end of 2011.

7.2. International Initiatives

7.2.1. INRIA Associate Teams

7.2.1.1. ANCOME

Title: Memory and applications memory behavior
INRIA principal investigator: Philippe Clauss
International Partner:
Institution: Universidad de Buenos Aires (Argentina)
Laboratory: Departamento de Computacion, Facultad de Ciencias Exactas y Naturales
Duration: 2011 - 2013
See also: http://lafhis.dc.uba.ar/wiki/index.php/EA-Ancome
This associate team focuses on developing original methods for the analysis of programs memory behavior, in particular in the context of applications using dynamic memory allocation. The proposed approaches consists of analyzing and modeling the runtime behavior, where extracted properties are then verified thanks to static analysis processes. Thus pure static approaches limits are overpassed. Further, the case of multi-threaded applications run on multi-core architectures is studied in order to elaborate and extend our analysis techniques and to extract properties specific to this context. The issues are mainly concerned with the conception of real-time applications using dynamic memory allocation.

7.2.2. INRIA International Partners

Rachid Seghir, researcher and teacher at the University of Batna, Algeria, works in close collaboration with Vincent Loechner. He is the co-author of the ZPolyTrans software and of a forthcoming paper in the journal ACM Transactions on Architecture and Code Optimization [13].
Benoît Meister, Managing Engineer at Reservoir Labs, New York, USA, has collaborated with Vincent Loechner and Rachid Seghir on a forthcoming publication [13].
Jean Christophe Beyler, Senior HPC Engineer at Intel and in the International Exascale project, University of Versailles, France, is experimenting energy saving strategies using the VMAD framework of the CAMUS team.
7.2.3. Visits of International Scientists

7.2.3.1. Visits

Sergio Yovine (from Jun 6 2011 until Jun 12 2011)
Institution: Universidad de Buenos Aires (Argentina), EA INRIA Ancome

Diego Garbervetsky (from Apr 1 2011 until Apr 10 2011 and from Aug 1 2011 until Sept 2 2011)
Institution: Universidad de Buenos Aires (Argentina), EA INRIA Ancome

7.2.3.2. Internships

Luis Mastrangelo (from Mar 2011 until Aug 2011)
Subject: A Virtual Machine for Automatic Program Parallelization
Institution: Universidad de Buenos Aires (Argentina)

Bruno Cuervo Parrino (from May 2011 until Oct 2011)
Subject: Formalizing a new validation mechanism under assumptions for speculative parallelism
Institution: Universidad de Buenos Aires (Argentina)

Jose Cacherosky (from Jul 2011 until Dec 2011)
Subject: Dynamic dependence profiling for Java
Institution: Universidad de Buenos Aires (Argentina)

7.2.4. Participation In International Programs

The CAMUS team is associated to the CNRS-CONICET Associated International Laboratory France-Argentina INFINIS\(^{10}\) (INformatique Fondamentale, logIque, laNgages, vérIfication et Systèmes) inaugurated in December 2011.

\(^{10}\) https://dri-dae.cnrs-dir.fr/spip.php?article3009
8. Partnerships and Cooperations

8.1. National Initiatives

- The french compiler community is now well identified and is visible through its web-page http://compilation.gforge.inria.fr/. The “journées françaises de la compilation”, initiated in 2010 and officially animated by Fabrice Rastello and Laure Gonnord, are now well-established as a biannual event. Their local organization is handled alternately by the different research teams (Lyon in summer 2010, Aussois in Winter 2010, Dinard in Spring 2011, St Hippolyte in Autumn 2011).

- Christophe Alias and Paul Feautrier have been active participants in an effort to structure the french high-level synthesis community, including both actors from academia (TIMA, IRISA, LaSTIC, ASIM) and industry (Thales, Bull). The aim of this effort was to submit an ANR proposal for the Arpege initiative. A first version was submitted in 2010, but was rejected mostly on the ground that the project leader should have been from industry rather than academia. A revised proposal, under the leadership of the Magillem company, was submitted in March 2011 and rejected too. It seems evident in retrospect that the HLS community has yet to find a clearer balance between new research and industrial development, and that a new submission must wait for a more mature approach.

8.2. Participation in International Programs

- Fabrice Rastello has obtained a FAPEMIG-INRIA (Brazil-France) funding to collaborate with Mariza A. S. Bigonha, Fernando M. Q. Pereira, and Roberto S. Bigonha from the Federal University of Mina Gerais (UFMG) in Brazil. The work on static single information form described in Section 6.7, and the work on register allocation to handle aliasing described in Section 6.5 are part of this collaboration.

- From July 2010 till July 2011, Fabrice Rastello was in a sabbatical year at Colorado State University within the group of Sanjay Rajopadhye, and in connection with the PathScale compiler company.

8.3. Informal Contacts

- Compsys has regular contacts with Sebastian Hack at Saarland University (Saarbrücken, Germany), Philip Brisk at University of California, Riverside (Riverside, USA), and Benoît Dupont de Dinechin (Kalray, Grenoble) on back-end code optimizations.

- Compsys has regular contacts with P. Sadayappan (Ohio State University), J. (Ram) Ramanujam (Louisiana State University), and Sanjay Rajopadhye (Colorado State University), on polyhedral code transformations. Fabrice Rastello was in sabbatical in 2010-2011 in Sanjay Rajopadhye’s group. Christophe Alias is co-advising a PhD with Sanjay Rajopadhye, with an agreement to be signed between ENS-Lyon and Colorado State University.

- In France, Compsys is particularly linked with researchers such as Albert Cohen (Parkas team, Inria), Steven Derrien (Cairn team, Inria), Alain Greiner (LIP6, Paris), Alain Ketterlin (Camus team, Inria), Benoît Dupont de Dinechin (Kalray), Christophe Guillon (STMicroelectronics).

- Compsys, as some other Inria projects, is involved in the network of excellence HiPEAC (High-Performance Embedded Architecture and Compilation, http://www.hipeac.net/). Compsys is also a (distant) partner of the network of excellence Artist2 to keep an eye on the developments of MPSoC.
- Florian Brandner is collaborating with the group of Andreas Krall at the Vienna University of Technology on topics related to the processor description language xADL and on compilation for explicitly parallel processors (EPICOpt, http://www.complang.tuwien.ac.at/epicopt/). He is additionally working with Martin Schöberl from the Technical University of Denmark (DTU) on topics evolving around time-predictable computing.

- Alain Darte is in contact with Yann Orlarey from the Grame team (Lyon, “Centre National de Création Musicale”). They co-advise a Master 1 internship on some features in the development of Faust, a compiled language for real-time audio signal processing.

8.4. Visits of Research Scientists

Since Autumn 2010, several researchers visited Compsys and gave talks in our working groups.

- Amir Ben Amram (Tel Aviv University, Israel).
- Sebastian Hack (Saarland University, Germany).
- Andreas Krall and Gergö Barany (Vienna University, Austria).
- J. Ramanujam (Baton Rouge University, Louisiana).
- Antoniu Pop (Ecole des Mines, Paris).
- Benoît Dupont de Dinechin (Kalray, Grenoble).
- Alain Ketterlin (Camus Inria team, Strasbourg).
- Albert Cohen (Parkas Inria team, Paris).

8.5. Internships

In Spring 2011, three internships were advised in Compsys.

- Guillaume Andrieu (Polytech’Lille engineering school, Master level): termination of big programs.
- Alexandre Isoard (ENS-Lyon, M1 Master level): retiming for Faust.
- François Gindraud (ENS-Lyon, M1 Master level): ψ-SSA, gated-SSA, and variants.
AOSTE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. CIM PACA

Participants: Robert de Simone, Jean-François Le Tallec, Carlos Gomez Cardenas.

This ambitious regional initiative is intended to foster collaborations between local PACA industry and academia partners on the topics of microelectronic design, though mutualization of equipments, resources and R&D concerns. We are so far actively participating in the Design Platform (one of the three platforms launched in this context), of which INRIA is a founding member.

This year the platform acquired more EDA tools, such as Synopsys Virtualizer (comprising the former CoWare virtual platform environment), and Docea Power Acceptor (which we are using in the course of the ANR HeLP project). Several Aoste members attended specific training sessions on these tools.

Jean-François Le Tallec is currently completing his PhD thesis (expected January 2012), which was partly funded on the CIM PACA initiative. Apart from this, which will close the lifespan of the Sys2RTL CIM PACA project, we are looking for further collaborative associations including the team of Michel Auguin at CNRS UMR LEAT, Texas Instruments, and maybe Synopsys amongst other partners. Discussions for project submissions are underway (one difficulty here is that US companies are not familiar with European or national collaborative fundings).

8.2. National Initiatives

8.2.1. ANR RT-Simex

Participants: Julien deAntoni, Kelly Garces Pernett, Frédéric Mallet.

The RT-Simex project is dedicated to the reverse engineering of analysis traces of simulation and execution back up to the source code, or in our case most likely into the original models in a MARTE profile representation. The prime contractor is OBEO, a software publishing company based in Nantes.

8.2.2. ANR HeLP

Participants: Jean-François Le Tallec, Carlos Gomez Cardenas, Dumitru Potop Butucaru, Robert de Simone.

The ANR HeLP project deals with joint modeling of functional behavior and energy consumption for the design of low-power heterogeneous SoCs. Partners are ST Microelectronics and Docea Power (SME) as industrial; INRIA, UNS (UMR LEAT), and VERIMAG (coordinator) as academics. Our goal in this project is twofold: first, combine SoC modeling with temporal behavior and logical time (as obtained in the ID/TL-M collaboration, see 7.1) with energy/power modeling as extra annotations on MARTE models; second, compare the capacities of high-level SystemC TLM abstraction with that of Esterel seen as a multiclock formalism based on logical abstract time.

The PhD thesis of Jean-François Le Tallec, originally funded in the CIM PACA programme, is being continued as part of the HeLP project. Additionally, part of Carlos Gomez Cardenas PhD work on metamodelling in MARTE of power consumption and links to dedicated tools is also presented to this project (in connection with complementary work at LEAT on this topic).

8.2.3. FUI Lambda

Participants: Charles André, Frédéric Mallet.
In the context of embedded software deployed on "off the shelf" execution platforms, the **LAMBDA** project has two major goals:

- To demonstrate the technical feasibility and the interest of model libraries by formalizing the key properties of execution platforms,
- To reconcile appropriated standards (SysML, MARTE, AADL, IP-XACT) with de facto standards (already implemented by widespread analysis and simulation tools.)

In this context we provided expertise mainly on the SyncCharts, MARTE, and SysML formalisms (our involvement in this project is only marginal, in support of other INRIA teams). The final project review was held at the end of September, 2011.

**8.2.4. FUI PARSEC**

**Participants:** Dumitru Potop Butucaru, Thomas Carle, Virginia Papailiopoulou, Yves Sorel.

The **Pars** project is a large collaboration with partners such as Thales, CEA, Elidiss, INRIA, Systerel, OpenWide, Alstom, and TelecomParisTech. The project aims at defining a framework for the development of distributed real-time embedded systems that are subject to strict certification standards such as DO-178B (for avionics), IEC 61508 (for transportation systems), or ISO/IEC 15408 (the Common Criteria for information technology security evaluation).

The AOSTE team uses its expertise in the modeling and distributed real-time implementation of embedded applications using synchronous formalisms and associated tools. The two main scientific challenges of the project are (1) a better modeling of the distributed implementation architectures, allowing code generation for novel architectures and better code generation for architectures we currently handle, and (2) the modeling and efficient implementation of mode changes, as they are specified in an industrial context.

Virginia Papailiopoulou was partially funded as post-doc on this project, which will also finance the PhD scholarship of Thomas Carle.

**8.2.5. FUI P**

**Participants:** Dumitru Potop Butucaru, Yves Sorel.

The main purpose of this project is to define a **Pivot** format that allows the automatic generation of certified code for safety critical applications. Partners of this project are: Aboard, ACG, Airbus, Adacore, Altair, Astrium, Atos, Continental, ENPC, INRIA, IRIT, LABSTICC, ONERA, RCF, SAGEM, Scilab, STI, Thales-AS, Thales-AV.

The project was only recently started, and first concrete results are expected for next year.

**8.2.6. AS GeMoC**

**Participants:** Julien deAntoni, Kelly Garces Pernett, Frédéric Mallet.

The purpose of the Action Spécifique by CNRS is to gather the French research community working around heterogeneous modeling of complex systems. Funding was granted for a couple of internal visits and plenary meetings this year. TimeSquare was presented in this context, and a survey of methods (including ours) is being conducted.

**8.2.7. CNRS GDR ASR ACTRISS group**

**Participant:** Laurent George.

The ACTRISS working group, supported by GDR ASR (CNRS, France), is meant to federate and promote research on real-time systems in France. A workshop on multiprocessor systems was organized in this framework in May 2011 (see [http://www-roc.inria.fr/who/Laurent.George/ACTRISS/](http://www-roc.inria.fr/who/Laurent.George/ACTRISS/)).
8.3. European Initiatives

8.3.1. FP7 Projects

8.3.1.1. CESAR

Participants: Régis Gascon, Yves Sorel, Robert de Simone.

Title: CESAR
Duration: February 2009 - July 2012
Coordinator: AVL - GmbH (Austria)

Others partners: AIRBUS Operations GbmH (Germany), AIRBUS Operations SAS (France), ABB AS (Norway), ABB AB (Sweden), AbsInt Angewandte Informatik GmbH (Germany), ACCIONA Infraestructuras S.A. (Spain), Ansaldo STS S.p.A. (Italy), ASTRIUM SAS (France), AIRBUS Operations Limited (United Kingdom), Aristotle University of Thessaloniki (Greece), Commissariat à l’Energie Atomique (France), CNRS (France), Centro Ricerche Fiat S.C.p.A. (Italy), Critical Software S.A. (Poland), Danieli Automation S.p.A. (Italy), Delphi France SAS (France), Deutsches Zentrum für Luft- und Raumfahrt e.V. (Germany), Dassault Systemes (France), EADS Deutschland GmbH (Germany), Fondación Tecnalia Research & Innovation (Italy), ESTEREL Technologies SA (France), Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung e.V. (Germany), Auviation Software Limited (United Kingdom), Hellenic Aerospace Industry S.A. (Greece), Infineon Technologies Austria AG (Austria), Infineon Technologies AG (Germany), Institut National de Recherche en Informatique et Automatique (France), ATHENA - Industrial Systems Institute (Greece), Kungliga Tekniska Högskolan (Sweden), Norwegian University of Science and Technology (Norway), National Technical University of Athens (Greece), OFFIS e.V. (Germany), Office national d’Etudes et de Recherches Aéropatielles (France), BTC - Embedded Systems AG (Germany), Oxford University (United Kingdom), Sagem Défense Sécurité (France), AleniaSIA Spa (Italy), Siemens AG (Germany), Stiftelsen SINTEF (Norway), Quintec Associates (Thales Consulting and Engineering) (United Kingdom), Thales Communications S.A. (France), Thales Avionics S.A. (France), Thales TRT (France), Alma Mater Studiorum - Università di Bologna (Italy), The University of Manchester (United Kingdom), Università degli Studi di Trieste (Italy), The Virtual Vehicle Competence Center (Austria), Volvo Technology Corporation (Sweden), Messier-Bugatti S.A. (France), TURBOMECA (France), SNECMA S.A. (France), Geensoft (France), Selex Sistemi Integrati (Italy).

See also: http://www.cesarproject.eu/

Abstract: CESAR stands for Cost-efficient methods and processes for safety relevant embedded systems and is a European funded project from ARTEMIS JOINT UNDERTAKING (JU). The three transportation domains automotive, aerospace, and rail, as well as the automation domain share the need to develop ultra-reliable embedded systems to meet societal demands for increased mobility and ensuring safety in a highly competitive global market. To maintain the European leading edge position in the transportation as well as automation market, CESAR aims to boost cost efficiency of embedded systems development and safety and certification processes by an order of magnitude. CESAR pursues a multi-domain approach integrating large enterprises, suppliers, SME’s and vendors of cross sectoral domains and cooperating with leading research organizations and innovative SME’s.

8.3.1.2. PRESTO

Participants: Frédéric Mallet, Marie-Agnès Peraldi Frati, Julien DeAntoni.

Title: PRESTO
Duration: April 2011 - March 2014
Coordinator: Miltech (Greece)
Abstract: The PRESTO project aims at improving test-based embedded systems development and validation, while considering the constraints of industrial development processes. This project is based on the integration of test traces exploitation, along with platform models and design space exploration techniques. Such traces are obtained by execution of test patterns, during the software integration design phase, meant to validate system requirements. The expected result of the project is to establish functional and performance analysis and platform optimisation at early stage of the design development. The approach of PRESTO is to model the software/hardware allocation, by the use of modelling frameworks, such as the UML profile for model-driven development of Real Time and Embedded Systems (MARTE). The analysis tools, among them timing analysis including Worst Case Execution Time (WCET) analysis, scheduling analysis and possibly more abstract system-level timing analysis techniques will receive as inputs on the one hand information from the performance modelling of the HW/SW-platform, and on the other hand behavioural information of the software design from tests results of the integration test execution.

The PRESTO project (ARTEMIS-2010-1-269362) is co-funded by the European Commission under the ARTEMIS Joint Undertaking Programme.

8.3.2. Collaborations in European Programs, except FP7

8.3.2.1. ITEA2 Timmo2U

Participants: Marie-Agnès Peraldi Frati, Julien DeAntoni, Arda Goknil, Jean-Vivien Millo, Yves Sorel.

Program: ITEA2
Project acronym: Timmo2Use
Project title: TIMing MOdel, TOols, algorithms, languages, methodology, and USE cases
Duration: October 2010 - October 2012
Coordinator: Volvo Technology AB (Sweden)

Other partners: AbsInt Angewandte Informatik GmbH (Germany), Arcticus Systems AB (Sweden), Chalmers University of Technology (Sweden), Continental Automotive GmbH (Germany), Delphi France SAS (France), dSPACE GmbH (Germany), INCHRON GmbH (Germany), Institut National de Recherche en Informatique et Automatique (France), Mälardalen University (Sweden), Rapita Systems Ltd. (United Kingdom), RealTime-at-Work (France), Robert Bosch GmbH (Germany), Syntavision GmbH (Germany), Technische Universität Braunschweig (Germany), Time Critical Networks (Sweden), Universität Paderborn (Germany).

See also: http://timmo-2-use.org/

Abstract: TIMMO develops different types of timing constraints and dynamic behaviour in the supply chain of the complex development process is of crucial importance when designing distributed real-time automotive systems. TIMMO-2-USE stands for TIMing MOdel - TOols, algorithms, languages, methodology, and USE cases which summarizes the main objectives of the project, i.e., the development of novel tools, algorithms, languages, and a methodology validated by use cases.

The project provides partial funding for the postdoctoral positions of Jean-Vivien Millo and Arda Goknil.
8.3.2.2.ITEA2 OpenProd

Participants: Simon Nivault, Yves Sorel.

Program: ITEA2

Project acronym: OpenProd

Project title: Open Model-Driven Whole-Product Development and Simulation Environment

Duration: June 2009 - May 2012

Coordinator: Siemens Industrial TurboMachinery AB (Sweden)

Other partners: Appedge (France), Bosch Rexroth AG (Sweden), CEA LIST (France), EADS Innovation Works (France), Electricité De France (France), Equa Simulation AB (Sweden), ETH Zürich (Switzerland), Fachhochschule Bielefeld (Germany), Fraunhofer FIRST (Germany), IFP (France), INRIA Rocquencourt (France), INSA Lyon (France), Linköping University (Sweden), LMS Imagine (France), MathCore Engineering AB (Sweden), Metso Automation (France), Nokia (Finland), Plexim GmbH (Germany), Pöyry Forest Industry (Finland), PSA Peugeot Citroen (France), Siemens AG, Sector Energy (Germany), SKF Sverige AB (Sweden), Technische Universität Braunschweig (Germany), TLK Thermo GmbH (Germany), VTT Technical Research Centre (Finland), XRG Simulation GmbH (Germany).

See also: http://www.ida.liu.se/~pelab/OpenProd/

Abstract: The OPENPROD project is developing an open whole-product, model-driven systems development, modelling and simulation (M&S) environment that integrates the leading open industrial software development platform Eclipse with open-source modelling and simulation tools such as OpenModelica and industrial M&S tools and applications. The project will enable a more formalised validation of production to cut time to market and ensure higher quality, using open solutions which will have a high impact, based on easy uptake and wide dissemination.

8.4. International Initiatives

8.4.1. INRIA International Partners

We are continuing a collaboration with East China Normal University (ECNU) in Shanghai, through the Software Engineering Institute headed by He Jifeng. This collaboration is shared with the OASIS EPI. As part of this we held a dedicated Workshop in Shanghai in November, met some of the LIAMA staff while there, and participated to a proposal for a new Associated Team mainly headed by OASIS. We are also hosting for a year Yin Ling, a PhD student from ECNU, on a chinese government grant.

8.4.2. Participation In International Programs

8.4.2.1. NoE Artist-Design

We are affiliated to this european Network of Excellence Artist-Design (http://www.artist-embedded.org/artist/), which sponsors events in our field.
DART Project-Team (section vide)
7. Partnerships and Cooperations

7.1. National Actions

Participants: Jean-Pierre Talpin, Thierry Gautier, Paul Le Guernic.

7.1.1. ONERA/Thales TORRENTS working group

Team Espresso participates to the TORRENTS working group since its inaugural seminar in 2010. TORRENTS is a federates the activities related to time-oriented embedded systems being primarily carried out in research labs in Toulouse. It is supported by the RTRA STAE foundation. TORRENTS aims at proposing a methodology for time-based design of embedded aerospace real-time systems.

http://www.irit.fr/torrents

7.2. European Actions

Participants: Thierry Gautier, Paul Le Guernic, Jean-Pierre Talpin, Eric Vecchie.

7.2.1. Network of excellence ARTIST2

The Espresso project-team participates to the Artist2 network of excellence. Detailed presentations on the aim and scope of the network can be found in the book [1] and the website http://www.artist-embedded.org/FP6 of the project. In particular, we have contributed to a survey of real-time programming languages edited by Alan Burns [42].

7.3. International collaborations

Participants: Loïc Besnard, Adnan Bouakaz, Thierry Gautier, Paul Le Guernic, Sun Ke, Jean-Pierre Talpin.

7.3.1. INRIA associate project POLYCORE

In the frame of three consecutive joint NSF-INRIA and INRIA associated project programs, together with additional funds from INRIA scientific direction, INRIA-Rennes, the University of Rennes, the ARTIST NoE, we have established a long-lasting and scientifically fruitful collaboration with the Fermat Laboratory at Virginia Tech (Pr. Sandeep Shukla) and UC San Diego (Pr. Rajesh Gupta). The collaboration started in 2002 and was prolonged until 2009 with the one-year sabbatical of Sandeep Shukla as invited professor. This collaboration resulted in the joint publication of 10 scientific books and series volumes as well as 22 international journal and conference articles. In the frame of this collaboration, we jointly created the ACM-IEEE MEMOCODE (http://www.memocode-conference.com) international symposium series as well as the FMGALS international workshop series. Finally, we jointly organized four tutorials. This series of collaborations resulted in a technology transfer of the Polychrony toolset with the launch of the project CodeSyn at Virginia Tech, funded by the US Air Force Research Laboratories (AFRL), and now employs one of our former post-doctorates, Julien Ouy.

Our collaboration is now been renewed in the frame of the 2011 INRIA Associate Project POLYCORE and extended to a key additional partner, the Embedded System Group of Pr. Klaus Schneider at TU Kaiserslautern.

Our joint project starts from an observation that can be shared with anyone how experienced with multi-threaded programming, to acknowledge the difficulty of designing and implementing such software. Resolving concurrency, synchronization, and coordination issues, and tackling the non-determinism germane in multi-threaded software is extremely difficult. Ensuring correctness with respect to the specification and deterministic behavior is however necessary for safe execution of such code on embedded architectures. It is therefore desirable to synthesize multi-threaded code from formal specifications using a provably 'correct-by-construction' approach.
In Europe, it has been widely claimed that the embedded software for 'fly-by-wire' was mostly automatically generated using tools based on the synchronous programming models. Unfortunately, software generated in those contexts usually operate in a time-triggered execution model. Such models are simple but way less efficient than multi-threaded software when run on multi-core processors, just because of the periodic synchronization overhead.

While time-triggered programming model simplifies code generation, our shared intuition is that multi-rate event driven execution models are much more efficiently adapted to tackle embedded software design challenges posed by forthcoming heterogeneous multi-core embedded architectures. To this aim, we plan to develop formal models, methods, algorithms and techniques for generating provably correct multi-threaded reactive real-time embedded software for mission-critical applications. For scalable modeling of larger embedded software systems, the specification formalism has to be compositional and hierarchical.

Our proposed formalism entails a model of computation (MoC) based on a multi-rate synchronous data-flow paradigm: Polychrony. It aims at combining the capabilities of Esterel/Quartz (ESG/TUKL) for correctly programming synchronous modules, with the capabilities of Polychrony (INRIA), to give high-level abstractions of complex multi-clocked networks and yet provide powerful communication and scheduling code synthesis, all combined in an application-specific modeling and programming environment, design in collaboration with Virginia Tech and the AFRL (whom we submitted the white-paper of a project proposal for funding in 2012).
LICT Exploratory Action

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. LISE (ANR)

The LISE project started in 2008 and is funded by the ANR SESUR programme. LISE is coordinated by LICIT and involves the AMAZONES and POP ARTINRIA project-teams, the Law Faculty of Versailles Saint-Quentin, the Law Faculty of Caen, VERIMAG and SUPELEC.

One of the motivations of the LISE project is the fact that, as observed by several authors, software quality and patterns of security frauds are directly related to legal liability patterns. But the precise definition of the expected functionalities of software systems is quite a challenge, not to mention the use of such definition as a basis for a liability agreement. Taking up this challenge was precisely the objective of LISE. To achieve this goal, the project has studied liability issues both from the legal and the technical points of view with the aim to put forward methods (1) to define liability in a precise and unambiguous way and (2) to establish liability in case of disagreement [5], [12], [11].

7.1.2. FLUOR (ANR)

The FLUOR project started in 2008 and is funded by the ANR SESUR programme. FLUOR is coordinated by ENSTB and involves the CNRS (IODE), INRIA (LICIT), the LIUPPA (University of Pau), SWID and the University of Polynésie Française.

The context of the FLUOR project is the protection of corporate documents circulating within companies. The main objectives of the project are (1) to unify information flow models and usage control models and (2) to analyse the legal issues raised by the use of these documents. Emphasis is put by LICIT on the specification of obligations within organizations [10].

7.2. European Initiatives

7.2.1. FP7 Projet

7.2.1.1. FI-WARE

Title: Future Internet Ware.
Type: COOPERATION (ICT).
Defi: PPP FI: Technology Foundation: Future Internet Core Platform.
Duration: May 2011 - April 2014.
Coordinator: Telefonica. (Spain)
Others partners: SAP (Germany), IBM (Israel, Switzerland), Thales Communications (France), Telecom Italia (Italy), France Telecom (France), Nokia Siemens Networks (Germany, Hungary, Finland), Deutsche Telekom (Germany), Technicolor (France), Ericsson (Sweden), Atos Origin (Spain), Ingeneria Informatica (Italy), Alcatel-Lucent (Italy, Germany), Siemens (Germany), Intel (Ireland), NEC (United Kingdom), Fraunhofer Institute (Germany), University of Madrid (Spain), University of Duisburg (Germany), University of Roma La Sapienza (Italy), University of Surrey (United Kingdom).

5 http://licit.inrialpes.fr/lise/
6 http://fluor.no-ip.fr/
See also: [http://www.fi-ware.eu/](http://www.fi-ware.eu/).

Abstract: The goal of the FI-WARE project is to advance the global competitiveness of the EU economy by introducing an innovative infrastructure for cost-effective creation and delivery of services, providing high QoS and security guarantees. FI-WARE is designed to meet the demands of key market stakeholders across many different sectors, e.g., healthcare, telecommunications, and environmental services. The project unites major European industrial actors in an unique effort never seen before. The key deliverables of FI-WARE will deliver an open architecture and implementation of a novel service infrastructure, building upon generic and reusable building blocks developed in earlier research projects. This infrastructure will support emerging Future Internet (FI) services in multiple Usage Areas, and will exhibit significant and quantifiable improvements in the productivity, reliability and cost of service development and delivery - building a true foundation for the Future Internet.

### 7.3. International Initiatives

**7.3.1. Visits of International Scientists**

Visiting scientist (one month): Gerardo Schneider from the university of Chalmers (Gothenburg, Sweden).
PARKAS Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. INRIA Action d’Envergure Synchronics

Participants: Albert Cohen, Marc Pouzet [contact], Louis Mandel.

This project is funded by INRIA for 4 years and started in Jan. 2008. The coordinators are A. Girault (INRIA Rhône Alpes) and M. Pouzet. http://synchronics.inria.fr/

The goal of the project is to propose new languages for the development of embedded systems allowing from a unique source to both simulate the system with its environment and generate code. It capitalizes on recent extensions of data-flow synchronous languages (Lucid Synchrone, ReactiveML), a relaxed form of synchrony, and means to mix discrete and continuous systems inside the synchronous model of time.

The project focuses on language extensions to increase modularity, dedicated type systems to ensure safety properties, efficient compilation and the mix of discrete and continuous time.

Partners: INRIA Rhône Alpes (Gwenaël Delaval, Alain Girault, Bertrand Jeannet), IRISA (Benoit Caillaud), VERIMAG (Erwan Jahier, Pascal Raymond), INRIA Rocquencourt (Albert Cohen, Marc Pouzet, Louis Mandel)

8.1.2. PARTOUT

Participants: Mehdi Dogguy, Louis Mandel [contact], Cédric Pasteur, Marc Pouzet.

This project is funded by ANR (program DEFIS). http://www-sop.inria.fr/mimosa/PARTOUT

It started on January 2009 for 4 years; the coordinator is Frédéric Boussinot from INRIA Indes.

Partners: INRIA Indes, CNAM, LRI.

The goal of the project PARTOUT is, from a programming language point of view, to study the impact on programming of the globalization of parallelism which now covers all the spectrum of informatics, ranging from multicore architectures and distributed systems, up to applications deployed on the Web.

8.1.3. Mediacom Project

Participants: Albert Cohen [contact], Ramakrishna Upadrasta.

Partners: INRIA CompSys, ALF, Arenaire.

Mediacom is one of the projects of the Nano2012 collaboration framework between STMicroelectronics and INRIA, 09/2009–12/2012. Mediacom is a collaboration between the compilation group of STMicroelectronics HED, led by Christian Bertin, and the INRIA CompSys, ARENAIRE, ALF and PARKAS (formerly ALCHEMY) groups. We are working on portable concurrent intermediate languages, inspired by data-flow synchronous languages and polyhedral compilation, and on just-in-time parallelization algorithms.

8.2. European Initiatives

8.2.1. HiPEAC network of excellence

HiPEAC is a network of excellence on High-Performance Embedded Architectures and Compilers. It was first established as an FP6 network in 2004, and renewed as an FP7 4 years later. INRIA is one of the partners of the network. Albert Cohen leads the Compiler Platform cluster (9 research clusters in total). 02/2008–01/2012.
8.2.2. TERAFLUX integrated project

The TERAFLUX project is funded under the FP7 FET pro-active program on teradevice computing, 01/2010-12/2013. Albert Cohen is responsible for WP4. Our work addresses data-flow synchronous parallel programming, polyhedral compilation for data-flow programs, and compiler support for data-driven multi-threaded architectures with hundreds of computing cores. We contribute compilation algorithms and experimental language designs, with prototypes based on LUCID SYNCHrone and direct contributions to GCC through the design of data-flow synchronous extensions of OpenMP. One of our goals is to transfer results of the project to production tools, including GCC and simulation platforms for many-core processors. A standardization effort (supported by INRIA’s D2T) aims for the adoption of the language extensions by the OpenMP Architecture Review Board.

8.2.3. PHARAON specific targeted research project

The PHARAON project is funded on the embedded systems strategic objective, 09/2011–08/2014. Albert Cohen is responsible for WP5. Our work addresses data-flow synchronous programming for multiprocessor systems-on-chip, with an emphasis on an embedded development methodology and tools to optimize energy consumption and facilitate the correct-by-construction refinement of a functional specification. The Heptagon and Streaming OpenMP platforms of the team are used in the project. PHARAON is led by Thales Communications and Security.

8.2.4. CARP specific targeted research project

The CARP project is funded on the computing systems strategic objective, 12/2011–11/2014. Our work addresses polyhedral automatic parallelization for vector accelerators, with an emphasis on extending the scope of polyhedral compilation and integrating vectorization and specialization techniques. isl is an important component of this work, along with a new source-to-source compilation framework being developed in the project. CARP is led by Imperial College, and our team collaborates closely with ARM Cambridge in the specification of a portable parallel intermediate language to facilitate automatic parallelization and vectorization.

8.2.5. Collaborations in European Programs, except FP7

8.2.5.1. Euro-TM COST action

This new action started in April 2011. It aims at consolidating European research on transactional memory, by coordinating the research groups working on the development of complementary, interdisciplinary aspects of Transactional Memories, including theoretical foundations, algorithms, hardware and operating system support, language integration and development tools, and applications. Our participation is focused on the interaction between data-flow and transactional memory models.

8.3. International Initiatives

8.3.1. Visits of International Scientists

8.3.1.1. International guests of the PARKAS seminars

- November 2011: Alex Nicolau, UCI. Variability, Accuracy, and Performance evaluation.
- September 2011: Daisuke Ishii, JSPS, National Institute of Informatics (Tokyo) and ProVal team, INRIA Saclay. An Execution Algorithm for a Hybrid Modeling Language HydLa.
- August 2011: Peter Gammie, the Australian National University and National ICT Australia. Verified Synthesis of Knowledge-Based Programs in Finite Synchronous Environments.
- June 2011: Jan Vitek, Purdue University. Virtualizing Real-time Embedded Systems with Java.

8.3.1.2. Other visits

• John Cavazos, University of Delaware, visited us in January and July 2011. We have been collaborating on statistical methods in polyhedral compilation since John’s postdoc at the University of Edinburgh. A joint paper was published at CGO 2011. Albert Cohen is on the PhD thesis committee of his student, Eunjung Park.

• P. Sadayappan, Ohio State University, visited us in December 2011. We collaborate for a long time on polyhedral compilation methods and tools. A joint paper was published at POPL 2011. P. Sadayappan has been the Master thesis advisor of Tobias Grosser and he is participating to the direction of his PhD thesis, and he hosts a former student, Louis-Noël Pouchet for more than 1 year as a postdoc.

• John Plaice, University of New South Wales, visited us in December 2011. He is a long-time synchronous programming and functional programming expert. His Translucid language experiment could be the basis for a collaboration on efficient compilation of array-based computations and synchronous language expressiveness.

8.3.1.3. Supervision of post-docs, theses and Internships

• Marc Pouzet supervised the 12-month post-doc of Timothy Bourke, from the University of New South Wales, from September 2010 to October 2011, and funded by the large scale initiative SYNCHRONICS of INRIA. Timothy worked on the semantics and implementation of hybrid modelers.

• Albert Cohen co-advised the PhD thesis of Sean Halle, from the University of California Santa Cruz, defended in June 2011. Sean Halle worked on parallel programming models and analytical performance models.
8. National Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR AutoChem: Chemical Programming

Participants: Pascal Fradet [contact person], Marnes Hoff.

The AUTOChem project aims at investigating and exploring the use of chemical languages (see Section 6.7.3) to program complex computing infrastructures such as grids and real-time deeply-embedded systems. The consortium includes INRIA Rennes – Bretagne Atlantique (PARIS team, Rennes), INRIA Grenoble – Rhône-Alpes (POP ART team, Montbonnot), IBISC (CNRS/Université d’Evry) and CEA List (Saclay). The project started at the end of 2007 and ended in November 2011.

8.1.2. ANR Asopt: Analyse Statique et OPTimisation

Participants: Bertrand Jeannet [contact person, coordinator], Lies Lakhdar-Chaouch, Pascal Sotin, Peter Schrammel.

The ASOPT (Analyse Statique et OPTimisation) project [end of 2008-2011] brings together static analysis (INRIA-POP ART, VERIMAG, CEA LMeASI), optimisation, and control/game theory experts (CEA LMeASI, INRIA-MAXPLUS) around some program verification problems. POP ART is the project coordinator.

Many abstract interpretations attempt to find “good” geometric shapes verifying certain constraints; this not only applies to purely numerical abstractions (for numerical program variables), but also to abstractions of data structures (arrays and more complex shapes). This problem can often be addressed by optimisation techniques, opening the possibility of exploiting advanced techniques from mathematical programming.

The purpose of ASOPT is to develop new abstract domains and new resolution techniques for embedded control programs, and in the longer run, for numerical simulation programs.

8.1.3. ANR Vedecy: Verification and Design of Cyber-physical Systems

Participants: Gregor Goessler [contact person], Bertrand Jeannet, Sebti Mouelhi.

The VEDECY project brings together hybrid systems and formal methods experts. Three partners are involved: Laboratoire Jean Kuntzmann (LJK), INRIA POP ART, and VERIMAG.

VEDECY aims at pursuing fundamental research towards the development of algorithmic approaches to the verification and design of cyber-physical systems. Cyber-physical systems result from the integration of computations with physical processes: embedded computers control physical processes which in return affect computations through feedback loops. They are ubiquitous in current technology and their impact on lives of citizens is meant to grow in the future (autonomous vehicles, robotic surgery, energy efficient buildings, ...).

Cyber-physical systems applications are often safety critical and therefore reliability is a major requirement. To provide assurance of reliability, model based approaches and formal methods are appealing. Models of cyber-physical systems are heterogeneous by nature: discrete dynamic systems for computations and continuous differential equations for physical processes. The theory of hybrid systems offers a sound modeling framework for cyber-physical systems. The purpose of VEDECY is to develop hybrid systems techniques for the verification and the design of cyber-physical systems.

8.1.4. INRIA Large Scale Action Synchronics: Language Platform for Embedded System Design

Participants: Gwenaël Delaval, Alain Girault [contact person, co-coordinator], Bertrand Jeannet, Xavier Nicollin, Peter Schrammel.

SYNCHRONICS capitalizes on recent extensions of data-flow synchronous languages, as well as relaxed forms of synchronous composition or compilation techniques for various platform, to address two main challenges with a language-centered approach: (i) the co-simulation of mixed discrete-continuous specifications, and more generally the co-simulation of programs and properties (either discrete or continuous); (ii) the ability, inside the programming model, to account for the architecture constraints (execution time, memory footprint, energy, power, reliability, etc.).

8.1.5. Collaborations inside INRIA

- VERTECS at INRIA Rennes – Bretagne Atlantique is working with us on applications of discrete controller synthesis, and in particular on the tool SIGALI.
- P. Fradet cooperates with R. Douence (ASCOLA, École des Mines de Nantes) on aspect-oriented programming.
- G. Goessler cooperates with D. Le Métayer (LICT, INRIA Grenoble – Rhône-Alpes) on logical causality and with G. Salaün (VASY, INRIA Grenoble – Rhône-Alpes) on realizability of choreographies with asynchronous communication.
- B. Jeannet cooperates with A. Miné and X. Rival (ABSTRACTION, INRIA Paris – Rocquencourt) and X. Allamigeon (MAXPLUS, INRIA Saclay – Île-de-France) on static analysis and abstract interpretation.
- G. Delaval cooperates with H. Marchand (VERTECS, INRIA Rennes – Bretagne Atlantique) and É. Rutten (SARDES, INRIA Grenoble – Rhône-Alpes) on modular controller synthesis and its applications.
- G. Delaval, A. Girault and B. Jeannet collaborate with the PARKAS team of ENS Ulm (INRIA Paris – Rocquencourt) on the distribution of higher-order synchronous data-flow programs and on static analysis of hybrid programs.

8.1.6. Cooperations with other laboratories

- P. Fradet cooperates with J.-L. Giavitto (CNRS/Ircam) on refinement of chemical programs.
- A. Girault collaborates with P. Roop, Z. Salcic, and S. Andalam (University of Auckland, New Zealand) and A. Malik (IBM Watson, USA) in the context of the AFMES associated team, with H. Kalla (University of Batna, Algeria) and I. Assayad (University of Casablanca, Morocco) on multicriteria scheduling.
- G. Goessler collaborates with A. Girard (LJK, Grenoble) on multi-scale controller synthesis, with J. Sifakis (EPFL) on distribution under real-time constraints, with J.-B. Raclet (IRIT, Toulouse) on modal contracts, with I. Lee and O. Sokolsky (U. of Pennsylvania) on causality analysis for medical devices, and with M. Bozga (VERIMAG) and B. Bonakdarpour (U. of Waterloo, Canada) on fault tolerance in component-based systems.
- A. Girault and G. Goessler collaborate with P. Roop (University of Auckland, New Zealand) on incremental converter synthesis.
• B. Jeannet collaborates with N. Halbwachs and M. Péron (VERIMAG), E. Goubault and S. Putot (CEA Saclay) on static analysis and abstract interpretation.
• G. Delaval and A. Girault collaborate with X. Nicollin (VERIMAG) on the automatic distribution of synchronous programs.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, except FP7

Program: ARTEMISIA.
Project acronym: CESAR32.
Project title: Cost-efficient methods and processes for safety relevant embedded systems.
Duration: January 2009 – April 2012.
Partners: There are 59 partners from academia and industry (both SMEs and large companies).
Abstract: We are particularly involved in the following sub-programs:

SP1: Task Force Safety 1.5.1 (State of the art survey on safety and diagnosability for cost-efficient safety critical embedded systems) and 1.5.2 (Identification of requirements for common cross domain core safety and diagnosability techniques and methods).
SP2: Requirements Engineering, along with two other INRIA teams (S4 and TRISKELL, from INRIA Rennes). We shall work on contracts based design for traceability.

8.3. International Initiatives

8.3.1. INRIA Associate Teams

8.3.1.1. AFMES

Title: Advanced Formal Methods for Embedded Systems.
INRIA principal investigator: Alain Girault.
International Partner:

Institution: University of Auckland (New Zealand).
Laboratory: Department of Electrical and Computer Engineering.
Principal investigator: Zoran Salcic.
Duration: January 2010 – December 2012.
See also: \texttt{http://pop-art.inrialpes.fr/~girault/Projets/Afmes/}
Embedded systems are characterized by several constraints, such as determinism and bounded reaction time. Accordingly, design methods for embedded systems should, when possible, guarantee these properties by construction. This allows the shifting of the burden of checking these constraints from the programmer to the design method and the associated compilers and code generation tools. In order to achieve this, our goal is to improve the existing design methods in several key directions: (1) Incremental converter synthesis. (2) Programming language for adaptive computing (SystemJ and beyond). (3) Time predictable programming language and execution architectures. Together, these advanced methods will provide a higher level of safety in the design of embedded systems.

8.3.2. Visits of International Scientists

• Hamoudi Kalla, assistant professor at University of Batna, Algeria, September 2011.
• Ismail Assayad, assistant professor at University of Casablanca, Morocco, September 2011.

8.3.2.1. Internship

• Emmanouil Komninos, 02-07/2011, co-advised by Pascal Fradet and Alain Girault, Power consumption optimization of data-flow applications on many-core systems, MSc at KTH, Sweden.

\textsuperscript{32} \texttt{http://www.cesarproject.eu}
7. Partnerships and Cooperations

7.1. Disc: Distributed Supervisory Control of Large Plants

**Participant:** Philippe Daronneau.

*ICT STREP 224498 Disc (September 2008 to December 2011), [http://www.disc-project.eu](http://www.disc-project.eu)*

Started on 1 September 2008, Disc is a project supported by the ICT program of the European Union.

The aim of the project is to enable the supervisory control of networked embedded systems. These distributed plants are composed by several local agents that take concurrently decisions, based on information that may be local or received from neighbouring agents; they require scalable and self-organising platforms for advanced computing and control. The evolution is guided by the occurrence of asynchronous events, as opposed to other real-time models where the event occurrence is time-triggered.

The partners of the project come from academia (University of Cagliari, CWI - Amsterdam, Ghent University, Technical University of Berlin, University of Zaragoza, INRIA, Czech Academy of Sciences), from industry (Akhela s.r.l., Italy and CyBio AG, Germany), and from a governmental instance (Ministry of the Flemish Government, Belgium).

Philippe Daronneau has worked in this context with Eric Badouel, Anne Bouillard and Jan Komenda (Czech Academy of Sciences, Brno) on the synthesis of robust delay-controllers for timed systems modelled with rational power series. He works also towards applying the synthesis of distributable Petri nets to asynchronous and distributed supervisory control.

7.2. Synchronics: Language Platform for Embedded System Design

**Participants:** Albert Benveniste, Timothy Bourke, Benoît Caillaud.

*Large initiative action funded by INRIA. [http://synchronics.inria.fr/](http://synchronics.inria.fr/)*

This project, started Jan 1st 2008, is supported by INRIA. It capitalizes on recent extensions of data-flow synchronous languages (mode automata, Lucid Synchrone, Signal, Lustre, ReactiveML, relaxed forms of synchronous composition or compilation techniques for various platforms). We aim to address the main challenges of embedded system design, starting from a single, semantically well founded programming language.

Our contribution in 2011 is detailed in Section 6.2. A detailed account of the work carried out in Synchronics can be found in the slides presented during the mid-term evaluation seminar of the action: [http://synchronics.inria.fr/doku.php/mid-term-review](http://synchronics.inria.fr/doku.php/mid-term-review)
TRIO Project-Team (section vide)
8. Partnerships and Cooperations

8.1. National Collaborations

Additionally, we collaborated in 2011 with the following INRIA project teams:

- **OASIS** (Sophia-Antipolis): distributed verification tools (Eric Madelaine);
- **POP-ART** (Rhône-Alpes): behavioral adaptation of software services and conformance checking of choreography specifications (Gregor Gössler);
- **SARDES** (Rhône-Alpes): verification of protocols for component-based architectures and virtualization (Fabienne Boyer, Olivier Gruber, and Noël de Palma).

Beyond INRIA, we had sustained scientific relations with the following researchers:

- Gaëlle Calvary and Sophie Dupuy (LIG, Grenoble);
- Pascal Poizat (LRI, Orsay);
- Meriem Ouederni (LINA, Nantes);
- Xavier Blanc and Cédric Teyton (LABRI, Bordeaux).

8.2. European Collaborations

The VASY project team is member of the FMICS (*Formal Methods for Industrial Critical Systems*) working group of ERCIM (see [http://fmics.inria.fr](http://fmics.inria.fr)). From July 1999 to July 2001, H. Garavel chaired this working group; since July 2002, he has been a member of the FMICS Board, and is in charge of dissemination actions. In November 2011, R. Mateescu was elected chairman of the FMICS working group.

In addition to our partners in aforementioned contractual collaborations, we had scientific relations in 2011 with several European universities and research centers, including:

- Polytechnic University of Bucharest (Valentin Cristea);
- Saarland University (Jonathan Bogdoll, Pepijn Crouzen, Arnd Hartmanns, and Holger Hermanns);
- University of Coimbra (Javier Camara);
- University of Málaga (Carlos Canal, Meriem Ouederni, and Ernesto Pimentel).

D. Thivolle defended his PhD thesis at the Polytechnic University of Bucharest on April 29, 2011.

Our long-term partnership with Saarland University has been strengthened by the Humboldt Forschungspreis received by H. Garavel, who started regular visits to Saarland University.

H. Garavel has participated in the review of the DFG (*Deutsche Forschungsgemeinschaft*) transregional project AVACS (*Automatic Verification And Analysis of Complex Systems*, see [http://www.avacs.org](http://www.avacs.org)) on September 14–15, 2011.

8.3. International Collaborations

H. Garavel is a member of IFIP (*International Federation for Information Processing*) Technical Committee 1 (*Foundations of Computer Science*) Working Group 1.8 on Concurrency Theory chaired successively by Luca Aceto and Jos Baeten.
8.4. Visits and Exchanges

In 2011, we had the following scientific exchanges:

- Nicolas Halbwachs (VERIMAG) visited us on January 28, 2011 and gave a talk entitled “Analyse de programmes: propriétés numériques et tableaux”.
- Thomas Lambolais and Thanh-Liem Phan (Ecole des Mines d’Alès) visited us on February 9, 2011.
- Meriem Ouederni (University of Málaga, Spain) visited us from June 27 to July 1, 2011 and from November 21 to November 25, 2011.
- Freark van der Berg (University of Twente, The Netherlands) visited us on October 17–21, 2011.
- Farhad Arbab (CWI, Amsterdam, The Netherlands) visited us on November 22, 2011 and gave a talk entitled “Interaction-Based Concurrency”.
- Gianluigi Zavattaro (University of Bologna, Italy) visited us on November 22, 2011 and gave a talk entitled “Parameterized Verification of Ad Hoc Network Protocols”.
- The annual VASY seminar was held in Autrans (France) on November 28–30, 2011.
- Xavier Blanc (LaBRI, Bordeaux) attended the VASY annual seminar and gave on November 28, 2011 a talk entitled “Vpraxis et évolution d’applications Internet”.
- Christian Attiogbe (LINA, Nantes) attended the VASY annual seminar and gave on November 29, 2011 a talk entitled “Composition dynamique de processus dans les systèmes complexes”.
- Grégory Batt (INRIA Rocquencourt) attended the VASY annual seminar and gave on November 30, 2011 a talk entitled “A general computational method for robustness analysis with applications to synthetic gene networks”.
- Holger Hermanns (Saarland University) visited us on December 1st, 2011 and gave a LiG keynote entitled “From Concurrency Models to Numbers: Performance, Dependability, Energy”.
7. Partnerships and Cooperations

7.1. National initiatives

7.1.1. ANR TesTec: Test of real-time and critical embedded system

Participants: Nathalie Bertrand, Thierry Jéron, Hervé Marchand.

The TesTec project is a three years [2008-2010] industrial research project that gathers two companies: an end-user (EDF R&D ) and one software editor for embedded real-time systems and automation systems (Geensys), and four laboratories from automation engineering and computer science (I3S, INRIA Rennes, LaBRI, LURPA). This project focuses on automatic generation and execution of tests for the class of embedded real-time systems. They are highly critical. Such systems can be found in many industrial domains, such as energy, transport systems. More precisely the project TesTec will address two crucial technological issues:

- optimisation of test generation techniques for large size systems, in particular by an explicit modelling of time and by simultaneous management of continuous and discrete variables in hybrid applications;
- reduction of the size of the tests derived from specification models by using the results of formal verification of implementation models.

The overall aim of this project is to propose a software tool for generation and execution of tests; this tool will be based on an existing environment for embedded systems design and will implement the scientific results of the project.

This year our contributions to this project were our works on test generation from timed models, as well as approximate determinization of timed automata.

In 2011, the post-doc position of Puneet Bhateja was funded by TestTec.

7.1.2. ANR VACSIM: Validation of critical control-command systems by coupling simulation and formal analysis

Participants: Nathalie Bertrand, Thierry Jéron, Hervé Marchand.

The Vacsim project (2011-2014) is a 3 years project with EDF R&D, Dassault Systèmes, LURPA Cachan, I3S Nice and Labri Bordeaux. The project aims at developing both methodological and formal contributions for the simulation and validation of control-command systems. The role of the Vertecs team will be to contribute to the advance of validation techniques for timed systems, including quantitative analysis and its application to testing, monitoring of timed systems, and verification of communicating timed automata.

7.1.3. Action Incitative VeSPa: Verification of security and privacy properties

Participant: Nathalie Bertrand.

The VeSpa "Action Incitative" is a one-year [2011] project funded by Rennes 1 University to develop emerging research themes. The goal of the project is to strat and verify security and privacy properties in protocols, using logic and games techniques. The participants are Sophie Pinchinat (leader, S4), Sébastien Gambs (Cidre), Guillaume Aucher (DistribCom), and Nathalie Bertrand (Vertecs). To gather researchers interested in the topic, the second edition of a workshop on Games, Logics and Security has been organized in October 2011.
7.2. European initiatives

7.2.1. Artist design network of excellence

**Participants:** Nathalie Bertrand, Thierry Jéron, Hervé Marchand.

Program: FP7  
Project acronym: Artist Design  
Project title: Artist - European Network of Excellence on Embedded System Design  
Duration: 01/08 - 12/11  
Coordinator: VERIMAG

Abstract: The central objective for ArtistDesign [http://www.artist-embedded.org/artist/ArtistDesign-Participants-.html](http://www.artist-embedded.org/artist/ArtistDesign-Participants-.html) is to build on existing structures and links forged in Artist2, to become a virtual Center of Excellence in Embedded Systems Design. This will be mainly achieved through tight integration between the central players of the European research community. Also, the consortium is smaller, and integrates several new partners. These teams have already established a long-term vision for embedded systems in Europe, which advances the emergence of Embedded Systems as a mature discipline.

The research effort aims at integrating topics, teams, and competencies, grouped into 4 Thematic Clusters: “Modelling and Validation”, “Software Synthesis, Code Generation, and Timing Analysis”, “Operating Systems and Networks”, “Platforms and MPSoC”. “Transversal Integration” covering both industrial applications and design issues aims for integration between clusters.

The Vertecs EPI is a partner of the “Validation” activity of the “Modeling and Validation” cluster. This year, the Vertecs EPI has contributed to quantitative verification of timed automata [15], approximate determinization of timed automata [18] and its adaptation to test generation [17], and control synthesis using abstract interpretation for infinite state systems [11], on decentralized [10] and distributed control [21], [22]. Amélie Stainer spent one month in Aalborg to implement the approximate determinization of timed automata using UPPAAL libraries.

7.2.2. PHC Tournesol STP : Verification of timed and probabilistic systems

**Participants:** Nathalie Bertrand, Amélie Stainer.

A two-year contract with the group of Thomas Brihaye (Université Mons) started in 2010. Its objective is to study timed and probabilistic systems. This year, Nathalie Bertrand visited Thomas Brihaye in Mons, and Thomas Brihaye came to Rennes to give a seminar and further discuss with Nathalie Bertrand and Amélie Stainer.

7.2.3. Followed collaborations with major European organizations

Université Libre Bruxelles (Belgium), Prof. Thierry Massart  
Testing and control of symbolic transitions systems

University of Kaiserslautern (Germany), Roland Meyer  
Petri nets

University of Dresden (Germany), Prof. Christel Baier  
Probabilistic automata over infinite words

7.3. International Initiatives

7.3.1. INRIA associate team

7.3.1.1. TREATIES
Title: Test of Real-Time Embedded Systems
INRIA principal investigator: Thierry Jéron

International Partner:
  Institution: Federal University of Campina Grande (Brazil)
  Laboratory: Universidade Federal do Campina Grande

Duration: 2009 - 2011
See also: http://www.irisa.fr/vertecs/Treaties.html

This associated team with the Federal University of Campina Grande (Prof. Patrícia D. L. Machado) and University Pernambuco (Prof. Augusto Sampaio) in Brazil started in 2009 and ended this year.

In 2011 Nathalie Bertrand and Sébastien Chédor visited the Brazilian team in Recife in November where a meeting took place, and we had the visit of Wilkerson Andrade in November.

This year the cooperation addressed problems in test generation for timed input/output symbolic transition systems (see 6.2.5 ) and compositional conformance verification for these models, on the problems of non-determinism in timed models for test generation (see 6.1.2.1 and 6.2.1 ), on test vector generation for timed models, and automatic test case generation and execution for regular graphs (see 6.2.2 ).

7.3.2. INRIA international partners

University of Michigan (Prof. Stéphane Lafortune) on control and diagnosis of discrete event systems.

7.3.3. Visits of international scientists

Laurie Ricker, associate professor at the Mathematics & Computer Science department of Mount Allison University (Canada) has visited Vertecs for 6 months, from January 2011 to June 2011. We collaborate on control of discrete event systems for distributed systems.
8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR projects

8.1.1.1. AbstractCell
Title: Formal abstraction of quantitative semantics for protein-protein interaction cellular network models
Instrument: ANR-Chair of Excellence (Junior, long term)
Duration: December 2009 - December 2013
Coordinator: INRIA (France)
Others partners: None
See also: http://www.di.ens.fr/feret/abstractcell
Abstract: The overall goal of this project is to investigate formal foundations and computational aspects of both the stochastic and differential approximate semantics for rule-based models. We want to relate these semantics formally, then we want to design sound approximations for each of these semantics (by abstract interpretation) and investigate scalable algorithms to compute the properties of both the stochastic and the differential semantics. Jérôme Feret is the principal investigator for this project.

8.1.1.2. AstréeA
Title: Static Analysis of Embedded Asynchronous Real-Time Software
Type: ANR Ingénierie Numérique Sécurité 2011
Instrument: ANR grant
Duration: January 2012 - December 2015
Coordinator: Airbus France (France)
Others partners: École normale supérieure (France)
See also: http://www.astreea.ens.fr
Abstract: The focus of the AstréeA project is on the development of static analysis by abstract interpretation to check the safety of large-scale asynchronous embedded software. During the Thésée ANR project (2006–2010), we developed a concrete and abstract models of the ARINC 653 operating system and its scheduler, and a first analyzer prototype. The gist of the AstréeA project is the continuation of this effort, following the recipe that made the success of Astrée: an incremental refinement of the analyzer until reaching the zero false alarm goal. The refinement concerns: the abstraction of process interactions (relational and history-sensitive abstractions), the scheduler model (supporting more synchronisation primitives and taking priorities into account), the memory model (supporting volatile variables), and the abstraction of dynamical data-structures (linked lists). Patrick Cousot is the principal investigator for this project.

8.1.1.3. Verasco
Title: Formally-verified static analyzers and compilers
Type: ANR Ingénierie Numérique Sécurité 2011
Instrument: ANR grant
Duration: Septembre 2011 - September 2015
Coordinator: INRIA (France)
Others partners: Airbus France (France), IRISA (France), INRIA Saclay (France)
See also: http://www.systematic-paris-region.org/fr/projets/verasco

Abstract: The usefulness of verification tools in the development and certification of critical software is limited by the amount of trust one can have in their results. A first potential issue is unsoundness of a verification tool: if a verification tool fails (by mistake or by design) to account for all possible executions of the program under verification, it can conclude that the program is correct while it actually misbehaves when executed. A second, more insidious, issue is miscompilation: verification tools generally operate at the level of source code or executable model; a bug in the compilers and code generators that produce the executable code that actually runs can lead to a wrong executable being generated from a correct program.

The project VERASCO advocates a mathematically-grounded solution to the issues of formal verifying compilers and verification tools. been mechanically proved to be free of any miscompilation will be continued. Finally, the tool qualification issues that must be addressed before formally-verified tools can be used in the aircraft industry, will be investigated.

8.2. European Initiatives

8.2.1. EU Project

8.2.1.1. MBAT

Title: Combined Model-based Analysis & Testing of Embedded Systems
Type: Artemis Call 10
Instrument: FP7 project
Duration: November 2011 - October 2014
Coordinator: Daimler (Germany)
Others partners: 38 partners in Austria, Denmark, Estonia, France, Germany, Italy, Sweden, and United Kingdom
See also: http://www.artemis-ia.eu/project/index/view/?project=29

Abstract: MBAT will mainly focus on providing a technology platform for effective and cost-reducing validation and verification of embedded systems, focusing primarily on transportation domain, but also to be used in further domains. The project involves thirty three European industrial (large companies and SMEs) and five academic partners. Radhia Cousot is the principal investigator for this project.

8.2.1.2. MemCad

Title: Memory Compositional Abstract Domains
Type: IDEAS
Instrument: ERC Starting Grant (Starting)
Duration: October 2011 - September 2016
Coordinator: INRIA (France)
Others partners: none
See also: http://www.di.ens.fr/rival/memcad.html
Abstract: The MemCAD project aims at setting up a library of abstract domains in order to express and infer complex memory properties. It is based on the abstract interpretation frameworks, which allows to combine simple abstract domains into complex, composite abstract domains and static analyzers. While other families of abstract domains (such as numeric abstract domains) can be easily combined (making the design of very powerful static analyses for numeric intensive applications possible), current tools for the analysis of programs manipulating complex abstract domains usually rely on a monolithic design, which makes their design harder, and limits their efficiency. The purpose of the MemCAD project is to overcome this limitation. Our proposal is based on the observation that the complex memory properties that need be reasoned about should be decomposed in combinations of simpler properties. Therefore, in static analysis, a complex memory abstract domain could be designed by combining many simpler domains, specific to common memory usage patterns. The benefit of this approach is twofold: first it would make it possible to simplify drastically the design of complex abstract domains required to reason about complex softwares, hereby allowing certification of complex memory intensive softwares by automatic static analysis; second, it would enable to split down and better control the cost of the analyses, thus significantly helping scalability. As part of this project, we propose to build a static analysis framework for reasoning about memory properties, and put it to work on important classes of applications, including large softwares.

8.3. International Initiatives

8.3.1. NSFC Project

8.3.1.1. NSFC

Title: Analysis and Verification of Dependable Cyber-Physical Software
Type: National Natural Science Foundation of China (NSFC)
Duration: January 2012 - December 2016
Coordinator: National University of Defense Technology (China)
Others partners: National University of Defense Technology (China), Seoul National University (Korea)
Abstract: The project addresses analysis and verification issues related to dependability properties of Cyber Physical Systems (CPS) software: safety (such as the numerical or and memory related runtime errors), quantitative properties (such as the worst-case execution time, upper bound of the memory consumption, etc.), stability and robustness (due to intrinsic uncertainty of CPS), as well as properties of hybrid system (which provides a model for describing the coordination of computation and physical, discrete and continuous processes). The project is expected to advance the analysis and verification methodology for dependable CPS software so as to contribute to the dependability assurance of CPS software in mission critical applications. Patrick Cousot is the principal investigator for this project.

8.3.1.2. Visiting professors

Yanjun Wen is associate professor at the Department of Computer Science and Technology, College of Computer, National University of Defense Technology, Changsha, P. R. China. He is visiting the team from June 2011 to May 2012 and is interested in the static analysis of parallel software by abstract interpretation.
Roberto Giacobazzi, professor at the University of Verona, Italy, visited in spring 2011.
Andreas Podelski, professor at the University of Freiburg, Germany, visited in fall 2011.

8.3.1.3. Internship

Marie Pelleau is a third year PhD student from the University of Nantes (France) under the supervision of Frédéric Benhamou, Pascal Van Hentenryck, and Charlotte Truchet. She spent one month (November 2011) in the team, under the supervision of Antoine Miné, on the application of numerical abstract domains (and in particular, the Apron library, 5.1) to constraint programming.
David Delmas is an engineer at Airbus France on educational leave to pursue the 2nd year of the Parisian Master of Research in Computer Science (MPRI) and a visitor in the team from September 2011 to August 2012.

Suzanne Renard is a third year student at École des Mines de Paris (France). She spent six months (September 2010 to February 2011) in the team, under the supervision of Xavier Rival; she was working on the extension of the XISA shape analysis frameworks in order to express set properties.
ATEAMS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

+ NWO TOP proposal “Domain-Specific Languages: A Big Future for Small Programs”
+ “Next Generation Auditing: Data Assurance as a Service” (Jacquard project)
+ “Escher: End-user SCripting for High-level software RepresenTation” (NWO)
+ “GrammarLab: Foundations For a Grammar Laboratory” (NWO)
+ “Model Driven Engineering in Digital Forensics” (NWO)
+ “EQuA: Early Quality Assurance in Software Production”

8.2. International Initiatives

8.2.1. Visits of International Scientists

- Prof. Dr. Michael Godfrey (University of Waterloo, Canada) is visiting for one year, starting August 2011.
- Dr. Anya Helene Bagge (Institutt for Informatikk Universitetet i Bergen, Norway) was visiting us for one year until October 2011.
- Prof. Dr. William Cook visited us for a week (University of Texas, U.S.A.)
- Prof. Dr. Eric van Wyk visited us for one week (University of Minnesota, U.S.A.)
- Prof. Dr. Terence Parr visited us for two days (University of San Francisco, U.S.A.)
- Dr. Markus Völter visited us for two days (Germany)
- Dr. Wolfgang Lohmann visited us for a day (EMPA, Switzerland)
- Prof. Dr. Ralf Lämmel visited us for a week (Universität Koblenz-Landau, Germany)
- Dr. Vlad Rusu visited us several times for two days (INRIA Lille, France)

8.2.1.1. Internships

- Wietse Venema 2011/2012
- Randy Fluit 2011
- Ahmadi Nasab 2010/2011
- Jouke Stoel 2011
- Christian Köppe 2011
- Davy Landman 2011
- Jan de Mooij 2011
8. Partnerships and Cooperations

8.1. National Initiatives

- ANR Complice
- Project CyS of GIS 3SGS on smartphone forensics.

We have active collaborations with:

- Alexander Shen (LIF),
- Laurent Bienvenu (LIAFA),
- Florian Deloup came in our group for six months as a CNRS researcher.

8.2. European Initiatives

8.2.1. FP7 Projekt

8.2.1.1. FI-WARE

Title: Morphus
Type: COOPERATION (ICT)
Def: PPP FI: Technology Foundation: Future Internet Core Platform
Instrument: Integrated Project (IP)
Duration: May 2011 - April 2014
Coordinator: Telefonica (Spain)
Others partners: Thales, SAP, INRIA
See also: http://www.fi-ware.eu/

Abstract: FI-WARE will deliver a novel service infrastructure, building upon elements (called Generic Enablers) which offer reusable and commonly shared functions making it easier to develop Future Internet Applications in multiple sectors. This infrastructure will bring significant and quantifiable improvements in the performance, reliability and production costs linked to Internet Applications ? building a true foundation for the Future Internet.

8.2.2. Major European Organizations with which Carte has followed Collaborations

- Stefano Galatolo (Università di Pisa),
- Daniel Graça (University of Faro),
- Georg Moser (University of Innsbruck),
- Klaus Weihrauch (FernUniversität Hagen).

8.3. International Initiatives

- ARC CaCO3 (France-Egypt), http://carte.loria.fr/index.php?option=com_content&view=article&id=63&Itemid=77

8.3.1. INRIA Associate Teams

8.3.1.1. COMPUTR
Title: COntinuous tiMe comPUTations, computation on the Reals  
INRIA principal investigator: Emmanuel Hainry  
International Partner:  
  Institution: Instituto de Telecomunicações (Portugal)  
  Laboratory: Security and Quantum Information Group  
Duration: 2009 - 2011  
See also: http://carte.loria.fr/index.php?option=com_content&view=article&id=60&Itemid=74

8.3.1.2. CRISTAL  
Title: Resource Control by Semantic Interpretations and Linear Proof Theory  
INRIA principal investigator: Romain Péchoux  
International Partner:  
  Institution: Universita degli Studi di Torino (Italy)  
  Laboratory: Dipartimento di informatica  
Duration: 2010 - 2012  
See also: http://carte.loria.fr/index.php?option=com_content&view=article&id=61&Itemid=75

8.3.2. INRIA International Partners  
We have active collaboration with:  
  • Peter Gács (Boston University),  
  • Cristóbal Rojas (Toronto),  
  • José Fernandez (Montreal),  
We also start some collaborations with Dawn Song at Berkeley.

8.3.3. Visits of International Scientists  
8.3.3.1. Internship  
  • Daniel Leivant (Indiana University, invited for six months)  
  • John Case (University of Delaware), http://www.cis.udel.edu/~case/  
  • Walid Gomaa (University of Cairo), http://www.alexeng.edu.eg/~wgomaa/
8. Partnerships and Cooperations

8.1. International Grants

- French-Tunisian project on *Security Policies and Configurations of Firewalls: Compilation and Automated Verification*. We collaborate with SupCom Tunis and the INRIA project-team Dahu in the context of STIC-Tunisia.

8.2. National Grants

- **ANR SESUR AVOTÉ—Formal Analysis of Electronic-Voting protocols**, duration: 4 years, started in January 2008. Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. However, the convenience of electronic elections comes with a risk of large-scale fraud. The AVOTÉ project aims at proposing techniques for formally analyzing e-voting protocols. Cassis is the coordinator of the project. Partners are: France Telecom Lannion, LSV Cachan, Verimag Grenoble.

- **ANR DECERT — Deduction and Certification**, coordinated by Thomas Jensen (IRISA). This project focuses on the design of decision procedures, in particular for fragments of arithmetic, and their integration into larger verification systems, including skeptical proof assistants. Partners are: IRISA Rennes, LRI Orsay, INRIA Sophia, Systerel and CEA. From INRIA Nancy, the teams Veridis and Cassis are involved. This project started in January 2009 for three years.

- **ANR TASCCC Test Automatique basé sur des Scénarios et Critères Communs – Automated Testing based on Scenarios and Common Criteria**, duration: 3 years, starting in December 2009. The project aims at completing the model-based testing process initiated in the POSE project, using scenarios to specify the test cases that have to be generated by model animation. The goal is here to provide an automated means for generating the scenarios from a given set of properties. The overall objective is to ease the Common Criteria evaluation of secure softwares. Partners: Trusted Labs (leader), Gemalto, LIG, LIFC, Supelec, Smartesting, and Serma Technologies. The local coordinator is Frédéric Dadeau.

- **ANR PROSE Protocoles de sécurité : modèle formel, modèle calculatoire, and implémentations — Security protocols : formal model, computational model, and implementations**, duration: 4 years, started in December 2010. 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: (i) the symbolic level, in which messages are terms, (ii) the computational level, in which messages are bitstrings, and (iii) the implementation level: the program itself. Partners are Cascade Paris (leader), LSV Cachan, Cassis and Verimag Grenoble.

- **ANR STREAMS Solution for Peer-to-peer Real-Time Social Web**, duration: 3 years, starting in October 2010. This project proposes to design peer-to-peer solutions that offer underlying services required by real-time social web applications and that eliminate the disadvantages of centralised architectures. There exists a tension between sharing data with friends in a social network deployed in an open peer-to-peer network and ensuring privacy. One of the most challenging issues in social applications is how to balance collaboration with access control to shared objects. This project aims at providing theoretical solutions to these challenges as well as practical experimentations. Partners are: LORIA Score team (leader), INRIA project-teams Regal, Asap, Cassis, and XWiki.
• ANR FREC Frontiers of recognizability, duration: 4 years, starting in October 2010. The goal of this project is to be a driving force behind the extension of the algebraic theory of regular languages made possible by recent advances. Four directions will be investigated: tree languages, λ-terms, automata with counters, algebraic and topological tools. Partners are LABRI (leader), LIAFA (University Paris 7). Pierre-Cyrille Héam is a member of this project, attached to Paris 7 for administrative facilities.

• FUI SQUASH Software QUality ASSurance enHancement, duration: 2 years, starting in April 2011. This project aims to industrialize and to structure software testing activities. The project can be provide methodology and tools framework based on open source components.

• ANR OSEP Online and offline model-based testing of SEcurity Properties, duration: 2 years, starting in December 2011. The goal of this project is to test the security with online and offline model-based testing approach. The main element of project is to capitalize or to reuse a test model with different testing method. So, we develop new algorithms to allow online testing. This approach must be compatible with our previous offline approach to increase the number of artefacts that can be shared. This approach can be applied to the components of security and the Software Radio. Partners are DGA and Smartesting.

• Collaborative Research Initiative INRIA, ARC ACCESS. This project is concerned with the security and access control for Web data exchange, in the context of Web applications and Web services. We aim at defining automatic verification methods for checking properties of access control policies (ACP) for XML, like consistency or secrecy. Partners are: INRIA project-teams Dahu, Mostrare and Cassis.

8.3. International Collaborations

• In the area of automated test generation from a formal model, we have an active collaboration with Dr Mark Utting from the Formal Method group from the University of Waikato. This cooperation is supported by the France-New-Zealand scientific program.

• In the area of business applications, we have been working on the may-/must semantics of coloured work-flow Petri nets with the Information System group of Professor W. van der Aalst from the Technical University of Eindhoven, The Netherlands.

• In the area of security protocols penetration testing, we have started a collaboration with Karlsruhe Institute of Technology (Germany) led by Prof. Alexander Pretschner. This collaboration is mainly supported by KIT, in the context of the FP7 SPACIOS project.

8.4. Individual Involvement


V. Cortier: Principal Investigator of the ERC Starting Grant ProSecure (2011-2016); coordinator of the ANR SESUR AVOTÉ (started in Jan. 2008); PC member of ESORICS 2011 (16th European Symposium on Research in Computer Security), MFPS 2011 (27th Conference on the Mathematical Foundations of Programming Semantics), FC 2011 (15th International Conference on Financial Cryptography and Data Security), RTA 2011 (22nd International Conference on Rewriting Techniques and Applications); member of selection committees: INRIA Bordeaux (CR position), Caen University (Full Professor); member of the Evaluation Committee of the INRIA since Sept. 2008.

8.5. Visits of Foreign Researchers

Adel Bouhoula (SupCom Tunis, Tunisie) has visited Cassis (July 14 - July 21) to work on firewall policies.

Chris Lynch (University of Clarkson, USA) has visited Cassis (August 8 - August 15) to work on automated deduction.

Paliath Narendran (University of Albany, USA) has visited Cassis (August 19 - August 25) to work on unification algorithms for security protocol analysis.

Olivier Pereira (Université Catholique de Louvain, Belgium) has visited Cassis to work on developments of Helios (November 28).

Valerio Senni (University of Roma “Tor Vergata”, Italy) has visited Cassis (30th September - 3rd October) for a seminar and to work on structured data generation for testing.

Bogdan Warinschi (University of Bristol, UK) has visited Cassis three times to work on privacy for voting protocols and combination techniques for soundness results of symbolic model (January 17-19, June 20 - 24, and November 20 - 30).
8.6. Visits of Team Members

*Olga Kouchnarenko* has visited Natalia Sidorova (Eindhoven Univ. of Technologies, Netherlands) to work on the may-/exit-semantics of workflow Petri nets and on their configurations to ensure weak termination (November 6 - 13).

*F. Dadeau and P.-C. Héam* have visited Alexander Pretschner (Karlsruhe Institute of Technology) to work on testing security protocols (August 25-26).
7. Partnerships and Cooperations

7.1. International Initiatives

7.1.1. INRIA International Partners

Since three years, we have developed a long-term collaboration with Yahia Lebbah, from University of Oran, Algeria. This collaboration has been fruitful with several publications, the last one being [19] and the INRIA International programme support DGRI. This fund permitted us to visit each other’s group in 2011 with the 1-month visit of N. Lazaar to the University of Oran and the 1-week visit of Y. Lebbah to INRIA Rennes in Dec. 2011.
7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR project PANDA: “Analyse du Parallélisme et de la Distribution”

This project is financed by the ANR, for the years 2009-2011. The partners involved are:

- EPIs Comète and Parsifal at INRIA Saclay. Responsible: Catuscia Palamidessi
- CEA Saclay. Responsible: Emmanuel Haucourt
- Pôle Parisien. Responsible: Damiano Mazza
- Pôle Méditerranéen. Responsible: Emmanuel Godard
- Airbus. Responsible: Jean Souyris.

7.1.2. ANR project CPP: Confidence, Proofs and Probabilities

This project is financed by the ANR, for the years 2009-2011. The partners involved are:

- LSV. Responsible: Jean Goubault-Larrecq
- EPIs Comète and Parsifal at INRIA Saclay. Responsible: Catuscia Palamidessi
- CEA LIST. Responsible: Olivier Bouissou
- Supelec SSE. Responsible: Gilles Fleury
- Supelec L2S. Responsible: Michel Kieffer

7.2. International Initiatives

7.2.1. DRI Equipe Associée PRINTEMPS

PRINTEMPS (PRobability and INformation Theory for Modeling Privacy and Secrecy) focuses on the applications of Information Theory to security. We are particularly interested in studying the interactions between Concurrency and Information Theory.

This project has started in January 2006 and includes the following sites:

- INRIA Futurs. Responsible: C. Palamidessi
- McGill University, Canada. Responsible: P. Panangaden

Home page: [http://www.lix.polytechnique.fr/comete/Projects/Printemps/](http://www.lix.polytechnique.fr/comete/Projects/Printemps/)

7.2.1.1. International Partners

- Moreno Falaschi, Dipartimento di Scienze Matematiche e Informatiche, Università di Siena, Italy.
- Camillo Rueda and Carlos Olarte, Pontificia Universidad Javeriana, Colombia.
- Geoffrey Smith, School of Computing and Information Sciences, Florida International University, USA
- Vladimiro Sassone, School of Electronics and Computer Science University of Southampton, United Kingdom.

7.3. Exterior research visitors

7.3.1. Visits of International Scientists
• Geoffrey Smith, Professor at the Florida International University, USA. He visited for four months, from 26/8/2011 until 23/12/2011.
• Moreno Falaschi, professor at the Università di Siena, Italy. He visited for one month, from 1/11/2011 till 30/11/2011.
• Vladimiro Sassone, professor at the University of Southampton, United Kingdom, Italy. He visited for one month, from 1/12/2011 till 31/12/2011.

7.3.2. Internship

• Marco Stronati, master student at the Università di Pisa, Italy. He is visiting for six months, from 1/10/2011 till 31/3/2012. He is doing his master thesis under the co-supervision of Giorgio Levi (Univ. di Pisa) and Catuscia Palamidessi.
• Lili Xu, PhD student at the Academy of Science of Beijing, China. She is visiting for nine months, from 15/10/2011 until 15/7/2012. She is doing her PhD thesis under the co-supervision of Huimin Li (Ch. Academy of Science, Beijing) and Catuscia Palamidessi.
8. Partnerships and Cooperations

8.1. National Initiatives

- ANR Investissement Avenir Iceberg project (2011-2016) coordinated by Grégory Batt, with Pascal Hersen (MSC lab, Paris Diderot Univ./CNRS), Reiner Veitia (Institut Jacques Monod, Paris Diderot Univ./CNRS), Olivier Gandrillon (BM2A lab, Lyon Univ./CNRS), Cedric Lhoussaine (LIFL/CNRS), and Jean Krivine (PPS lab, Paris Diderot Univ./CNRS).


- ANR Cosinus Syn2art project (2010-2013) coordinated by Grégory Batt, with Oded Maler, CNRS Verimag, Dirk Drasdo, EPI Bang, and Ron Weiss, MIT.


- ANR Syscomm project CALAMAR (2009-2011) “Compositional modeling and Analysis of LAarge MoleculAR Regulatory networks - application to the control of human cell proliferation.”, coordinated by C. Chaouiya, TAGC INSERM Marseille, L. Calzone, Institut Curie, Paris,


- GENCI (2009-) attribution of 300000 computation hours per year on the cluster SGI of 10000 processors at CINES, Montpellier.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, except FP7

Program: EraNet SYsBio
Project acronym: C5Sys
Project title: Circadian and cell cycle clock systems in cancer
Duration: mars 2010 - mars 2013
Coordinator: Francis Lévi, INSERM Hopital Paul Brousse, Villejuif, France and David Rand, Warwick Systems Biology, UK,
Other partners: EPI BANG, Erasmus University Medical Center, Rotterdam, University College London, UK, CNRS Nice, and L2S, Orsay.
Abstract: Mammalian cells are endowed with biological oscillators which time their activities. The circadian clock (circa, about; dies, day) generates a 24-hour rhythm which controls both cellular metabolism and cell division. The cell division cycle is an oscillator which times DNA synthesis, mitosis, and related apoptosis and DNA repair. Our understanding of the molecular mechanisms at work in both oscillators has greatly improved. In sharp contrast, little is known about how these two crucial oscillators interact, and how these interactions affect cellular proliferation in normal or cancer cells. On the one hand, the disruption of circadian clocks impairs cell physiology and quality of life. On the other hand, disruption of cell cycle, DNA repair or apoptosis impacts on cell and organism survival. Experimental and clinical data show that circadian disruption accelerates malignant proliferation, and that DNA damage can reset the circadian clock. The central question addressed is how interactions between the circadian clock and cell cycle affect cellular proliferation and genotoxic sensitivity in normal and cancer cells, and how this knowledge translates into new prevention or therapeutic applications. Seven teams in France, Netherlands and United Kingdom integrate experimental, mathematical and bioinformatic approaches, so as to develop novel cell lines, biomarker monitoring methods and mathematical tools. C5Sys triggers innovative chronotherapeutic research for human cancers and advances systems medicine for improving patient care.

8.3. International Initiatives

8.3.1. INRIA International Partners

We have tight collaborations with the Weiss lab for synthetic biology at MIT, USA, through participation in the ANR Syne2arti project coordinated by Grégory Batt, and through the joint supervision of Xavier Duportet’s PhD thesis.

We also have a starting collaboration with the Center for Systems and Control at the Delft University of Technology (The Netherlands) on developing formal probabilistic approaches for robust control of gene expression. This collaborative project is funded by the Frans/Nederlandse Academie as part of the van Gogh Programm (Coordination Alessandro Abate/Grégory Batt).

8.3.2. Visits of International Scientists

8.3.2.1. Visiting Professor

Calin Belta, Boston University, USA (2 months),

8.3.2.2. Internships

Gopalakrishnan Kumar
Subject: Stochastic model of the yeast Met3 promoter
Institution: IIT Bombay (India)

Armando Gonçalves Da Silva Junior
Subject: Generating Explanatory Traces for Rule-Based Constraint Reasoning CHR
Institution: Federal University of Pernambuco (UFPE) (Brazil)

Philip Robin
Subject: Hybrid Simulations with Events
Institution: IIT New Delhi (India)

8.3.2.3. Short visits

Xuefeng Gao, University College, Cork, Ireland,
Neda Saeedloei, University of Texas, Dallas, USA
Yaakov Setty, Weizmann Institute, Rehovot, Israel,
Szymon Stoma, Humboldt University, Berlin, Germany

8.3.3. Participation In International Programs

Program: STIC AmSud
Project acronym: TODAS
Project title: Trace Observation Driven Adaptive Solvers
Duration: janvier 2010 - décembre 2011
Coordinator: Pierre Deransart INRIA
Other partners: Eric Monfroy, UFSTM, Chile, Luis Menezes, UPE, Brazil, J. Robin, UFPE, Brazil, and F. Saubion, LERIA, U. Angers.
Abstract: The objective of the project is to define or improve self-adaptive constraint solving algorithms (Boolean, finite domains, local search or rules CHR) and their essential parameters, with an approach partly based on generic traces, to allow experimentation on different classes of solvers. At INRIA we worked in two directions: the development of a generic trace for CHR\(^*\) [11], and the integration of the approach of generic trace to describe different kinds of adaptive solvers.
FORMES Team

8. Partnerships and Cooperations

8.1. National Initiatives

- FORMES is part of the working group LTP on Languages, Types and Proofs of the GDR GPL\(^{10}\), the French research network on software engineering.
- FORMES is part of the working group LAC on Logic, Algebra and Calculus of the GDR IM\(^{11}\), the French research network on mathematics and computer science.

8.2. International Initiatives

8.2.1. Visits of International Scientists

8.2.1.1. Long-term visitors

- Jean-Jacques Lévy (INRIA, France), director of the MSR-INRIA Joint Center, visited FORMES from September 26 to November 18, gave lectures on reductions and causality.
- Pierre-Louis Curien (PPS, CNRS and University Paris 7) visited FORMES in April and May, and co-organized a working group on rewriting theory and algebra.
- Joseph Sifakis (VERIMAG, France) visited FORMES in March and October and participated to various working groups.

8.2.1.2. Short-term visitors

- Zhang Min (JAIST, Japan) gave a talk on December 20 on algebraic-based verification of a dynamic software updating system.
- Vladimir Voevodsky (IAS Princeton, USA), Fields Medal 2002, gave a talk on December 12 on univalent semantics of constructive type theories.
- Jianhua Gao (ISCAS, China) gave a talk on November 25 on the clausal presentation of theories in deduction modulo.
- Iddo Tzameret (ITCS, Tsinghua University) gave a talk on November 18 on short propositional refutations for dense random 3-CNF formulas.
- Eric Madelaine (INRIA, France) gave a talk on November 11 at Shenzhen SIAT on specification, model generation and verification of distributed applications.
- Jean-Raymond Abrial (ETH, Switzerland) gave a talk on September 9 on modeling, refining and proving with Event-B.
- Graham Steel (LSV, ENS Cachan, France) gave lectures on the security of APIs at Tsinghua University and Nokia from August 22 to August 25.
- Thomas Anberree (Nottingham University at Ningbo, China) gave a talk on June 22 on definable quotients in type theory.
- Hsu-Chun Yen (National Taiwan University) gave a talk on May 20 on two-way transducers and parametrized machines.
- Lijun Zhang (Denmark Technical University) gave a talk on May 13 on ODEs in probabilistic model checking.

\(^{10}\) http://gdr-gpl.cnrs.fr/
\(^{11}\) http://www.gdr-im.fr/
• Flemming Nielson (Denmark Technical University) gave a talk on May 13 on model checking as static analysis of modal logic.

• Christian Urban (TU Munich, Germany) gave a talk on April 29 on verifying a regular expression matcher and formal language theory.

• Zhaohui Luo (University of London, UK) visited FORMES in April and gave lectures on type theory from April 13 to April 19.

• On April 11, for the 1st Tsinghua Software Day organized by the FORMES team, we had the following talks: A journey into the semantics of programming languages, by Pierre-Louis Curien; type theory and its application, by Zhaohui Luo; advances towards the formal proof of the classification of finite groups, by Georges Gonthier; from boolean to quantitative theories of software, by Tom Henzinger.

• Joseph Sifakis (VERIMAG, France) gave a talk on March 10 on a vision for computer science: the system perspective.

8.2.2. Participation In International Programs

• SIVES\textsuperscript{12} is a French-Chinese ANR-NSFC project for 2009-2011 between INRIA FORMES, Tsinghua University and ST Microelectronics on the development of a “Simulation and Verification based platform for Embedded Systems” (coordinated by Frédéric Blanqui on the French side and Ming Gu on the Chinese side).

• Logical Frameworks is a grant from the National Science Foundation of China obtained by Jean-Pierre Jouannaud and Jianqi Li to sustain their work on the subject.

\textsuperscript{12} http://formes.asia/cms/sives
GALLIUM Project-Team

8. Partnerships and Cooperations

8.1. National initiatives

8.1.1. ANR U3CAT

Participant: Xavier Leroy.

The Gallium project participates in the “U3CAT” project of the Arpège programme of Agence Nationale de la Recherche. This 3.5-year action (2009-2012) is coordinated by CEA LIST and focuses on program verification tools for critical embedded C codes. We are involved in this project on issues related to memory models and formal semantics for the C language, at the interface between compilers and verification tools.

8.1.2. FNRAE Ascert

Participant: Xavier Leroy.

The “Ascert” project (2009-2011) is coordinated by David Pichardie at INRIA Rennes and funded by Fondation de Recherche pour l’Aéronautique et l’Espace. The objective of Ascert is to investigate the formal verification of static analyzers.

8.1.3. IRIILL

Participants: Roberto Di Cosmo, Didier Rémy.

Roberto Di Cosmo has been working on the creation of the IRIILL (Initiative d’Innovation et Recherche sur le Logiciel Libre), also known as FSRII (Free Software Research and Innovation Institute), which has the ambition of providing an attractive environment to researchers working on the new, emerging scientific issues coming from Free Software (the work on package dependencies is an archetypical example), to industry players willing to collaborate with researchers on these issues, and to educators working on improving the CS Curricula using Free and Open Source Software.

IRILL is an INRIA joint initiative with University Paris Diderot and University Pierre et Marie Curie. It was established by an agreement formally signed on November 2nd 2010, and its activity started with the IRIILL Days event in October 2010. IRIILL is currently hosting three major research projects (see http://www.irill.org).

8.1.4. LaFoSec

Participant: Damien Doligez.

The LaFoSec study, commissioned by ANSSI, aims at studying the security properties of functional languages, and especially of OCaml. The study is done by a consortium led by the SafeRiver company. It has produced more than 600 pages of documents. Most of these documents will be available from the ANSSI Web site (http://ssi.gouv.fr/). The study continues with the production of a prototype of a secure XML/XSD validator following the recommendations proposed in the first part of the study.

8.2. Regional initiatives

8.2.1. Digiteo Metal

Participants: François Pottier, Nicolas Pouillard.

The Metal project (2008-2011) of the Digiteo RTRA is coordinated by François Pottier. It focuses on formal foundations and static type systems for meta-programming.

8.2.2. Digiteo Hisseo

Participant: Xavier Leroy.

The Hisseo project (2008-2011) of the Digiteo RTRA is coordinated by Pascal Cuq at CEA LIST. It studies issues related to floating-point arithmetic in static analyzers and verified compilers.
MARELLE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

- We were the leader of the ANR project Galapagos, which started on Nov. 19th 2007 and finished on Nov. 19th 2011. Other participants in this contract are the universities of Strasbourg and Poitiers, ENSIEE in Evry and the Ecole Normale Supérieure in Lyon. The objective of this contract is to study the formal description of geometric concepts and algorithms.

- We participated to the ANR SCALP, which started on January 1st, 2008. Other participants in this contract were DCS-Verimag (Grenoble), Plume-LIP (Lyon), Proval-LRI (Orsay), CPR-Cédric (Cnam, Paris). In this project we focused on the formalization of Cryptography.

- We participated to the ANR project DeCert, which started on January 2009. Other participants are CEA List (Paris), LORIA-INRIA (Nancy), Celtique (IRISA Rennes), Proval (LRI Orsay), Typical (INRIA Saclay), Systerel (Aix-en-provence). The objective of the DeCert project was to design an architecture for cooperating decision procedures. 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.

- We participate to the ANR project TAMADI, which started in October 2010. Other participants are ARENAIRE-INRIA Rhone-Alpes and the PEQUAN team from University of Paris VI Pierre and Marie Curie. The objective of the TAMADI project is to study question of precision in floating-point arithmetic and to provide formal proofs on this topic.

7.2. European Initiatives

7.2.1. FP7 Projet

7.2.1.1. FORMATH

Title: Formath
Type: COOPERATION (ICT)
Defi: FET Open
Instrument: Specific Targeted Research Project (STREP)
Duration: March 2010 - February 2013
Coordinator: University of Göteborg (Sweden)
Others partners: Radboud University Nijmegen, (the Netherlands), University of La Rioja, (Spain).
See also: http://wiki.portal.chalmers.se/cse/pmwiki.php/ForMath/ForMath

Abstract: The objective of this project is to develop libraries of formalised mathematics concerning algebra, linear algebra, real number computation, and algebraic topology. The libraries that we plan to develop in this proposal are especially chosen to have long-term applications in areas where software interacts with the physical world. The main originality of the work is to structure these libraries as a software development, relying on a basis that has already shown its power in the formal proof of the four-colour theorem, and to address topics that were mostly left untouched by previous research in formal proof or formal methods.

7.2.2. Major European Organizations with which you have followed Collaborations

Chalmers University, Programming Logic Group, (Sweden)
Type Theory and its application to formalizing of mathematics, especially algebraic concepts.

Radboud University, ICIS, Foundations group, (the Netherlands)
Type theory and its application to formalizing mathematics, especially numeric computation.

University of La Rioja, Programming and Symbolic Computation Team, (Spain)
Formal study of algebraic algorithms and application to algebraic topology.
8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. DIGITEO 2009-27HD CoChat: Covert Channels in Timed Systems

**Participant:** Serge Haddad.

Attacks with timing channels have been described and simulated for instance on TCP/IP protocols, Web communications or cryptographic operations. The scientific objective of the CoChat project is to study the conditions under which such attacks can occur in timed systems, with two main directions. a. The first step consists in defining a theoretical framework, in which timing channels can be formally described. b. A second part of the work concerns the design of detection and verification algorithms, for which decidability issues are involved. Progress in both steps will have to take into account practical examples like the case studies mentioned above, in order to validate the formal approach.

8.1.2. DIGITEO 2010 PhD Grant (LoCoReP)

**Participants:** Benedikt Bollig, Aiswarya Cyriac, Paul Gastin, Marc Zeitoun.

Benedikt Bollig and Paul Gastin obtained a DIGITEO PhD grant for their student Aiswarya Cyriac. The aim of the PhD will be to design linear-time temporal logics for concurrent recursive programs.

8.1.3. DIGITEO 2011 PhD Grant (TECSTES)

**Participants:** Stefan Haar, Hernán Ponce de Léon.

Stefan Haar and Delphine Longuet of LRI, Univ. Paris-Sud/Orsay, have obtained a DIM/LSC grant for the project TECSTES which finances the PhD thesis of their student Hernán Ponce de Léon. The subject of the project is the asynchronous testing of concurrent systems via Event Structures.

8.2. National Initiatives

8.2.1. ANR ImpRo ANR-2010-BLAN-0317

**Participants:** Sandie Balaguer, Thomas Chatain, Stefan Haar, Serge Haddad, Stefan Schwoon.

This project involves IRCCyN (Nantes), IRISA (Rennes), LIP6 (Paris), LSV (Cachan), LIAFA (Paris), LIF (Marseille)

It addresses the issues related to the practical implementation of formal models for the design of communicating embedded systems: such models abstract many complex features or limitations of the execution environment. The modeling of time, in particular, is usually ideal, with infinitely precise clocks, instantaneous tests or mode commutations, etc. Our objective is thus to study to what extent the practical implementation of these models preserves their good properties. We will first define a generic mathematical framework to reason about and measure implementability, and then study the possibility to integrate implementability constraints in the models. We will particularly focus on the combination of several sources of perturbation such as resource allocation, the distributed architecture of applications, etc. We will also study implementability through control and diagnostic techniques. We will finally apply the developed methods to a case study based on the AUTOSAR architecture, a standard of the automotive industry.

8.2.2. ANR CHECKBOUND ANR-06-SETI-002

**Participants:** Hilal Djafri, Serge Haddad.
The increasing use of computerised systems in all aspects of our lives gives an increasing importance on the need for them to function correctly. The presence of such systems in safety-critical applications, coupled with their increasing complexity, makes indispensable their verification to see if they behave as required. Thus the model checking techniques, i.e. the automated form of formal verification, are of particular interest. Since verification techniques have become more efficient and more prevalent, the natural extension is to extend the range of models and specification formalisms to which model checking can be applied. Indeed the behaviour of many real-life processes is inherently stochastic, thus the formalism has been extended to probabilistic model checking. Therefore, different formalisms in which the underlying system has been modelled by Markovian models have been proposed.

Stochastic model checking can be performed by numerical or statistical methods. In model checking formalism, models are checked to see if the considered measures are guaranteed or not, bounding techniques become useful. We propose to apply Stochastic Comparison technique for numerical stochastic model checking. The main advantage of this approach is the possibility to derive transient and steady-state bounding distributions as well as the possibility to avoid the state space explosion problem. For the statistical model checking we propose to study the application of perfect simulation by coupling in the past. This method has been shown that to be efficient when the underlying system is monotonic for the exact steady-state distribution sampling. We consider to extend this approach for transient analysis and to model checking by means of bounding models and the stochastic monotonicity. One of difficult problems for model checking formalism, we envisage to study is when the state space is infinite. In some cases, it would be possible to consider bounding models defined in finite state space.

Indeed, formal verification using model checking and performance and dependability evaluation have a lot of things in common. We think that it would be interesting to apply the methods that we have a large experience in quantitative evaluation in the context of stochastic model checking.

8.3. European Initiatives

8.3.1. FP7 Projects

8.3.1.1. Univerself

Participants: Stefan Haar, Serge Haddad.

Title: Univerself
Type: COOPERATION (ICT)
Defi: The Network of the Future
Instrument: Integrated Project (IP)
Duration: September 2010 - August 2013
Coordinator: Alcatel Lucent (France)

Others partners:
- Universiteit Twente,
- Alcatel Lucent Ireland,
- Alcatel Lucent Deutschland,
- Valtion Teknillinen Tutkimuskeskus (Finland),
- University of Piraeus,
- France Telecom,
- Telecom Italia,
- National University of Athens,
- Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung.
Abstract: *UniverSelf* unites 17 partners with the aim of overcoming the growing management complexity of future networking systems, and to reduce the barriers that complexity and ossification pose to further growth. *UniverSelf* has been launched in October 2010 and is scheduled for four years.

### 8.3.2. Collaborations in European Programs, except FP7

#### 8.3.2.1. DISC: Grant Agreement 224498

**Participants:** Stefan Haar, Serge Haddad.

Serge Haddad and Stefan Haar are participating, as associate members of INRIA Rennes, in the Project on *Distributed Supervisory Control of Large Plants - DISC*. The European Commission supports the project financially by the EU.ICT program, Challenge ICT-2007.3.3 (Information and Communication Technologies (ICT)). 1 September 2008 - 1 September 2011. Project partners:

- University of Cagliari (coordinator),
- CWI - Amsterdam, Ghent University,
- Technical University of Berlin,
- University of Zaragoza,
- INRIA,
- Akhela s.r.l. Italy,
- Czech Academy of Sciences,
- Ministry of the Flemish Government,
- CyBio AG.

Serge Haddad and Stefan Haar are among the INRIA participants of the IP *UniverSelf* on autonomous Management in telecommunications, along with members of the Distribcom group at INRIA Rennes and the MADYNES group at INRIA Nancy. The project consortium is:

#### 8.3.2.2. Hycon2

**Participants:** Stefan Haar, Serge Haddad.

**Title:** Hycon2 (Highly-complex and networked control systems)

**Type:** COOPERATION (ICT)

**Defi:** Engineering of Networked Monitoring and Control Systems

**Instrument:** Network of Excellence (NoE)

**Duration:** September 2010 - August 2014

**Coordinator:** CNRS (France)

**Others partners:**
8.3.3. Major European Organizations with which we cooperate

TU München, Lehrstuhl Esparza (Germany) organisme 1, labo 1 (pays 1)
Unfoldings of Petri nets (reveals relation)

University of Padova, Department of Pure and Applied mathematics (Italy)
Analysis of Contextual nets and their unfoldings

DISCO team, Università degli Studi di Milano (Italy)
Structural analysis of partially ordered structures, in particular orthomodularity.

8.4. International Initiatives

8.4.1. Visits of International Scientists
• Madhavan Mukund of CMI Chennai, India, visited (within the ARCUS project) from May 1 to May 2011.
• K. Narayan Kumar of CMI Chennai, India, visited (within the ARCUS project) from May 2 to June 5 and from Nov 7 to November 20.
• From February 23 to 25, the team received the visit of Lucia Pomello, Luca Bernardinello (both professors of the University of Milan, Italy) and Carlo Ferigato researcher at JRC Ispra, Italy.

8.4.1.1. Internship

Roshan Kumar (IIT Delhi, India) cancelled his summer internship due to illness

Subject: Petri net unfolding methods for verifying weak properties
Institution: IIT Delhi (India)

8.4.2. Visit to other laboratories

• Stefan Schwoon visited the LABRI on February 16 to work with Jerome Leroux and to give a talk in the MVTSI seminar. From Nov 17 to 21, he visited Javier Esparza’s group at TU München and gave a talk in the PUMA seminar.
• Within the DISC project, Serge Haddad and Stefan Haar participated in the project meeting at CWI Amsterdam, March 14–16, and the summer school in Cagliari, June 6-10.
• Stefan HAAR visited the DISCO team of Lucia Pomello and Luca Bernardinello at University of Milan from June 8 to June 10.
• In October 2011, Benedikt Bollig joined Dietrich Kuske’s group at the Technische Universität Ilmenau, Germany, for two weeks.
• Serge Haddad gave talks at the DISC summer school in Cagliari (June 6-10) and an invited talk at the summer school of the University of Western Brittany (August 29 to September 1).

8.4.3. Participation In International Programs

8.4.3.1. ARCUS Inde

Most members of the team have participated in the sub-project 4, Formal approaches for computer systems, of the Île de France/INDE project of the ARCUS Program (Region Île de France and French Ministry of foreign affairs), initially funded for 3 years (2008–2010) and extended until September 2011.

To pursue the very active and fruitful collaboration with our Indian partners, we have proposed the creation of an INTERNATIONAL ASSOCIATED LABORATORY (LIA). The LIA is called INFORMEL which stands for INdo-French FORmal MEthods Lab. The scientific coordinators are Paul Gastin (LSV, ENS Cachan) and Madhavan Mukund (CMI, Chennai). The french partners are mainly from LSV (ENS Cachan) and LaBRI (Bordeaux). The indian partners are from the Chennai Mathematical Institute (CMI), the Institute of Mathematical Sciences (IMSc) and the Indian Institute of Science (IISc) of Bangalore. The LIA proposal has been positively evaluated by the CoNRS and should be created on January 1st 2012.
MOSCOVA Project-Team (section vide)
7. Partnerships and Cooperations

7.1. National Initiatives

We participate in the “Logic and Complexity” part of the GDR–IM (CNRS Research Group on Mathematical Computer Science), in the projects “Logic, Algebra and Computation” (mixing algebraic and logical systems) and “Geometry of Computation” (using geometrical and topological methods in computer science).

We participate and co-animate the “Transformation” group of the GDR–GPL (CNRS Research Group on Software Engineering).

7.1.1. ANR Complice (2009-2012)

Participant: Yves Guiraud.

The ANR project “Complexité implicite, concurrence et extraction” (Complice), headed by Patrick Baillot (CNRS, LIP Lyon), federates researchers from Lyon (LIP), Nancy (LORIA) and Villetaneuse (LCR). The coordinator for the LORIA site is Guillaume Bonfante (Carte).

7.1.2. ARC ACCESS (2010-2011)

Participant: Horatiu Cirstea.

This project is concerned with the security and access control for Web data exchange, in the context of Web applications and Web services. We aim at defining automatic verification methods for checking properties of access control policies (ACP) for XML, like consistency or secrecy. A more detailed presentation is available at http://acxml.gforge.inria.fr/.

7.1.3. FRAE QUARTEFT (2009-2012)

Participants: Jean-Christophe Bach, Horatiu Cirstea, Pierre-Etienne Moreau.

“QUARTEFT: QUAlifiable Real TimE Fiacre Transformations” is a research project founder by the FRAE (Fondation de Recherche pour l’Aéronautique et l’Espace). A first goal is to develop an extension of the Fiacre intermediate language to support real-time constructs. A second goal is to develop new model transformation techniques to translate this extended language, Fiacre-RT, into core Fiacre. A main difficulty consists in proposing transformation techniques that could be verified in a formal way. A more detailed presentation is available at http://quarteft.loria.fr/dokuwiki/.

7.2. International Initiatives

7.2.1. Visits of International Scientists

Cooperation with Prof. Mark van den Brand from Technical University of Eindhoven.
7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. CPP: ANR on Confidence, Proofs, and Probabilities

**Participants:** Ivan Gazeau, Dale Miller.

The ANR Blanc titled “CPP: Confidence, Proofs, and Probabilities” has started 1 October 2009. This grant brings together the following institutions and individuals: LSV (Jean Goubault-Larrecq), CEA LIST (Eric Goubault, Olivier Bouissou, and Sylvie Putot), INRIA Saclay (Catuscia Palamidessi, Dale Miller, and Stéphane Gaubert), Supelec L2S (Michel Kieffer and Eric Walter), and Supelec SSE (Gilles Fleury and Daniel Poulton). This project proposes to study the joint use of probabilistic and formal (deterministic) semantics and analysis methods, in a way to improve the applicability and precision of static analysis methods on numerical programs. The specific long-term focus is on control programs, e.g., PID (proportional-integral-derivative) controllers or possibly more sophisticated controllers, which are heavy users of floating-point arithmetic and present challenges of their own. To this end, we shall benefit from case studies and counsel from Hispano-Suiza and Dassault Aviation, who will participate in this project, but preferred to remain formally non-members, for administrative reasons.

7.1.2. Panda: ANR on Parallelism and Distribution Analysis

**Participant:** Dale Miller.

The ANR Blanc titled “Panda: Parallelism and Distribution Analysis” has started 1 October 2009. This project brings together researchers from INRIA Saclay (Comète and Parsifal), CEA LIST, MeASI as well labs in Paris (LIPN, PPS, LSV, LIP, LAMA), and on the Mediterranean (LIF, IML, Airbus). Scientifically, this proposal deals with the validation of concurrent and distributed programs, which is difficult because the number of its accessible states is too large to be enumerated, and even the number of control points, on which any abstract collecting semantics is based, explodes. This is due to the great number of distinct scheduling of actions in legal executions. This adds up to the important size of the codes, which, because they are less critical, are more often bigger. The objective of this project is to develop theories and tools for tackling this combinatorial explosion, in order to validate concurrent and distributed programs by static analysis, in an efficient manner. Our primary interest lies in multithreaded shared memory systems. But we want to consider a number of other paradigms of computations, encompassing most of the classical ones (message-passing for instance as in POSIX or VXWORKS) as well as more recent ones.

7.1.3. PSI: ANR on Proof Search in Interaction with Domain-specific methods

**Participants:** Stéphane Lengrand, Mahfuza Farooque.

The ANR Jeune Chercheuse / Jeune chercheur titled “PSI: Proof Search in Interaction with Domain-specific methods” has started 1 September 2009. This project investigates how proof-search can be performed in a framework where reasoning is subject to highly specific inference rules or axioms. This encompasses reasoning modulo a theory for which we may have a decision procedure (linear arithmetic, etc), or reasoning in a particular type theory (e.g. in a Pure Type system). The field of automated reasoning offers a variety of techniques (SAT-modulo-Theory, etc) which we like to see in terms of proof search. The project represent 192 000 euros of funding over four years, and is in collaboration with Assia Mahboubi at the TypiCal team.
7.2. International Initiatives

7.2.1. STRUCTURAL: ANR blanc International

Participants: Kaustuv Chaudhuri, Nicolas Guenot, Willem Heijltjes, Clément Houtmann, Dale Miller, Lutz Straßburger.

- Title: Structural and computational proof theory
- Duration: 01/01/2011 – 31/12/2013
- Partners:
  - University Paris VII, PPS (PI: Michel Parigot)
  - INRIA Saclay–IdF, EPI Parsifal (PI: Lutz Straßburger)
  - University of Innsbruck, Computational Logic Group (PI: Georg Moser)
  - Vienna University of Technology, Theory and Logic Group (PI: Matthias Baaz)
- Total funding by the ANR: 242 390,00 EUR (including 12 000 EUR pôle de compétivité: SYSTE-MTIC Paris région)

This project is a consortium of four partners, two French and two Austrian, all being internationally recognized for their work on structural proof theory, but each coming from a different tradition. One of the objective of the project is build a bridge between these traditions and develop new proof-theoretic tools and techniques of structural proof theory having a strong potential of applications in computer science, in particular at the level of the models of computation and the extraction of programs and effective bounds from proofs.

On one side, there is the tradition coming from mathematics, which is mainly concerned with first-order logic, and studies, e.g., Herbrand’s theorem, Hilbert’s epsilon-calculus, and Gödel’s Dialectica interpretation. On the other side, there is the tradition coming from computer science, which is mainly concerned with propositional systems, and studies, e.g., Curry-Howard isomorphism, algebraic semantics, linear logic, proof nets, and deep inference. A common ground of both traditions is the paramount role played by analytic proofs and the notion of cut elimination. We will study the inter-connections of these different traditions, in particular we focus on different aspects and developments in deep inference, the Curry-Howard correspondence, term-rewriting, and Hilbert’s epsilon calculus. As a byproduct this project will yield a mutual exchange between the two communities starting from this common ground, and investigate, for example, the relationship between Herbrand expansions and the computational interpretations of proofs, or the impact of the epsilon calculus on proof complexity.

Besides the old, but not fully exploited, tools of proof theory, like the epsilon-calculus or Dialectica interpretation, the main tool for our research will be deep inference. Deep inference means that inference rules are allowed to modify formulas deep inside an arbitrary context. This change in the application of inference rules has drastic effects on the most basic proof theoretical properties of the systems, like cut elimination. Thus, much of the early research on deep inference went into reestablishing these fundamental results of logical systems. Now, deep inference is a mature paradigm, and enough theoretical tools are available to think to applications. Deep inference provides new properties, not available in shallow deduction systems, namely full symmetry and atomicity, which open new possibilities at the computing level that we intend to investigate in this project. We intend to investigate the precise relation between deep inference and term rewriting, and hope to develop a general theory of analytic calculi in deep inference. In this way, this project is a natural continuation of the ANR project INFER which ended in May 2010.

7.2.2. Eternal: INRIA ARC

Participants: Kaustuv Chaudhuri, Dale Miller, Lutz Straßburger.

Title: Interactive Resource Analysis
webpage: http://eternal.cs.unibo.it/
INRIA principal investigator: Dale Miller  
INRIA Partner:  
- Institution: INRIA  
- Team: FOCUS  
- Researcher: Ugo Dal Lago  

INRIA Partner:  
- Institution: INRIA  
- Team: pi.r2  
- Researcher: Pierre-Louis Curien  

Duration: 2011 - 2013  
This project aims at putting together ideas from Implicit Computational Complexity and Interactive Theorem Proving, in order to develop new methodologies for handling quantitative properties related to program resource consumption, like execution time and space. The task of verifying and certifying quantitative properties is undecidable as soon as the considered programming language gets close to a general purpose language. So, full-automatic techniques in general cannot help in classifying programs in a precise way with respect to the amount of resources used and moreover in several cases the programmer will not gain any relevant information on his programs. In particular, this is the case for all the techniques based on the study of structural constraints on the shape of programs, like many of those actually proposed in the field of implicit computational complexity. To overcome these limitations, we aim at combining the ideas developed in the linear logic approach to implicit computational complexity with the ones of interactive theorem proving, getting rid of the intrinsic limitations of the automatic techniques. In the obtained framework, undecidability will be handled through the system’s user, who is asked not only to write the code, but also to drive the semi-automatic system in finding a proof for the quantitative properties of interest. In order to reduce the user effort and allow him to focus only on the critical points of the analysis, our framework will integrate implicit computational complexity techniques as automatic decision procedures for particular scenarios. Moreover, in order to be widely applicable, the modularity of the framework will permit to deal with programs written in different languages and to consider different computational resources. The kind of study proposed by this project has been almost neglected so far. Here, we aim at providing such a framework for both theoretic investigations and for testing in practice the effectiveness of the approach.  

7.2.3. INRIA Associate Teams  
7.2.3.1. RAPT  
Participants: Beniamino Accattoli, Kaustuv Chaudhuri, Quentin Heath, Clément Houtmann, Dale Miller.  
Title: Computational logic systems  
INRIA principal investigator: Kaustuv Chaudhuri  
International Partner:  
- Institution: McGill University (Canada)  
- Laboratoray: School of Computer Science  
- Researcher: Brigitte Pientka  

International Partner:  
- Institution: Carnegie Mellon University (United States)
Laboratory: Department of Computer Science
Researcher: Frank Pfenning

Duration: 2011 - 2013
See also: http://www.lix.polytechnique.fr/~kaustuv/rapt/

Many aspects of computation systems, ranging from operational semantics, interaction, and various forms of static analysis, are commonly specified using inference rules, which themselves are formalized as theories in a logical framework. While such a use of logic can yield sophisticated, compact, and elegant specifications, formal reasoning about these logic specifications presents a number of difficulties. The RAPT project will address the problem of reasoning about logic specifications by bringing together three different research teams, combining their backgrounds in type theory, proof theory, and the building of computational logic systems. We plan to develop new methods for specifying computation that allow for a range of specification logics (e.g., intuitionistic, linear, ordered) as well as new means to reason inductively and co-inductively with such specifications. New implementations of reasoning systems are planned that use interactive techniques for deep meta-theoretic reasoning and fully automated procedures for a range of useful theorems.

7.2.4. Visits of International Scientists

7.2.4.1. Invited Researchers

- Alberto Momigliano, Associate Professor, University of Milan
  24 - 28 January and 30 - 31 August.

- Vivek Nigam, Research Scientist, LMU, Munich, Germany.
  26 April - 6 May.

- Chuck Liang, Professor, Hofstra University, NY, USA.
  2 June - 1 July

- Gopalan Nadathur, Professor, University of Minnesota, MN, USA.
  6 - 10 June and 3 - 28 October.

- Elaine Pimentel, Associate Professor, Universidade Federal de Minas Gerais.
  13 - 24 June.

- Brigitte Pientka, Associate Professor, McGill University, Montreal, Canada.
  16 - 20 May.

- Alwen Tiu, Research Scientist, Australian National University.
  22 - 26 August.

- Anupam Das, PhD Student, University of Bath, UK.
  21 - 25 November 2011

7.2.4.2. Internships

- Andrew Cave, PhD student at McGill Univ., Montreal, Canada.
  Internship during May – July 2011

- Salil Joshi, PhD student at Carnegie Mellon Univ., USA.
  Internship during June – August 2011

- Chris Martens, PhD student at Carnegie Mellon Univ., USA.
  Internship during June – August 2011

7.2.5. Participation In International Programs

The team has travel funds within the following international programs.

- PHC Germaine de Staël 2011: funding travel between Bern, Switzerland and INRIA.
- 63.123 - 63ème CPCFQ: Commission permanente de coopération franco-québécoise: funding exchanges between the McGill and INRIA.
- INRIA-FAPEMIG: funding between INRIA and the Brazilian funding agency FAPEMIG located in the state of Minas Gerais.
PI.R2 Project-Team

8. Partnerships and Cooperations

8.1. International Initiatives

8.1.1. INRIA Associate Teams

8.1.1.1. SEMACODE

Title: Proof theory and functional programming languages
INRIA principal investigator: Alexis SAURIN

International Partner:
Institution: University of Oregon (United States)
Laboratory: Computer and Information Science Department
Researcher: Zena ARIOLA

International Partner:
Institution: University of Novi Sad
Laboratory: Faculty of Engineering
Researcher: Silvia GHILEZAN

Duration: 2011 - 2013
See also: http://www.pps.jussieu.fr/~saurin/EA-SEMACODE

Cross-fertilization between logic and programming languages theory is at the root of many striking developments in programming concepts as well as tools for formal analysis of programs. Our associated team project aims at gathering senior and young researchers from both sites in order to put a joint research effort on the following research themes: formalizing particular evaluation strategies of functional languages based logical techniques coming from sequent calculi. More specifically, we shall be interested in incorporating control operator directly in call-by-need and in developing a uniform framework for call-by-value and call-by-name calculi with delimited control investigating (delimited) control operators, in particular to unveil the logical interpretation of delimited control (that is its logical counter-part with respect to Curry-Howard correspondence), and developing connections between delimited control and stream calculi; developing the logical content of realistic abstract machines and associated formal analysis tools for realistic abstract machines building on Curien-Herbelin lambda-bar calculi. The project will gather PiR2 expertise in proof theory and in the logical foundations of functional programming languages, the expertise of the oregonian group on call-by-need evaluation and delimited control as well as respective crucial inputs of Gaboardi and Ghilezan on stream calculi, delimited control, semantics and type theory. The project will in particular allow to have the INRIA and American students and post-docs involved in the project (7 out of 13 people involved) to travel between both sites and to organize joint workshops (one such workshop is planned in June 2011).

8.1.2. Visits of International Scientists

Olivier Danvy (University of Aarhus) visited πr² and PPS for one month and gave a talk on call-by-need abstract machines.

Beta Ziliani (MPI, Sarbrucken) visited πr² and PPS for a week in november and gave a talk on ad-hoc proof automation.
Danko Ilik visited π² and PPS for one week and gave a talk on normalization by evaluation for delimited control.

Silvia Ghilezan (University of Novi Sad) visited π² and PPS for one week and worked with Alexis Saurin and Hugo Herbelin on the classification of several calculi of delimited control.

Zerna Ariola (University of Oregon) visited π² for one week and worked with Alexis Saurin and Hugo Herbelin on the definition of abstract amchines for classical call-by-need.

Keiko Nakata (University of Tallin) visited π² and worked with Hugo Herbelin on recursive definitions and control operators in call-by-need λ-calculus.

Gyesik Lee visited π² for one week and worked with Hugo Herbelin on the formal representation of binders in Coq and on representing primitive recursive arithmetic in Coq.

8.1.2.1. Internship

Paul Downen and Luke Maurer (University of Oregon) spent two months in the team during the summer, working with Alexis Saurin and Hugo Herbelin. Paul Downen studied calculi for multi-prompt, the derivation of abstract machines as well as infinitary λ-calculi. Luke Maurer studied Coq and did some formalization in Coq and studied Zeilberger’s polarized approach to delimited control as well as connections with Λµ-calculus.

8.1.3. Visits abroad of members of the team

Matthieu Sozeau visited Ana Bove in Gothenburg for a week in January and gave a talk on Equations and dependent pattern-matching. They worked on a joint paper on tools and methods for recursion in type theory.

Matthieu Sozeau visited Alexandar Nanvesky at IMDEA Madrid from 19th to 23rd october and gave a talk on Type Classes and unification. They worked on the unification algorithm of Coq.

Guillaume Munch-Maccagnoni visited the Programming, Logic, and Semantics Group at the University of Cambridge from March to June. He is grateful to the Fondation Sciences Mathematiques de Paris which provided the funding.

Pierre-Louis Curien visited the University of Tsinghua in Beijing for three months, from March to May (funded by the Professor Group Chair of the Software School of this university). He was hosted by Gu Ming and Jean-Pierre- Jouannaud.
8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Hisseo
Participants: Sylvie Boldo [contact], Claude Marché, Guillaume Melquiond, Thi-Minh-Tuyen Nguyen.

Hisseo is a 3 years Digiteo project that started in September 2008. http://hisseo.saclay.inria.fr

The Hisseo project focuses on the problems related to the treatment of floating-point computations in the compilation process, especially in the case of the compilation of critical C code.

Partners: CEA List (Saclay), INRIA Paris-Rocquencourt (Team Gallium).

8.1.2. Coquelicot
Participants: Sylvie Boldo [contact], Catherine Lelay, Guillaume Melquiond.

Coquelicot is a 3 years Digiteo project that started in September 2011. http://coquelicot.saclay.inria.fr. S. Boldo is the principal investigator of this project.

The Coquelicot project aims at creating a modern formalization of the real numbers in Coq, with a focus on practicality. This is sorely needed to ease the verification of numerical applications, especially those involving advanced mathematics.

Partners: LIX (Palaiseau), University Paris 13

8.1.3. Pactole
Participants: Évelyne Contejean, Jean-Christophe Filliâtre, Xavier Urbain [contact].

Pactole is a 3 year Digiteo project which started in October 2009.

The Pactole project focuses on automation and formal verification for ubiquitous, large scale environments. Tasks include proof automation techniques for distributed systems, verification conditions for fault tolerant distributed systems, specification and design of fundamental services for mobile sensor networks. The principal investigator of Pactole is Xavier Urbain.

Partners: CÉDRIC (CNAM/ENSIIE), LIP6 (UPMC).

8.2. National initiatives

8.2.1. U3CAT
Participants: Jean-Christophe Filliâtre, Claude Marché [contact], Guillaume Melquiond, Kalyan Krishnamani, Asma Tafat, Paolo Herms.

U3CAT (Unification of Critical C Code Analysis Techniques) is a project funded by ANR within its programme “Systèmes Embarqués et Grandes Infrastructures - ARPEGE”. It aims at verification techniques of C programs, and is partly a follow-up of the former CAT project. It started in January 2009 and will end in 2012.

The main goal of the project is to integrate various analysis techniques in a single framework, and make them cooperate in a sound way. We address the following general issues:

- Verification techniques for floating-point programs;
- Specification and verification of dynamic or temporal properties;
- Combination of static analysis techniques;
- Management of verification sessions and activities;
- Certification of the tools chains for compilation and for verification.
Partners: CEA-List (Saclay, project leader), Lande team (INRIA Rennes), Gallium team (INRIA Rocquencourt), Dassault Aviation (Saint-Cloud), Airbus France (Toulouse), ATOS Origin (Toulouse), CNAM Cedric laboratory (Evry), CS Communication & Systems (Toulouse), Hispano-Suiza/Safran (Moissy-Cramayel).

8.2.2. INRIA ADT Alt-Ergo

Participants: Sylvain Conchon [contact], Evelyne Contejean, Claude Marché, Alain Mebsout, Mohamed Iguernelala.

The ADT (Action de Développement Technologique) Alt-Ergo is a 2-years project funded by INRIA, started in September 2009.

The goal is the maturation of the Alt-Ergo prover towards its use in an industrial context in particular for avionics. The expected outcomes of this ADT are the following:

- improving the efficiency of Alt-Ergo;
- fine tuning of Alt-Ergo for the SMT competition;
- generation of counter-examples;
- the qualification of Alt-Ergo for the norm DO-178B.

External Collaborators: Airbus France (Toulouse), Dassault Aviation (Saint-Cloud), team Typical (INRIA, École Polytechnique).

8.2.3. FOST

Participants: Sylvie Boldo [contact], Jean-Christophe Filliâtre, Guillaume Melquiond.

FOST (Formal prOofs of Scientific compuTation programs) is a 3 years ANR “Blanc” project started in January 2009. S. Boldo is the principal investigator of this project. [http://fost.saclay.inria.fr](http://fost.saclay.inria.fr)

The FOST project follows CerPAN’s footprints as it aims at developing new methods to bound the global error of a numerical program. These methods will be very generic in order to prove a large range of numerical analysis programs. Moreover, FOST aims at providing reusable methods that are understandable by non-specialists of formal methods.

Partners: University Paris 13, INRIA Paris - Rocquencourt (Estime).

8.2.4. SCALP

Participants: Christine Paulin-Mohring [contact], David Baelde, Xavier Urbain.

This project is funded by ANR (program SESUR). [http://scalp.gforge.inria.fr/](http://scalp.gforge.inria.fr/)

It started on January 2008 for 4 years; the coordinator is Yassine Lakhnech from VERIMAG.

The SCALP project (Security of Cryptographic Algorithms with Probabilities) aims at developing automated tools for the verification of cryptographic systems.

Partners: Verimag, INRIA Sophia-Antipolis(Everest then Marelle team), ENS Lyon, LRI, CNAM.

8.2.5. DECERT

Participants: Sylvain Conchon, Évelyne Contejean, Stéphane Lescuyer.

DECERT (DEduction and CERTification) is an ANR “Domaines Emergents” project. It started on January 2009 for 3 years; the coordinator is Thomas Jensen from the Lande team of IRISA/INRIA Rennes.

The goal of the project DECERT is to design and implement new efficient cooperating decision procedures (in particular for fragments of arithmetics), to standardize output interfaces based on certificates proof objects and to integrate SMT provers with skeptical proof assistants and larger verification contexts such as the Rodin tool for B and the Frama-C/Jessie tool chain for verifying C programs.

The partners are: CEA List, LORIA/INRIA Nancy - Grand Est, IRISA/INRIA Rennes - Bretagne Atlantique, INRIA Sophia Antipolis - Méditerranée, Systerel
8.3. European Initiatives

8.3.1. Collaborations in European Programs, except FP7

8.3.1.1. FoVeOOS

Participants: Claude Marché [contact], Romain Bardou, François Bobot, Asma Tafat.


Project acronym: FoVeOOS (IC-0701, http://www.cost-ic0701.org/)

Project title: Formal Verification of Object-Oriented Software

Duration: May 2008 - April 2012

Coordinator: B. Beckert, University Karlsruhe, Germany

Other partners: 40 academic groups among 18 countries in Belgium, Denmark, Estonia, France, Germany, Ireland, Israel, Italy, The Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland and United Kingdom.

Abstract: The aim of this action is to develop verification technology with the reach and power to assure dependability of object-oriented programs on industrial scale.

8.4. International Initiatives

8.4.1. Visits of International Scientists

• D. Ishii (National Institute of Informatics, Japan) visited the team for 8 months to work on applying program verification methods to hybrid systems.

8.4.2. Supervision of Post-docs and Internships

• S. Boldo supervised the 6-month post-doc intern of E. Makarov (from University of Vermont, USA) about numerical analysis proofs in higher dimensions.

• C. Marché supervised the post-doc intern of K. Krishnamani (from University of Trento, Italy) until August: predicate abstraction techniques for critical C programs ([38] http://proval.lri.fr/agen).


• S. Conchon supervises the post-doc intern of D. Cousineau since October 2011: interpretation of Alt-Ergo’s proof traces in the Coq proof assistant.

• C. Paulin supervised the internship of N. Gaspar (Universidade da Beira Interior, Portugal) from January to September 2011. He studied the formal proof of concurrent programs using a rely-guarantee approach.

• E. Contejean, together with V. Benzaken (LRI), supervise the internship of S. Yuan (Zhejiang University, China) from October 2011 to March 2012: Automated constraints verification for databases with SMT solvers.

8.4.3. Participation In International Programs

C. Paulin is the representative of Univ. Paris-Sud for the education part of the EIT KIC ICT Labs. She contributed to the proposition of two master programs as well as the action on weaving Innovation and Entrepreneurship in Doctoral programs and the preparation of the SummerSchool “Imagine the future in ICT”.

7. Partnerships and Cooperations

7.1. Regional Initiatives


7.2. National Initiatives

  In the context of proofs of safety properties for critical software, The CPP project proposes to study the joint use of probabilistic and formal (deterministic) semantics and analysis methods, in a way to improve the applicability and precision of static analysis methods on numerical programs. See http://www.lix.polytechnique.fr/~bouissou/cpp/index.php.
  Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. However, the convenience of electronic elections comes with a risk of large-scale fraud and their security has seriously been questioned. The AVOTÉ project aims at proposing formal methods to analyze electronic voting protocols. See http://www.lsv.ens-cachan.fr/anr-avote/.
  The goal of the ProSe 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; and the implementation level: the program itself. This project is a continuation of the FormaCrypt project. See https://crypto.di.ens.fr/projects:prose:main.

7.3. INRIA Actions of Technological Development

- ADT Phalaenopsis, Dec. 2010-Dec. 2011. General improvement of the ORCHIDS tool (user interface, connexion with vulnerability and topology databases, enriching the signature base), and weaving a web of relations with interested industrial and institutional partners. Baptiste Gourdin was hired on this ADT in 2010-2011.

7.4. International Initiatives

7.4.1. Visits of International Scientists

- Olivier Pereira, Université Catholique de Louvain, Belgium, one week, March 2011.
- Mahesh Viswanathan, University of Illinois at Urbana-Champaign, one month, May 2011.

7.4.1.1. Internship
• Jan Degrieck, *Graph Reduction for Analysing Secure Routing Protocols*, advisor Stéphanie Delaune (with co-advisor Véronique Cortier);

• Daniel Pasaila, *Algorithms for Deciding Symbolic Equivalence*, advisors Stéphanie Delaune and Steve Kremer;

8. Partnerships and Cooperations

8.1. Regional Initiatives

The goal of Ligéro 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.

8.2. National Initiatives

- Cooperation with J.-C. Régin from Univ. Nice on efficient filtering algorithms (3 papers in 2011).
- Cooperation with A. Miné from ENS Paris on abstract domains by M. Pelleau and C. Truchet (2 visits in Paris).

8.3. European Initiatives

- Cooperation with P. Van Hentenryck from Univ. Brown (USA) for the supervision of the PhD of M. Pelleau (1 visit in Nantes).
- Cooperation with P. Flener from Univ. Uppsala (Sweden) on automata, invited (3 visits in Uppsala, 1 visit in Nantes).
- Cooperation with H. Simonis from 4C (Ireland) on the constraint and model seekers (2 visits in Cork, 1 visit in Nantes, 2 papers in 2011).
- Cooperation with M. Carlsson from SICS (Sweden) on the global constraint catalog (negation of automata with and without counters) (1 visit in Uppsala, update of the global constraint catalog in September 2011).
7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Digiteo Paso

Participants: Assia Mahboubi, Benjamin Werner [Contact].

The PASO project (Preuves, Interprétation abstraite, and Optimisation cal properties of programs, arising in particular from the modeling of complex systems with critical security issues. It gathers computer scientists from CEA-LIST/MaESI, INRIA Saclay/Typical and LIX and specialists from Optimization or Control theory from LIX/MaESI, INRIA Saclay/MaXplus and CMAP, and Supelec/L2S. The goal of this exploratory project is to cross-fertilize these fields, by applying advanced algorithms or techniques inspired by global optimization, by the analysis and identification of dynamical systems, or by zero-sum game theory, in order to improve the precision or the scalability of current methods in proof and static analysis. These applications coming from computer science turn out to raise new challenges for the applied mathematicians. The project started in October 2008 and ended in November 2011.

7.1.2. Digiteo Coquelicot

Participant: Assia Mahboubi [Contact].

Coquelicot is a 3 years Digiteo project that started in September 2011. Sylvie Boldo (INRIA, project-team ProVal) is the principal investigator of this project. The Coquelicot project aims at creating a modern formalization of the real numbers in Coq, with a focus on practicality. This is sorely needed to ease the verification of numerical applications, especially those involving advanced mathematics.

7.2. National Initiatives

7.2.1. ANR DeCert

Participants: Germain Faure, Chantal Keller, Assia Mahboubi [Contact].

This project is funded by the call Domaines Emergents 2008, a program of the Agence Nationale de la Recherche. It started in January 2009 and will end in December 2012. 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.

7.2.2. ANR PSI

Participants: Germain Faure, Assia Mahboubi [Contact], Revantha Ramanayake.

This project is is funded by the call Jeunes Chercheurs Jeunes Chercheuses 2009, a program of the Agence Nationale de la Recherche. It started in September 2009 and will end in September 2013. The PSI project aims at investigating how to take into account the specificities of a given theory when designing proof search methods, both in the theory of proof search and in the design of automated tools.

7.2.3. ANR Paral-ITP

Participants: Bruno Barras [Local coordinator for Inria Saclay – Île - de - France], Germain Faure, Assia Mahboubi, Enrico Tassi.
This project is funded by the call Ingénierie Numérique et Sécurité 2011, a program of the Agence Nationale de la Recherche. The Paral-ITP project intends to overcome the sequential model for Coq, to make the resources of multi-core hardware available for even larger proof developments. Beyond traditional processing of proof scripts as sequence of proof commands, there is a large space of possibilities and challenges for pervasive parallelism. Coq shall be connected to a uniform document model that integrates parallel and asynchronous evaluation processes with notions of history and change management, over the rich structure of formal content. This can then serve as a basis for an editor document model in direct user interaction, and background library management with continuous proof checking, in the style of modern IDEs like Eclipse or Netbeans. Ultimately, the general document model and front-end technology will accommodate end-users and builders of add-on tools. One typical instance is the add-on that imports proofs constructed by automated deduction systems (SAT and SMT solvers).

7.3. European Initiatives

7.3.1. FP7 Projet

7.3.1.1. FORMATH

Title: FORMATH
Type: COOPERATION (ICT)
Defi: FET Open
Instrument: Specific Targeted Research Project (STREP)
Duration: March 2010 - February 2013
Coordinator: Univ Gothenburg (Sweden)
Others partners: University of Gothenburg, Radboud University Nijmegen, Universidad de la Rioja, INRIA.
See also: FORMATH
Abstract: This project proposes to develop libraries of formalized mathematics concerning algebra, linear algebra, real number computation, and algebraic topology.

7.4. International Initiatives

7.4.1. Visits of International Scientists

7.4.1.1. Internship

Gilles Dowek has been the advisor of Jianhua Gao (University of Tsinghua, Beijing, China), who spent a year in Paris as part of its Doctoral degree.
VERIDIS Team

8. Partnerships and Cooperations

8.1. European Initiatives

8.1.1. Cooperation with NUI Maynooth, Ireland

We are involved in a bilateral research project with the National University of Ireland at Maynooth, funded by the Ulysses program between France and Ireland. The project addresses the question of formally verifying safety critical properties of software control systems, guaranteeing their reliability and safety. In particular, we address the following questions: What is the best methodology for generating a formal system requirements document (written in Event-B) for an already existing tram control system? What is the relationship between Event-B and Programmable Logic? How effectively can we support the formal translation of a system specification written in Event-B to its implementation written in programmable logic? Can we demonstrate that this formal transformation preserves the safety critical properties as specified for an existing tram control system? A combination of reverse engineering and refinement techniques are used to prove the safety critical properties of a tram control system, generating a suite of proof based patterns that may be used in the verification of safety critical properties of similar systems. Case studies involving subsystems of the tram control system will be used to develop Master level courses, ensuring technology transfer between industry and the classroom, and vice versa. Visits of Dominique Méry in February, August and December led to a series of lectures in the master program and in a Summer School organised by NUI Maynooth; Dominique Méry is completing models for ensuring the quality of produced codes. During a reciprocal visit of Rosemary Monahan of NUI Maynooth in October, she gave a tutorial on the verification of C# programs using Spec# and Boogie 2.

8.2. International Initiatives

8.2.1. INRIA International Partners

8.2.1.1. Cooperation with Universidade Federal do Rio Grande de Norte, Brazil

VeriDis has a close working relationship with a team at Universidade Federal do Rio Grande de Norte (UFRN), Brazil, and more particularly with Prof. Anamaria Martins Moreira and Prof. David Déharbe. Two long exchanges took place in 2011. Bruno Woltzenlogel Paleo visited UFRN for one month in March, and David Déharbe visited VeriDis from June 20 to July 20 as an INRIA invited researcher. The project is centered around the development and applications of the veriT solver (section 5.1), of which David Déharbe and Pascal Fontaine are the main developers. Diego Caminha was previously a student at UFRN and prepared his PhD thesis with the VeriDis team. Our cooperation is also supported by the INRIA-CNPq project SMT-SAvsS from 2010 throughout 2012.

8.2.1.2. Cooperation with Tiaret University

Mostapha Belardi (Université Ibn Khaldoun de Tiaret), Camel Tanougast (Univ. Paul Verlaine, Metz), Dominique Méry and Stephan Merz have started a joint project entitled CIPRONoC : Conception Incrémentale Prouvée pour pRototypage rapide de NoC Tolérant aux Fautes à base de technologie FPGA. The project is sponsored by the STIC Algérie program.

8.2.2. Visits of International Scientists

8.2.2.1. INRIA Internship program

Hernán Ponce de Leon (from April 2011 until August 2011)

Subject: Formally Verified Automata Construction for Real Linear Equations
Institution: Universidad Nacional de Rosario (Argentina)
8.2.2.2. Invited scientists

David Déharbe from Universidade Federal do Rio Grande de Norte, Brazil, visited VeriDis from June 20 to July 20 as an INRIA invited researcher. The work resulted in several improvements of the veriT solver and contributed to its integration within the toolsets for the B and TLA\(^+\) methods.