RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2013

Section Partnerships and Cooperations

Edition: 2014-03-20

ARIC Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR HPAC Project

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

"High-performance Algebraic Computing" (HPAC) is a four year ANR project that started in January 2012. The Web page of the project is http://hpac.gforge.inria.fr/. HPAC is headed by Jean-Guillaume Dumas (CASYS team, LJK laboratory, Grenoble); it involves AriC as well as the Inria project-team MOAIS (LIG, Grenoble), the Inria project-team PolSys (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-based cryptography and algebraic cryptanalysis. HPAC conducts 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, their integration into state-of-the-art software, and innovative high performance solutions for cryptology challenges.

8.1.2. ANR TaMaDi Project

Participants: Nicolas Brisebarre, Florent de Dinechin, Guillaume Hanrot, Vincent Lefèvre, Jean-Michel Muller, Damien Stehlé, Serge Torres.

The TaMaDi project (Table Maker's Dilemma, 2010-2013) was funded by the ANR and headed by Jean-Michel Muller. It started in October 2010 and ended in October 2013. 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 was 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-requirement 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.

The various documents on the project can be found at http://tamadiwiki.ens-lyon.fr/tamadiwiki/index.php/Main_Page.

8.1.3. PEPS Quarenum

Participants: Nicolas Louvet, Nathalie Revol.

"Quarenum" is an abbreviation for *Qualité et Reproductibilité Numériques dans le Calcul Scientifique Haute Performance*. This project focuses on the numerical quality of scientific software, more precisely of high-performance numerical codes. Numerical validation is one aspect of the project, the second one regards numerical reproducibility.

8.2. European Initiatives

8.2.1. FP7 Projects

Damien Stehlé was awarded in 2013 a "starting" ERC grant for his project "Euclidean lattices: algorithms and cryptography" (LattAC).

8.3. International Initiatives

8.3.1. Inria Associate Teams

QOLAPS (Quantifier elimination, Optimization, Linear Algebra and Polynomial Systems) is an Associate Team between the Symbolic Computation Group at North Carolina State University (USA), the PolSys team at LIP6, Paris 6, and the AriC team. Participants: Clément Pernet, Nathalie Revol, Gilles Villard.

8.3.2. Inria International Partners

8.3.2.1. Declared Inria International Partners

We contributed to the creation in 2008 of the IEEE 1788 working group on the standardization of interval arithmetic http://grouper.ieee.org/groups/1788/. and N. Revol chairs this group since its creation. More than 140 persons from over 20 countries take part in the discussions, around 2500 public messages were exchanged in 2013. The deadline granted by IEEE is December 2014. In 2013 we managed to elaborate a close-to-final draft of the standard text. This last year will be devoted to the final ballot from the working group and to a sponsor ballot, by experts designated by IEEE.

The annual in-person meeting, chaired by N. Revol, took place at the end of the IFSA-NAFIPS 2013 conference in Edmonton, Canada, the 25th of June.

V. Lefèvre participated in various discussions, either in the mailing-list or in small subgroups (he sent around 390 email messages in 2013).

8.3.2.2. Informal International Partners

Our international academic collaborators are from Courant Institute of Mathematical Sciences (USA), Hamburg University of Technology (Germany), Imperial College (UK), Macquarie University (Australia), Mc Gill University (Canada), Monash University (Australia), Nanyang Technological University (Singapore), North Carolina State University (USA), Technical University of Cluj-Napoca (Romania), University of California, Los Angeles (USA), University of Delaware (USA), University of Southern Denmark (Denmark), University of Western Ontario (Canada), University of Waterloo (Canada), Uppsala University (Sweden).

We also collaborate with Intel (Portland, USA).

8.3.3. Participation In other International Programs

CANTAL (Cryptography, Algorithmic Number Theory and Lattices) is a CNRS Associate Team between the cryptography group of Macquarie University (Australia), the cryptography group of Monash University (Australia) and the AriC team. Participants: Nicolas Brisebarre, Guillaume Hanrot, Fabien Laguillaumie, Adeline Langlois, Damien Stehlé.

Damien Stehlé is a Partner Investigator in the Australian Research Council Discovery Grant on Cryptography and Algorithmic Number Theory, headed by Christophe Doche (Macquarie U.), Igor Shparlinski (U. of New South Wales), and Ron Steinfeld (U. of Monash), and in a Singaporean Ministry of Education grant of Code-based and Lattice-based cryptography, headed by San Ling (Nanyang Technological U.) and Huaxiong Wang (Nanyang Technological U.).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Xiao-Wen Chang (McGill U., Canada) visited the team from mid-April to mid-June 2013, under the invited professor scheme from ENS de Lyon.

Warwick Tucker (Uppsala U., Sweden) visited the team from mid-February to the end of March 2013, both under the invited professor scheme from ENS de Lyon and thanks to a funding provided by the LIP laboratory.

Peter Kornerup (U. of Southern Denmark) visited the team the last two weeks of September 2013.

8.4.1.1. Internships

Saruchi (IIT Delhi) did a 3-month Master degree internship under the supervision of Damien Stehlé, from April to June 2013.

8.4.2. Visits to International Teams

Nicolas Brunie was invited for 6 months by Intel (Portland, USA) to work on the implementation of elementary functions.

CARAMEL Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Function field sieve: implementation and hardware acceleration

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

The team has obtained for the years 2012 and 2013 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.

While the more FPGA-related aspects of this project were put on hold in 2013, the GPU option was explored further. To this end, eight NVIDIA GeForce GTX 680 graphics cards were bought and installed in four nodes connected by an InfiniBand. Hamza Jeljeli was able to extend his GPU implementation of sparse linear algebra routines so as to take multi-GPU and multi-node computations into account. This setup was for instance used to break the discrete-logarithm record over an 809-bit binary field [15].

8.2. National Initiatives

The team participates in the “Calcul formel, arithmétique, protection de l’information” research pole of the GDR-IM (CNRS Research Groupon Mathematical Computer Science). The team is a member of the “Arithmétique”, “Calcul formel” and “Codage et Cryptographie” working groups.

8.2.1. ANR CATREL (Cribles: Améliorations Théoriques et Résolution Effective du Logarithme discret)

Participants: Razvan Barbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé [contact], Marion Videau, Paul Zimmermann.

The CATREL proposal has been accepted in ANR “programme Blanc” in 2012. This project involves CARAMEL as a leading team, in cooperation with two other partners which are Inria project-team GRACE (Inria Saclay, LIX, École polytechnique), and the Arith team of the LIRMM Laboratory (Montpellier). The project targets the algorithms for solving the discrete logarithm problem in finite fields, using the Number Field Sieve and the Function Field Sieve algorithms. Actual work on the CATREL project started in January 2013. Three meetings have taken place already: in Nancy on Dec. 14th, 2012 (kick-off), in Palaiseau on June 19, 2013, and in Monpellier on November 12-13, 2013.

8.2.2. GDR-IM supported travel for PhD students

Hamza Jeljeli collaborated with Bastien Vialla from LIRMM, Montpellier to integrate RNS-based code in $\texttt{mp}\mathbb{F}_q$ and CADO-NFS. This collaboration was funded by the GDR-IM program “visite de doctorants".

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Shi Bai from the univeristy of Auckland, NZ, visited us in June 2013.

Thorsten Kleinjung, from the EPFL, visited us in October 2013.

CASCADE Project-Team

5. Partnerships and Cooperations

5.1. ANR Projects with Industrials

- **SAPHIR-II** *(Sécurité et Analyse des Primitives de Hachage Innovantes et Récentes)*
  Security and analysis of innovating and recent hashing primitives.
  Participants: Patrick Derbez, Jérémy Jean.

  From April 2009 to March 2013.
  Partners: France Telecom R&D, Gemalto, EADS, SAGEM, DCSSI, Cryptolog, Inria/Secret, UVSQ, XLIM, CryptoExperts.
- **BEST: Broadcast Encryption for Secure Telecommunications.**
  Participants: David Pointcheval, Elizabeth Quaglia, Mario Strefler, Damien Vergnaud, Aurore Guillevic, Sorina Ionica.

  From December 2009 to December 2013.
  Partners: Thales, Nagra, CryptoExperts, Univ. Paris 8.
  This project aims at studying broadcast encryption and traitor tracing, with applications to the Pay-TV and geolocalisation services.
- **PRINCE: Proven Resilience against Information leakage in Cryptographic Engineering.**
  Participants: Fabrice Ben Hamouda, Sonia Belaid, Alain Passelègue, Michel Ferreira Abdalla, David Pointcheval.

  From December 2010 to December 2014.
  Partners: UVSQ, Oberthur Technologies, Ingenico, Gemalto, Tranef.
  We aim to undertake research in the field of leakage-resilient cryptography with a practical point of view. Our goal is to design efficient leakage-resilient cryptographic algorithms and invent new countermeasures for non-leakage-resilient cryptographic standards. These outcomes shall realize a provable level of security against side-channel attacks and come with a formally verified implementation. For this every practical aspect of the secure implementation of cryptographic schemes must be taken into account, ranging from the high-level security protocols to the cryptographic algorithms and from these algorithms to their implementation on specific devices which hardware design may feature different leakage models.
- **SIMPATIC: SIM and PAiring Theory for Information and Communications security.**
  Participants: Damien Vergnaud, Olivier Sanders, David Pointcheval.

  From February 2013 to August 2016.
  Partners: Orange Labs,INVIA, Oberthur Technologies, STMicroelectronics, Université Bordeaux 1, Université de Caen Basse-Normandie, Université de Paris VIII
  We aim at providing the most possible efficient and secure hardware/software implementation of a bilinear pairing in a SIM card.

5.2. ANR Projects within Academics

- **ProSe: Security protocols : formal model, computational model, and implementations.**
  Participant: David Pointcheval.

  From December 2010 to November 2014.
  Partners: ENS Cachan-Inria/Secsi, LORIA-Inria/Cassis, Inria/Prosecco, Verimag.
  The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the symbolic level, in which messages are terms; the computational level, in which messages are bitstrings; the implementation level: the program itself.

- **ROMAnTIC: Randomness in Mathematical Cryptography.**
  Participants: Damien Vergnaud, David Pointcheval, Adrian Thillard, Sylvain Ruhault.

  From October 2012 to September 2016.
  Partners: ANSSI, Univ. Paris 7, Univ. Paris 8.
  The goal of this project is to get a better understanding of the interplay between randomness and cryptography and to study the security of various cryptographic protocols at different levels (information-theoretic and computational security, number-theoretic assumptions, design and provable security of new and existing constructions).
- **CLE: Cryptography from Learning with Errors.**
  Participant: Vadim Lyubashevsky.

  From October 2013 to September 2017.
  Partners: UVSQ, Univ. Paris 8, Inria/SECRET.
  The main objective of this project is to explore the potential practical implications of the Learning with Errors problem and its variants. The plan is to focus on the constructions of essential primitives whose use is prevalent in the real world. Toward the end of the project, the hope is to propose and standardize several public key and symmetric key schemes that have specific advantages over ones that are currently deployed.

5.3. European Initiatives

- **ECRYPT-II: Network of Excellence in Cryptology.**
  From August 2008 to July 2013.
  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.
- **SecFuNet: Security for Future Networks.**
  From July 2011 to April 2014.
  The goal of the SECFUNET project is to design and develop a coherent security architecture for virtual networks and cloud accesses.

5.4. International Research Visitors

- Mario Cornejo (Ms student) – Chile
- Nuttapong Attrapadung – The National Institute of Advanced Industrial Science and Technology, Japan
- Yu Long – Shanghai Jiao Tong University, China

CRYPT Team

5. Partnerships and Cooperations

5.1. National Initiatives

5.1.1. MOST's 973 Grant

Grant 2013CB834205

PIs Phong Nguyen and Xiaoyun Wang

Duration 2013-17

MOST is China's Ministry of Science and Technology.

5.1.2. NSFC Grant

Grant NSFC Key Project 61133013

PIs Phong Nguyen and Xiaoyun Wang

Duration 2013-16

NSFC is the National Natural Science Foundation of China.

5.2. European Initiatives

5.2.1. FP7 Projects

Phong Nguyen was leader of the Virtual Lab MAYA of FP7's ECRYPT-II Network of Excellence, which finished in 2013.

5.2.2. Collaborations with Major European Organizations

CWI: Ronald Cramer's crypto team (Netherlands). In December 2013, Cramer's crypto team officially became a partner of LIAMA's CRYPT international project: in particular, Marc Stevens expects to do joint work on the cryptanalysis of hash functions.

5.3. International Initiatives

5.3.1. Inria International Labs

- CRYPT is an international project from LIAMA in China, located at Tsinghua University in Beijing. It is a joint project between Inria, Tsinghua University and CAS Academy of Mathematics and System Sciences.
- Phong Nguyen is the new European director of LIAMA, since December 2013: previously, he was the scientific coordinator of LIAMA in 2013.

5.4. International Research Visitors

5.4.1. Visits of International Scientists

Shi Bai (Univ. of Auckland, New-Zealand)

Nicolas Gama (UVSQ and CNRS, France)

Ming-Deh Huang (Univ. Southern California, USA)

Gaëtan Leurent (UCL, Belgium)

Cheng Qi (Univ. Oklahoma, USA)

Marc Stevens (CWI, Netherlands)

Guangwu Xu (Univ. Wisconsin, USA)

GEOMETRICA Project-Team

8. Partnerships and Cooperations

8.1. Technological Development Actions

8.1.1. ADT PH

Participants: Jean-Daniel Boissonnat, Frédéric Chazal, David Cohen-Steiner, Sonali Digambar Patil, Marc Glisse, Steve Oudot, Clément Maria, Mariette Yvinec.

- Title: Persistent Homology

- Coordinator: Mariette Yvinec (GEOMETRICA)

- Duration: 1 year renewable once, starting date December 2012.
- Others Partners: Inria team ABS, Gipsa Lab (UMR 5216, Grenoble, http://www.gipsa-lab.inpg.fr/)

- Abstract: Geometric Inference is a rapidly emerging field that aims to analyse the structural, geometric and topological, properties of point cloud data in high dimensional spaces. The goal of the ADT PH is to make available, a robust and comprehensive set of algorithmic tools resulting from recent advances in Geometric Inference. The software will include:

tools to extract from the data sets, families of simplicial complexes,

data structures to handle those simplicial complexes,

algorithmic modules to compute the persistent homology of those complexes,

applications to clustering, segmentation and analysis of scalar fields such as the energy landscape of macromolecular systems.

8.1.2. ADT OrbiCGAL

Participants: Mikhail Bogdanov, Aymeric Pellé, Monique Teillaud.

- Title: OrbiCGAL

- Coordinator: Monique Teillaud (GEOMETRICA)

- Duration: 1 year renewable once, starting date September 2013.
- Abstract: OrbiCGAL is a software project supported by Inria as a Technological Development Action (ADT). It is motivated by applications ranging from infinitely small (nano-structures) to infinitely large (astronomy), through material engineering, physics of condensed matter, solid chemistry, etc

The project consists in developing or improving software packages to compute triangulations and meshes in several types of non-Euclidean spaces: sphere, 3D closed flat manifolds, hyperbolic plane.

8.2. Regional Initiatives

8.2.1. Digiteo project TOPERA

Participants: Frédéric Chazal, Marc Glisse, Anaïs Vergne.

TOPERA is a project that aims at developing methods from Topological Data Analysis to study covering properties and quality of cellular networks. It also involves L. Decreusefond and P. Martins from Telecom Paris.

- Starting date: December 2013

- Duration: 18 months

8.3. National Initiatives

8.3.1. ANR Présage

Participants: Olivier Devillers, Marc Glisse, Ross Hemsley, Monique Teillaud, Rémy Thomasse.

- Acronym: Presage.

- Type: ANR blanc.

- Title: *méthodes PRobabilistes pour l'Éfficacité des Structures et Algorithmes GÉométriques*.

- Coordinator: Xavier Goaoc.

- Duration: 31 december 2011 - 31 december 2015.

- Other partners: Inria VEGAS team, University of Rouen.

- Abstract: This project brings together computational and probabilistic geometers to tackle new probabilistic geometry problems arising from the design and analysis of geometric algorithms and data structures. We focus on properties of discrete structures induced by or underlying random continuous geometric objects. This raises questions such as:

- What does a random geometric structure (convex hulls, tessellations, visibility regions...) look like?
- How to analyze and optimize the behavior of classical geometric algorithms on *usual* inputs?
- How can we generate randomly *interesting* discrete geometric structures?

- Year publications: [16], [31], [51].

8.3.2. ANR GIGA

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

- Acronym : GIGA.

- Title : Geometric Inference and Geometric Approximation.

- Type: ANR blanc

- Coordinator: Frédéric Chazal (GEOMETRICA)

- Duration: 4 years starting October 2009.
- Others Partners: Inria team-project Titane, Inria team-project ABS, CNRS (Grenoble), Dassault Systèmes.

- Abstract: 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.

- See also: http://www-sop.inria.fr/geometrica/collaborations/giga/

8.3.3. ANR TOPDATA

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

- Acronym : TopData.

- Title : Topological Data Analysis: Statistical Methods and Inference.

- Type : ANR blanc

- Coordinator : Frédéric Chazal (GEOMETRICA)

- Duration : 4 years starting October 2013.
- Others Partners: Département de Mathématiques (Université Paris Sud), Institut de Mathḿatiques (Université de Bourgoogne), LPMA (Université Paris Diderot), LSTA (Université Pierre et Marie Curie)

- Abstract: TopData aims at designing new mathematical frameworks, models and algorithmic tools to infer and analyze the topological and geometric structure of data in different statistical settings. Its goal is to set up the mathematical and algorithmic foundations of Statistical Topological and Geometric Data Analysis and to provide robust and efficient tools to explore, infer and exploit the underlying geometric structure of various data.

Our conviction, at the root of this project, is that there is a real need to combine statistical and topological/geometric approaches in a common framework, in order to face the challenges raised by the inference and the study of topological and geometric properties of the wide variety of larger and larger available data. We are also convinced that these challenges need to be addressed both from the mathematical side and the algorithmic and application sides. Our project brings together in a unique way experts in Statistics, Geometric Inference and Computational Topology and Geometry. Our common objective is to design new theoretical frameworks and algorithmic tools and thus to contribute to the emergence of a new field at the crossroads of these domains. Beyond the purely scientific aspects we hope this project will help to give birth to an active interdisciplinary community. With these goals in mind we intend to promote, disseminate and make our tools available and useful for a broad audience, including people from other fields.

8.4. European Initiatives

8.4.1. FP7 Projects

8.4.1.1. CG-Learning

Type: COOPERATION

Defi: FET Open

Instrument: Specific Targeted Research Project

Objectif: FET-Open: Challenging Current Thinking

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)

Inria contact: Mariette Yvinec

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 algorithm 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.

8.5. International Initiatives

8.5.1. Inria Associate Teams

8.5.1.1. COMET

Title: Computational methods for the analysis of high-dimensional data

Inria principal investigator: Steve Y. Oudot

International Partner (Institution - Laboratory - Researcher):

Stanford University (United States) - Computer Science - Leonidas Guibas

Ohio State University (United States) - Computer Science and Engineering - 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.

8.6. International Research Visitors

Mirel Ben Chen (Technion - Israel Institute of Technology)

Benjamin Burton (University of Queensland)

Pedro Machado Manhães de Castro (Universidade Federal de Pernambuco)

Arijit Ghosh (Indian Statistical Institute)

Michael Hemmer (University of Technology Braunschweig)

Dmitriy Morozov (Berkeley)

Yusu Wang (Ohio State University)

Jian Sun (Tsinghua University - China)

Yuan Yao (Peiking University - China)

GRACE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- ISN-Privacy. From late 2012 through the year 2013, Daniel Augot was heavily involved in the preparation of the *Institut de la société du numérique* (Digital Society Institute) proposal within IDEX Paris-Saclay. Led by N. Boujemaa, this proposal aims to be a catalyst for interdisciplinary research (involving computer scientists and researchers from the humanities) on societal challenges inherent to eLife/life digitization. The proposal has initial funding from the IDEX, and will hopefully be self-funding within three years. Two kick-off projects were defined: joint human & machine interaction, and privacy and digital identity.

  Daniel Augot engaged in monthly brainstorming meetings with researchers from Inria Paris–Rocquencourt (project-team SMIS), Université Jean Monnet's ADIS and CERDI labs (Alain Rallet, Alexandra Bensamoun), and Télécom ParisTech (Claire Levallois-Barth). Topics under discussion include terms of service of various cloud storage providers, SMIS's *TrustedCell* secure token initiative for helding private and secure personnal data, privacy leaks, and measurements on smartphones.

  A seminar will be held in Summer 2014. Within IDEX Paris-Saclay, the PAIP (Pour une Approche Interdisciplinaire de la Privacy) project was proposed and accepted in September 2013, with a small budget (30 keuros) for all the partners of the privacy group.

8.2. National Initiatives

8.2.1. ANR

- CATREL (accepted June 2012, Kickoff December 14, 2012, Starting January 1st, 2013): "Cribles: Améliorations Théoriques et Résolution Effective du Logarithme" (Sieve Algorithms: Theoretical Advances and Effective Resolution of the Discrete Logarithm Problem). This project aims to make effective "attacks" on reduced-size instances of the discrete logarithm problem (DLP). It is a key ingredient for the assessment of the security of cryptosystems relying on the hardness of the DLP in finite fields, and for deciding on relevant key sizes.

8.2.2. DGA

- DIFMAT: this two-year project aims to find matrices with good diffusion over small finite fields. These matrices are used in block ciphers and hash functions; coding theory helps to build and analyse them. Guillaume Quintin was hired as a postdoctoral researcher using this funding.
- Daniel Augot is co-advising Gwezheneg Robert with Pierre Loidreau (DGA, Rennes University).

8.2.3. PEPS ICQ (Projet Exploratoire de Premier Soutien - Information et Communication Quantique)

- ToCQ is a one-year project exploring the connections between algebraic topology, combinatorics, and Low Density Parity Check Quantum Codes. Alain Couvreur and Nicolas Delfosse are members of this project. The other partners are Inria Paris–Rocquencourt, Université Bordeaux I and Aix–Marseille Université.

8.3. European Initiatives

8.3.1. Collaborations in European Programs, except FP7

Program: COST

Project acronym: COST 4175/11

Project title: Random Network Coding and Designs over GF(q) http://www.network-coding.eu/index.html

Duration: 04/2012 - 04/2016

Coordinator: Marcus Greferath

Other partners: Camilla Hollanti, Aalto University, Finland Simon R. Blackburn, Royal Holloway, University of London, UK Tuvi Etzion, Technion, Israel Ángeles Vázquez-Castro, Autonomous University of Barcelona, Spain Joachim Rosenthal, University of Zurich, Switzerland (Chairs of the five working groups).

Abstract: Random network coding emerged through an award-winning paper by R. Koetter and F. Kschischang in 2008 and has since then opened a major research area in communication technology with widespread applications for communication networks like the internet, wireless communication systems, and cloud computing. It allows transmitting information through a network by disregarding any of its topological features. Worldwide, there exists a larger number of workgroups focusing on this topic, which includes several groups located in Europe. This COST Action will set up a European research network and establish network coding as a European core area in communication technology. Its aim is to bring together experts from pure and applied mathematics, computer science, and electrical engineering, who are working in the areas of discrete mathematics, coding theory, information theory, and related fields.

8.4. International Initiatives

8.4.1. Inria International Partners

8.4.1.1. Informal International Partners

- Martin Bossert, Institute of Communications Engineering, Ulm Universität.
- Steven Galbraith, Department of Mathematics, University of Auckland.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Internships

- Charlotte Scribot is spending the period September 2013 - February 2014 as an intern with GRACE as part of her professional masters program (Paris 7). She is working with Benjamin Smith and François Morain on parameter selection for efficient elliptic curve cryptosystems.

LFANT Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANRPeace – Parameter spaces for Efficient Arithmetic and Curve security Evaluation

Participants: Bill Allombert, Karim Belabas, Jean-Marc Couveignes, Andreas Enge, Nicolas Mascot, Enea Milio, Aurel Page, Damien Robert.

http://chic2.gforge.inria.fr/

The PEACE project is joint between the research teams of Institut de Recherche en Mathématiques de Rennes (IRMAR), LFANT and Institut Mathématiques de Luminy (IML).

The project aims at constituting a comprehensive and coherent approach towards a better understanding of theoretical and algorithmic aspects of the discrete logarithm problem on algebraic curves of small genus. On the theoretical side, this includes an effective description of moduli spaces of curves and of abelian varieties, the maps that link these spaces and the objects they classify. The effective manipulation of moduli objects will allow us to develop a better understanding of the algorithmic difficulty of the discrete logarithm problem on curves, which may have dramatic consequences on the security and efficiency of already deployed cryptographic devices.

One of the anticipated outcomes of this proposal is a new set of general criteria for selecting and validating cryptographically secure curves (or families of curves) suitable for use in cryptography. Instead of publishing fixed curves, as is done in most standards, we aim at proposing generating rationales along with explicit theoretical and algorithmic criteria for their validation.

Meetings:

- Paris: 11/04–12/04, talks and mini-courses;
- Rennes: 02/12–03/12, talks.

8.1.2. ANRSimpatic – SIM and PAiring Theory for Information and Communications security

Participant: Damien Robert.

The SIMPATIC project is an industrial research project, formed by academic research teams and industrial partners: Orange Labs, École Normale Supérieure, INVIA, Oberthur Technologies, ST-Ericsson France, Université de Bordeaux 1, Université de Caen Basse-Normandie, Université de Paris 8.

The aim of the SIMPATIC project is to provide the most efficient and secure hardware/software implementation of a bilinear pairing in a SIM card. This implementation will then be used to improve and develop new cryptographic algorithms and protocols in the context of mobile phones and SIM cards. The project will more precisely focus on e-ticketing and e-cash, on cloud storage and on the security of contactless and of remote payment systems.

As a participant, D. Robert will aim to bridge the gap between the theoretical results described in the pairing module and the practical realisation of pairing-based SIM cards in an industrial setting.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. ANTICS

Title: Algorithmic Number Theory in Cryptology

Type: IDEAS

Instrument: ERC Starting Grant

Duration: January 2012 - December 2016

Coordinator: Inria (France)

Abstract: Data security and privacy protection are major challenges in the digital world. Cryptology contributes to solutions, and one of the goals of ANTICS is to develop the next generation public key cryptosystem, based on algebraic curves and abelian varieties. Challenges to be tackled are the complexity of computations, certification of the computed results and parallelisation, addressed by introducing more informatics into algorithmic number theory.

8.3. International Initiatives

8.3.1. Inria International Labs

The *MACISA* project-team (Mathematics Applied to Cryptology and Information Security in Africa) is one of the new teams of LIRIMA. Researchers from Inria and the universities of Bamenda, Bordeaux, Dakar, Franceville, Maroua, Ngaoundéré, Rennes, Yaoundé cooperate in this team.

The project is concerned with public key cryptology and more specifically the role played by algebraic maps in this context. The team focus on two themes:

- Theme 1 : Rings, primality, factoring and discrete logarithms;
- Theme 2 : Elliptic and hyperelliptic curve cryptography.

The project is managed by a team of five permanent researchers: G. Nkiet, coordinator of the project, J.-M. Couveignes, vice coordinator, T. Ezome and D. Robert, responsible for each of the two scientific working areas, A. Enge, head of the LFANT project team. The managing team organises the cooperation, schedules meetings, prepares reports, controls expenses, reports to the LIRIMA managing team and administrative staff.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Tony Ezome Mintsa, University of Franceville, Gabon, 02/2013 and 11–12/2013
- Loïc Grenie, University of Bergamo, 11–12/2013
- Matthias Waack, University of Leipzig, Germany, 10–11/2013
- Eduardo Friedman, University of Chile, 01–02/2013
- Francisco Diaz y Diaz, emeritus, 01–02/2013
- Bernadette Perrin-Riou, Université d'Orsay, 03/2013

8.4.1.1. Internships

- Fritz Hiesmayr, ÉNS Lyon, 06–07/2013
- Gregor Seiler, Technische Universität Berlin, Germany, 10/2013–03/2014

8.4.2. Visits to International Teams

D. Robert visited the cryptology team at Microsoft Research from August 06 to August 14.

POLSYS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR Jeunes Chercheurs CAC Computer Algebra and Cryptography (2009-2013).** The contract CAC "Computer Algebra and Cryptography started in October 2009 for a period of 4 years. This project investigates 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 (Participants: L. Perret [contact], J.-C. Faugère, G. Renault).
- **ANR Grant (international program) EXACTA (2010-2013): Exact/Certified Algorithms with Algebraic Systems.**
  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 (2010-2013) 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.
- **ANR Grant HPAC: High Performance Algebraic Computing (2012-2016).** 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 project 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 (J.-C. Faugère [contact], L. Perret, G. Renault, M. Safey El Din).
- **ANR Grant GeoLMI: Geometry of Linear Matrix Inequalities (2011-2015).** he GeoLMI project 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 (Participants: J.-C. Faugère, M. Safey El Din [contact], E. Tsigaridas).

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. A3

Type: PEOPLE

Defi:

Instrument: Career Integration Grant

Objectif: NC

Duration: May 2013 - April 2017

Coordinator: Jean-Charles Faugère

Partner: Institut National de Recherche en Informatique et en Automatique (Inria), France

Inria contact: Elias Tsigaridas

Abstract: The project Algebraic Algorithms and Applications (A3) is an interdisciplinary and multidisciplinary project, with strong international synergy. It consists of four work packages The first (Algebraic Algorithms) focuses on fundamental problems of computational (real) algebraic geometry: effective zero bounds, that is estimations for the minimum distance of the roots of a polynomial system from zero, algorithms for solving polynomials and polynomial systems, derivation of non-asymptotic bounds for basic algorithms of real algebraic geometry and application of polynomial system solving techniques in optimization. We propose a novel approach that exploits structure and symmetry, combinatorial properties of high dimensional polytopes and tools from mathematical physics. Despite the great potential of the modern tools from algebraic algorithms, their use requires a combined effort to transfer this technology to specific problems. In the second package (Stochastic Games) we aim to derive optimal algorithms for computing the values of stochastic games, using techniques from real algebraic geometry, and to introduce a whole new arsenal of algebraic tools to computational game theory. The third work package (Non-linear Computational Geometry), we focus on exact computations with implicitly defined plane and space curves. These are challenging problems that commonly arise in geometric modeling and computer aided design, but they also have applications in polynomial optimization. The final work package (Efficient Implementations) describes our plans for complete, robust and efficient implementations of algebraic algorithms.

8.3. International Initiatives

8.3.1. Inria Associate Teams

The POLSYS Team and ARIC at ENS Lyon are part of the QOLAPS (Quantifier Elimination, Optimization, Linear Algebra and Polynomial Systems) Associate Team with the Symbolic Computation Group at North Carolina State University. Activities of this associate team are described at the following url:

http://www-polsys.lip6.fr/QOLAPS/index.html

8.3.1.1. Informal International Partners

- Crypto team at Royal Holloway, University of London, UK.
- Prof. Victor Y. Pan, Department of Mathematics and Computer Science Lehman College, City University of New York, USA.

8.3.2. Inria International Labs

The POLSYS Team is involved in the ECCA (Exact Certified Computation with Algebraic Systems) at LIAMA in China.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Prof. K. Yokoyama (Japan) visited the POLSYS team during January 2013.

Prof. C. Yap (Courant Institute, New-York, USA) was an Inria invited professor and visited the POLSYS team during June and July 2013.

Prof. B. Sturmfels (Univ. Berkeley, USA) visited the POLSYS team during July 2013.

Prof. I. Bomze (Univ. of Vienna, Austria) visited the POLSYS team during October 2013.

Prof. J. Guttierez (Univ. Santander, Spain) visited the POLSYS team during November 2013.

Prof. J. Hauenstein (North Carolina State Univ., USA) visited the POLSYS team during November 2013.

J. Rohal (North Carolina State Univ., USA) visited the POLSYS team during November 2013.

8.4.1.1. Internships

- T. Verron (Internship M2 and ENS Paris): Computation of Gröbner bases for quasi-homogeneous systems.

SECRET Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- **ANR SAPHIR-2** ($03/09 \rightarrow 03/13$)
  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 BLOC** ($10/11 \rightarrow 09/15$)
  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** ($12/11 \rightarrow 12/15$)
  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.
- **ANR CLE** ($10/13 \rightarrow 10/17$)
  Cryptography from learning with errors
  ANR program: Jeunes Chercheurs, SIMI2
  Coordinator: Vadim Lyubashevsky (Inria, EPI Cascade)
  The aim of this project is to combine algorithmic and algebraic techniques coming from asymmetric and symmetric cryptology in order to improve some attacks and to design some symmetric primitives which have a good resistance to side-channel attacks.

7.1.2. Others

- **French Ministry of Defense** ($01/11 \rightarrow 12/13$)
  Funding for the supervision of Marion Bellard's PhD.
  30 kEuros.
- **French Ministry of Defense** ($10/12 \rightarrow 09/15$)
  Funding for the supervision of Audrey Tixier's PhD.
  30 kEuros.

- **DGA-MI** $(12/11 \rightarrow 02/13)$
  Analysis of binary streams.
  20 kEuros.
- **PEPS IQC 2013** $(04/13 \rightarrow 03/14)$
  Topology and quantum codes
  coordinated by G. Zémor, Institut de Mathématiques de Bordeaux.
  http://www.cnrs.fr/mi/spip.php?article301
- **PEPS IQC 2013** $(04/13 \rightarrow 03/14)$
  Quantum Cryptography and distributed computing
  coordinated by Frédéric Grosshans, Laboratoire Aimé Cotton.
  http://www.cnrs.fr/mi/spip.php?article301

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7

Program: COST
Project acronym: ICT COST Action IC1306
Project title: Cryptography for Secure Digital Interaction
Duration: January 2014 - November 2017
Coordinator: Claudio Orlandi, Aarhus University, Denmark
Other partners: see http://www.cost.eu/domains_actions/ict/Actions/IC1306
Abstract: The aim of this COST action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments.

7.3. International Initiatives

7.3.1. Inria International Partners

7.3.1.1. Informal International Partners

- 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:
  Lightweight symmetric crytography and code-based cryptography
- Indian Statistical Institute, Kolkata, India:
  Symmetric cryptography

7.4. International Research Visitors

7.4.1. Visits of International Scientists

- Grigory Kabatianskiy, Institute for Problems of Information Transmission, Moscow, Russia, November 23-30
- Paulo Barreto, University of Sao Paulo, Brazil, November 22-30
- Dimitrios Simos, SBA Research, Vienna, Austria, June 30-July 6
- Bimal Roy, Indian Statistical Institute, Kolkata, India, June 15-23

7.4.2. Visits to International Teams

- University of Sherbrooke, Canada, July 14-21 (J.P. Tillich)
- Newton Institute for Mathematical Sciences, Cambridge, United Kingdom, November 6-8, invitation to the *Mathematical Challenges in Quantum Information* Program, (A. Leverrier)
- CWI, Amsterdam, Netherlands, November 26-27, collaboration with Christian Schaffner, (A. Leverrier)
- FHNW, Windisch, Switzerland, May 27-31, visiting Willi Meier (M. Naya-Plasencia)

Specfun Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- Project *Coquelicot*, funded jointly by the Fondation de Coopération Scientifique "Campus Paris-Saclay" and Digiteo.
  Goal: Create a new Coq library for real numbers of mathematics.
  Leader: S. Boldo (INRIA Saclay, Toccata). Participant: A. Mahboubi.
  Website: http://coquelicot.saclay.inria.fr/.

8.2. National Initiatives

8.2.1. ANR

- *Psi* (ANR-09-JCJC-0006).
  Duration: 2009-2013. Goal: Proof-Search control in Interaction with domain-specific methods. Coordinator: Stéphane Lengrand (CNRS, LIX).
  Participant: A. Mahboubi.
  Website: http://www.lix.polytechnique.fr/~lengrand/PSI/.
- *ParalITP* (ANR-11-INSE-001).
  Goal: Improve the performances and the ergonomics of interactive provers by taking advantage of modern, parallel hardware.
  Leader: B. Wolff (University of Orsay, Paris XI). Participants: A. Mahboubi, E. Tassi.

8.2.2. Other

- PEPS Grant *Holonomix*.
  Goal: Asymptotics of special functions arising in physics, computer science, and number theory.
  Leader: Cyril Banderier (CNRS, LIPN). Participant: A. Bostan, F. Chyzak.
  Website: http://www.cnrs.fr/ins2i/spip.php?article143.

8.3. European Initiatives

8.3.1. FP7 Projects

- *Formalisation of Mathematics* (*ForMath*, EU FP7 STREP FET-open project).
  Partners: University of Gothenburg (Sweden); Radboud University Nijmegen (The Netherlands); Inria (France); Universidad de La Rioja (Spain).
  Goal: Investigate how recent advances in the methodology and design of computer-checked libraries of formalized mathematics apply to so-far-unexplored areas of mathematics, like real analysis or certified efficient computations.
  Leader: Th. Coquand (University of Gothenburg, Sweden). Participant: A. Mahboubi (work package leader for WP1).
  Website: http://wiki.portal.chalmers.se/cse/pmwiki.php/ForMath/ForMath.

VEGAS Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. ANR PRESAGE

The white ANR grant PRESAGE brings together computational geometers (from the VEGAS and GEOMETRICA projects of Inria) and probabilistic geometers (from Universities of Rouen, Orléans and Poitiers) to tackle new probabilistic geometry problems arising from the design and analysis of geometric algorithms and data structures. We focus on properties of discrete structures induced by or underlying random continuous geometric objects.

This is a four year project, with a total budget of 400kE, that started on Dec. 31st, 2011. It is coordinated by Xavier Goaoc (VEGAS).

6.1.2. ANR SingCAST

The objective of the young-researcher ANR grant SingCAST is to intertwine further symbolic/numeric approaches to compute efficiently solution sets of polynomial systems with topological and geometrical guarantees in singular cases. We focus on two applications: the visualization of algebraic curves and surfaces and the mechanical design of robots.

After identifying classes of problems with restricted types of singularities, we plan to develop dedicated symbolic-numerical methods that take advantage of the structure of the associated polynomial systems that cannot be handled by purely symbolical or numerical methods. Thus we plan to extend the class of manipulators that can be analyzed, and the class of algebraic curves and surfaces that can be visualized with certification.

This is a 3.5 years project, with a total budget of 100kE, that will start on March 1st 2014, coordinated by Guillaume Moroz.

6.2. International Research Visitors

Nuno Gonçalves, University of Coimbra (Portugal), visited the VEGAS project for 1 week in January.

William J. Lenhart, Williams College (USA), visited the VEGAS project for 2 weeks in May..

6.2.1. Internships

Ioannis Psarros

Subject: Common tangents to ellipsoids in $\mathbb{R}^3$.

Date: from Apr. 2013 until July 2013.

Institution: University of Athens, Greece.

Oswald Hounkounou

Subject: Study with computer algebra system of a conjecture relating the width of a convex polygon with the width of its inscribed triangles.

Date: from Apr. 2013 until Aug. 2013.

Institution: Telecom Nancy de l'université de Lorraine.

Judit Recknagel

Subject: Topology of planar singular curves resultant of two trivariate polynomials.

Date: from Apr. 2013 until Aug. 2013

Institution: Halle-Wittenberg university, Germany.

ALF Project-Team

8. Partnerships and Cooperations

8.1. International Initiatives

8.1.1. Participation In International Programs

8.1.1.1. Imhotep (Egypt)

Program: PHC

Title: Code obfuscation through JIT compilation

Inria principal investigator: Erven ROHOU

International Partner (Institution - Laboratory - Researcher):

Egypt-Japan University for Science and Technology (Egypt)

Duration: Jan 2013 - Dec 2013

This project leverages JIT compilation to make software tamper-proof. The idea is to constantly generate different versions of an application, even while it runs, to make reverse engineering much more complex. A strong random number generator guarantees that generated code is not reproducible – though the semantics is the same. In the course of the project, we also studied new forms of On-Stack-Replacement that let us recompile code even from the middle of a function. Finally, we studied how threads can be exploited to generate new forms of obfuscation, leveraging the fact that parallelism is error-prone, and difficult to debug and reverse-engineer.

8.1.2. Informal International Partners

The ALF team has informal collaborations with several international teams: Carnegie Mellon (Pr Mutlu), Georgia Tech (Pr Qureshi), University of Wisconsin (Pr Wood), University of Cyprus (Pr Sazeides), University of Ghent (Dr Eyerman), XLNS Research (Dr Arnold), UFMG Brazil (Pr Pereira), Barcelona Supercomputing center (Pr Cazorla and Pr Abella),

8.2. National Initiatives

8.2.1. Inria Project Lab: Multicore

Participants: Erven Rohou, Alain Ketterlin, Nabil Hallou.

The Inria Project Lab (formerly *Action d'Envergure*) started in 2013. It is entitled "Large scale multicore virtualization for performance scaling and portability". Partner project-teams include: ALF, ALGORILLE, CAMUS, REGAL, RUNTIME, as well as DALI. This project aims to build collaborative virtualization mechanisms that achieve essential tasks related to parallel execution and data management. We want to unify the analysis and transformation processes of programs and accompanying data into one unique virtual machine.

8.2.2. ADT IPBS 2013-2015

Participants: Sylvain Collange, Erven Rohou, André Seznec, Thibault Person.

As multi-core CPUs and parallel accelerators become pervasive, all execution platforms are now parallel. Research on architecture, compilers and systems now focuses on parallel platforms. New contributions need to be validated against parallel applications that are expected to be representative of current or future workloads. The research community relies today on a few benchmarks sets (SPLASH, PARSEC, ..) Existing parallel benchmarks are scarce, and some of them have issues such as aging workloads or non-representative input sets. The IPBS initiative aims at leveraging the diversity of parallel applications developed within Inria to provide a set of benchmarks, named the Inria Parallel Benchmark Suite, to the research community.

8.2.3. ADT Padrone 2012–2014

Participants: Erven Rohou, Alain Ketterlin, Emmanuel Riou.

Computer science is driven by two major trends: on the one hand, the lifetime of applications is much larger than the lifetime of the hardware for which they are initially designed; on the other hand the diversity of computing hardware keeps increasing. The net result is that many applications are not optimized for their current executing environment. The objective of Padrone is to design and develop a platform for reoptimization of binary executables at run-time. There are many advantages: actual hardware is known, the whole application is visible (including libraries), profiling can be collected, and source code is not necessary (interesting in the case of proprietary applications).

8.2.4. ANR W-SEPT

Participants: Hanbing Li, Isabelle Puaut, Erven Rohou.

Critical embedded systems are generally composed of repetitive tasks that must meet drastic timing constraints, such as termination deadlines. Providing an upper bound of the worst-case execution time (WCET) of such tasks at design time is thus necessary to prove the correctness of the system. Static WCET estimation methods, although safe, may produce largely over-estimated values. The objective of the project is to produce tighter WCET estimates by discovering and transforming flow information at all levels of the software design process, from high level-design models (e.g. Scade, Simulink) down to binary code. The ANR W-SEPT project partners are Verimag Grenoble, IRIT Toulouse, Inria Rennes. A case study is provided by Continental Toulouse.

8.3. European Initiatives

8.3.1. FP7 Projects

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

Type: IDEAS

Instrument: ERC Advanced Grant

Duration: April 2011 - March 2016

Coordinator: André Seznec

Inria contact: André Seznec

Abstract: In the DAL, Defying Amdahl's Law project, 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 information, see http://www.irisa.fr/alf/index.php?option=com_content&view=article&id=55&Itemid=3&lang=e

8.3.2. Collaborations in European Programs, except FP7

8.3.2.1. HiPEAC3 NoE

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 HiPEAC3. HiPEAC3 addresses the design and implementation of high-performance commodity computing devices in the 10+ year horizon, covering both the processor design, the optimizing compiler infrastructure, and the evaluation of upcoming applications made possible by the increased computing power of future devices.

8.3.2.2. COST Action TACLe - Timing Analysis on Code-Level (http://www.tacle.eu) 10-2012/09-2015

Participants: Damien Hardy, Isabelle Puaut.

Embedded systems increasingly permeate our daily lives. Many of those systems are business- or safety-critical, with strict timing requirements. Code-level timing analysis (used to analyze software running on some given hardware w.r.t. its timing properties) is an indispensable technique for ascertaining whether or not these requirements are met. However, recent developments in hardware, especially multi-core processors, and in software organization render analysis increasingly more difficult, thus challenging the evolution of timing analysis techniques.

New principles for building "timing-composable" embedded systems are needed in order to make timing analysis tractable in the future. This requires improved contacts within the timing analysis community, as well as with related communities dealing with other forms of analysis such as model-checking and type-inference, and with computer architectures and compilers. The goal of this COST Action is to gather these forces in order to develop industrial-strength code-level timing analysis techniques for future-generation embedded systems, through several working groups:

- WG1 Timing models for multi-cores and timing composability
- WG2 Tooling aspects
- WG3 Early-stage timing analysis
- WG4 Resources other than time

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Pr Ahmed El-Mahdy, from the Egyptian-Japanese University of Science and Technology visited the ALF project for 1 week in October 2013.
- Pr Onur Mutlu, from Carnegie Mellon visited the ALF project for 3 weeks June-July 2013.

ATEAMS Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. Master Software Engineering

ATEAMS is the core partner in the Master Software Engineering at Universiteit van Amsterdam. This master is a collaboration between SWAT/ATEAMS, Universiteit van Amsterdam, Vrije Universiteit and Hogeschool van Amsterdam.

6.1.2. Early Quality Assurance in Software Production

The EQUA project is a collaboration among Hogeschool van Amsterdam (main partner) Centrum Wiskunde & Informatica (CWI), Technisch Universiteit Delft, Laboratory for Quality of Software (LaQuSo), Info Support, Software Improvement Group (SIG), and Fontys Hogeschool Eindhoven.

6.1.3. Model-Driven Engineering in Digital Forensics

In this project ATEAMS works with the Dutch National Forensics Institute on next generation carving software for recovering evidence from damaged or erased data storage media.

6.1.4. Next Generation Auditing: Data-assurance as a service

This collaboration between Centrum Wiskunde & Informatic (CWI) PriceWaterhouseCoopers (PWC), Belastingdienst (National Tax Office), and Computational Auditing, is to enable research in the field of computational auditing.

6.2. European Initiatives

6.2.1. FP7 Projects

OSSMETER aims to extend the state-of-the-art in the field of automated analysis and measurement of open-source software (OSS), and develop a platform that will support decision makers in the process of discovering, comparing, assessing and monitoring the health, quality, impact and activity of open-source software. The project started in October 2012. ATEAMS contributes to this project by focusing on software analysis and related areas.

6.3. International Research Visitors

6.3.1. Visits of International Scientists

- Oscar Nierstrasz, PhD, Professor - Professor of Computer Science at the Institute of Computer Science (IAM) of the University of Bern
- Anya Helene Bagge, PhD - University of Bergen, Norway
- Sebastian Erdweg, PhD - TU Darmstadt

6.3.1.1. Internships

- Kevin van der Vlist
- Davy Meers
- Wouter Kwakernaak
- Jimi van der Woning
- Ioana Rucareanu
- Ioannis Tzanellis
- George Marminidis
- Vlad Lep
- Dimitrios Kyritsis
- Chris Mulder

CAIRN Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

The CAIRN team has currently some collaboration with the following laboratories: CEA List, CEA Leti, LEAT Nice, Lab-Sticc (Lorient, Brest), LIRMM (Montpellier, Perpignan), LIP6 Paris, IETR Rennes, Ireena Nantes; and with the following Inria project-teams: Aric, Compsys, Socrate.
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. E. Casseau is in charge of the architecture topic of the reconfigurable platform working group.
- 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 and ARITH working group on Computer Arithmetic

7.1.1. ANR Blanc - PAVOIS (2012–2016)

Participants: Arnaud Tisserand, Emmanuel Casseau, Romuald Rocher, Philippe Quémerais, Jérémie Métairie, Nicolas Veyrat-Charvillon, Nicolas Estibals, Thomas Chabrier, Karim Bigou.

PAVOIS (in French: *Protections Arithmétiques Vis à vis des attaques physiques pour la cryptOgraphIe basée sur les courbeS elliptiques*) is a project on Arithmetic Protections Against Physical Attacks for Elliptic Curve based Cryptography. It involves IRISA-CAIRN (Lannion) and LIRMM (Perpignan and Montpellier). This project will provide novel implementations of curve based cryptographic algorithms on custom hardware platforms. A specific focus will be placed on trade-offs between efficiency and robustness against physical attacks. One of our goal is to theoretically study and practically measure the impact of various protection schemes on the performance (speed, silicon cost and power consumption). Theoretical aspects will include an investigation of how special number representations can be used to speed-up cryptographic algorithms, and protect cryptographic devices from physical attacks. On the practical side, we will design innovative cryptographic hardware architectures of a specific processor based on the theoretical advancements described above to implement curve based protocols. We will target efficient and secure implementations for both FPGA an ASIC circuits. For more details see http://pavois.irisa.fr.

7.1.2. ANR INFRA 2011 - FAON (2012-2015)

Participants: Raphaël Bardoux, Arnaud Carer, Matthieu Gautier, Pascal Scalart.

The FAON (Frequency based Access Optical Networks) project objectives are to demonstrate the technology and feasibility of a new type of Passive Optical Network (PON) for broadband access which uses a Frequency based shared access technique known as Frequency Division Multiplexing (FDM). These goals completely fall into the line of the expected capacity increase in PON which is today forecasted to go from 100 Mbps per user to 1 Gbps. For more details, see http://www.anr-faon.fr/. Faon involves Orange Labs, CEA-LETI, University of South Brittany (Lab-STICC laboratory) and University of Rennes 1 (Foton laboratory and CAIRNteam). CAIRNaims at developing a high-rate architecture at the receiver side. Specific receiver algorithms (synchronization and equalization) and FPGA implementation are the key issues that will be addressed.

7.1.3. Equipex FIT - Future Internet (of Things)

Participants: Vaibhav Bhatnagar, Arnaud Carer, Matthieu Gautier, Ganda-Stéphane Ouedraogo, Olivier Sentieys.

FIT is one of 52 winning projects from the first wave of the French Ministry of Higher Education and Research's "Équipements d'Excellence" (Equipex) research grant programme. FIT involves UPMC, Inria, LSIIT and the Institut Mines-Telecom and runs over a nine-year period. FIT offers a federation of several independent experimental testbeds to provide a larger-scale, more diverse and higher performance platform for accomplishing advanced experiments. For more details, see http://fit-equipex.fr/. Inria (CAIRNand Socrate teams) develops the cognitive radio testbed that will provide a full experimental environment for evaluating the coexistence and the cooperation between heterogeneous multistandard nodes. To this aim, a fully open architecture based on software defined radio nodes is developed. CAIRNaims at proposing an FPGA based software defined radio with high level specifications. Cognitive radio testbed development is supported by an ADT funding of Inria.

7.1.4. ANR Ingénérie Numérique et Sécurité - ARDyT (2011-2015)

Participants: Arnaud Tisserand, Thomas Chabrier, Philippe Quémerais.

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

7.1.5. ANR Ingénérie Numérique et Sécurité - COMPA (2011-2015)

Participants: Emmanuel Casseau, Steven Derrien, Antoine Courtay, Mythri Alle.

COMPA (model oriented design of embedded and adaptive multiprocessor) is a project which involves CAIRN, IETR (Institut d'Electronique et de Télécommunications de Rennes), Lab-STICC (University of Bretagne Sud), CAPS Entreprise, and Modae Technologies. The goal of the project is to design adaptive multiprocessor embedded systems to the execute dataflow programs. The use case is Reconfigurable video coding (RVC) standard. More specifically, we focus on the portable and platform-independent RVC-CAL language to describe the applications. We use transformations to refine, increase parallelism and translate the application model into software and hardware components. Task mapping, instruction and processor allocation, and specific scheduling are also investigated for runtime execution and reconfiguration.

7.1.6. ANR Ingénérie Numérique et Sécurité - DEFIS (2011-2015)

Participants: Olivier Sentieys, Daniel Menard [external collaborator], Romuald Rocher, Nicolas Simon.

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

7.1.7. ANR ARPEGE - GRECO (2010-2013)

Participants: Olivier Sentieys, Olivier Berder, Arnaud Carer, Trong-Nhan Le.

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

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

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

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

7.2. European Initiatives

7.2.1. FP7 FLEXTILES

Participants: Olivier Sentieys, Emmanuel Casseau, Antoine Courtay, Daniel Chillet, Philippe Quémerais, Christophe Huriaux, Quang-Hoa Le.

Program: FP7-ICT-2011-7

Project acronym: Flextiles

Duration: Oct. 2011 - Sep. 2014

Coordinator: Thales

Other partners: Thales (FR), UR1 (FR), KIT (GE), TU/e (NL), CSEM (SW), CEA LETI (FR), Sundance (UK)

Project title: Self Adaptive Heterogeneous Manycore Based on Flexible Tiles

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.

7.2.2. FP7 ALMA

Participants: Steven Derrien, Romuald Rocher, Olivier Sentieys, Maxime Naullet, Ali Hassan El-Moussawi.

Program: FP7-ICT-2011-7

Project acronym: Alma

Project title: Architecture oriented paraLlelization for high performance embedded Multicore systems using scilAb

Duration: Sep. 2011 - Aug. 2014

Coordinator: KIT

Other partners: KIT (GE), UR1 (FR), Recore Systems (NL), Univ. of Peloponnese (GR), TEI-MES (GR), Intracom SA (GR), Fraunhofer (GE)

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 abstraction descriptions. 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 Europe 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 multicore 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.

7.2.3. Collaborations with Major European Organizations

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

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

Code and Cryptography group of University College Cork (Ireland), Arithmetic operators for cryptography, side channel attacks for security evaluation, and WSN for health monitoring

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

7.3. International Initiatives

7.3.1. Inria International Partners

7.3.1.1. Declared Inria International Partners

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

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

7.3.1.2. Informal International Partners

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

7.3.2. CNRS PICS - SPiNaCH (2012 - 2014)

Title: Secure and low-Power sensor Networks Circuits for Healthcare embedded applications

Principal investigator: Arnaud Tisserand, Olivier Berder, Olivier Sentieys

International Partner (Institution - Laboratory - Researcher): Code&Crypto group in University College Cork (Ireland)

Duration: 2012 - 2014

Biomedical sensor networks may be used more and more in the future. For instance, they allow patient's health-care parameters to be remotely monitored at home. In this project, we plan to address two important challenges in the design of biomedical sensors networks: i) design of low-power sensor devices for embedded autonomous systems (health monitoring, pace-maker...) with long battery life; ii) confidentiality and security aspects and especially with public key cryptography processor that are robust against side channel attacks (measure of the computation time, the power consumption or the electromagnetic radiations of the circuit) and with limited power-energy resources.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Prof. Russel Tessier (University of Massachusetts, UMass Reconfigurable Computing Group, USA) for one month in June-July (Visiting professor position from University Rennes 1).

Prof. Liam Marnane (University College Cork, Ireland) for one month in June (Visiting professor position from University Rennes 1).

Prof. Emanuel Popovici (University College Cork, Ireland) for two weeks in July (Visiting professor position from University Rennes 1).

Prof. Manav Bhatnagar, (Department of Electrical Engineering, Indian Institute of Technology, Delhi, India) for two weeks in December (Visiting professor position from University Rennes 1).

Dr. Michele Magno, post-doc, (University College Cork, Ireland) for one week in July (funded by CNRS PICS SpiNaCH project).

7.4.2. Internships

Participant: Simara Pérez Zurita.

Subject: Optimizing Computational Precision in High-level Synthesis of Signal Processing Systems: Theory and Implementation using TDS and GECOS

Date: from Oct 2012 until Aug 2013

Institution: *Technical University of Kaiserslautern* (Kaiserslautern, Germany)

Participant: Rengarajan Ragavan.

Subject: Reconfigurable Microtasks for Ultra-Low Power Wireless Sensor Network Nodes

Date: from Jan 2013 until Jul 2013

Institution: *Linkoping University* (Linkoping, Sweden)

Participant: Amith Vikram Pai.

Subject: Design and Validation of a Low-Power Embedded FPGA

Date: from Jan 2013 until Jun 2013

Institution: Birla Institute of Technology and Science, Pilani (India)

CAMUS Team

8. Partnerships and Cooperations

8.1. National Initiatives

Philippe Clauss, Alain Ketterlin, Cédric Bastoul and Vincent Loechner are involved in the Inria Large Scale Initiative entitled "Large scale multicore virtualization for performance scaling and portability" and regrouping several french researchers in compilers, parallel computing and program optimization. The project started officially in January 2013. In this context and since January 2013, Philippe Clauss is co-advising with Erven Rohou of the Inria team ALF, Nabil Hallou's PhD thesis focusing on dynamic optimization of binary code.

The CAMUS team is taking part of the NANO 2017 national research program with the company STMicroelectronics, starting January 2014.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, except FP7

Program: ITEA

Project acronym: MANY

Project title: Many-core Programming and Resource Management for High-Performance Embedded Systems

Duration: 09/2011 - 08/2014

Coordinator: XDIN

Other partners: France: Thales Communications and Security, CAPS Entreprise, Telecom SudParis; Spain: UAB; Sweden: XDIN; Korea: ETRI, TestMidas, SevenCore; Netherlands: Vector Fabrics, ST-Ericsson, TU Eindhoven; Belgium: UMONS.

Abstract: Adapting Industry for the for the disruptive landing of many-core processors in Embedded Systems in order to provide scalable, reusable and very fast sofware development.

8.3. International Initiatives

8.3.1. Inria Associate Teams

8.3.1.1. ANCOME

Title: Memory and applications memory behavior

Inria principal investigator: Philippe Clauss

International Partner (Institution - Laboratory - Researcher):

University of Buenos Aires (Argentina) - Departamento de Computación, Facultad de Ciencias Exactas y Naturales - Philippe Clauss

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 consist in analyzing and modeling the runtime behavior, where extracted properties are then verified thanks to static analysis processes. Thus pure static approaches limits will be overpassed. Further, the case of multi-threaded applications run on multi-core architectures will be 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.

8.3.2. Inria International Partners

8.3.2.1. Informal International Partners

The CAMUS team maintains regular contacts with the following entities:

- Reservoir Labs, New York, NY, USA
- Intel, Santa Clara, CA, USA
- UPMARC, University of Uppsala, Sweden
- University of Batna, Algeria
- University El Manar, Tunis, Tunisia
- Ohio State University, Colombus, USA
- Louisiana State University, Baton Rouge, USA
- Indian Institute of Science (IIIS) Bangalore, India
- University of Delaware, DE, USA

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Diego Garbervetsky, University of Buenos Aires, Argentina, has made three visits in the CAMUS team at the following dates: Dec. 1-14, Oct. 14-20 and Jan. 15-23.

Rachid Seghir, University of Batna, Algeria, visited the team from May the 30th to June the 13th.

8.4.1.1. Internships

Javier Corti

Subject: Certified Compiler for polyhedral transformations

Date: from Mar 2013 until Aug 2013

Institution: Universidad National de Rosario (Argentina)

Imen Fassi

Subject: Multifor for Multicore

Date: from Mar 2013 until Aug 2013

Institution: Université de Tunis El Manar - Faculté des Sciences (Tunisia)

Dhruva Tirumala Bukkapatnam

Subject: Evaluation of the Kalray MPPA and extension of the Pluto compiler

Date: from Apr 2013 until Oct 2013

Institution: Birla Institute of Technology and Science, Birla (India)

8.4.2. Visits to International Teams

Philippe Clauss has spent one week in the LAFHIS team, University of Buenos Aires, Argentina, in October 2013.

COMPSYS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Compsys has increased its relationship with the CITI laboratory (Insa-Lyon) and, in particular, the team of Tanguy Risset (Socrate Inria project http://www.citi-lab.fr/team/socrate/). Compsys and Socrate made several common working groups in 2012 and 2013, and are mutually invited to seminars organized by the other team. Streaming languages are a common topic of interest. In this context, Socrate, with the help of Compsys, will organize a thematic day (April 14, 2014) on the "compilation and execution of streaming programs", in Domaine des Hautannes, St Germain au Mont d'Or. Lionel Morel and Laure Gonnord have also common topics of interest.

Compsys has stronger connections with the Grame music/computer laboratory (http://www.grame.fr) in Lyon and, in particular, Yann Orlarey, also due to common interests on streaming languages, in particular the language Faust developed by Grame. Yann Orlarey was one of the invited speaker of the keynotes on parallel languages (see the description the thematic quarter on compilation in Section 9.1.2). Alexandre Isoard's Master 1 training period was on Faust, co-advised by Alain Darte and Yann Orlarey. For 2014, Laure Gonnord and Yann Orlarey proposed a Master research topic on the generation of invariants for the Faust language.

Compsys is also involved in the Labex MILYON (Mathématiques et Informatique Fondamentale de Lyon), which regroups Institut Camille Jordan, and the mathematics and computer science labs of ENS-Lyon. The aim of MILYON is "to strengthen our international relationships, in particular by organizing thematic quarters which will allow world experts of a subject to gather in Lyon and work together in a stimulating environment." In this context, Compsys organized a thematic quarter on compilation from April 2013 to July 2013, see details in Section 9.1.2 . Compsys also follows or participates to the activities of LyonCalcul (http://lyoncalcul.univ-lyon1.fr/), a network to federate activities on computing in Lyon.

8.2. National Initiatives

8.2.1. CNRS PEPS

Christophe Alias and Laure Gonnord initiated with the DART/Emeraude team at LIFL Laboratory (University of Lille) a CNRS PEPS ("Projets Exploratoire Premier Soutien") called "HLS and real time" (8 Keuros/year, during two years in 2011-2013). The goal of this project is to investigate how to introduce real-time constraints in the high-level synthesis workflow.

8.2.2. Inria AEN MULTICORE

Fabrice Rastello is part of an Inria Large Scale Initiative (AEN: action d'envergure nationale) called MULTICORE, which regroups researchers from seven teams: Camus, Regal, Alf, Runtime, Algorille, Dali, and thus Compsys on "Large scale multicore virtualization for performance scaling and portability". One of the goals of this project is to enable loop transformations by combining dynamic and static analysis/compilation techniques.

8.2.3. French Compiler Community

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" were initiated in 2010 and are still animated by Fabrice Rastello and Laure Gonnord as a biannual event. Their local organization is handled alternately by the different research teams: Lyon (by Compsys) in Summer 2010, Aussois in Winter 2010, Dinard in Spring 2011, St Hippolyte in Autumn 2011, Rennes in Summer 2012, Annecy (by Compsys again) in Spring 2013, Dammarie-les-lys in December 2013.

8.3. European Initiatives

8.3.1. Collaborations with Major European Organizations

Alain Darte, Paul Feautrier, and Fabrice Rastello are members or affiliate members of the European Network of Excellence on High Performance and Embedded Architecture and Compilation (HiPEAC). Fabrice Rastelloattended the computing system week in may 2013 (Paris), and the computing system week in October 2013 (Tallinn). He participated to the organization of two thematic sessions in Paris: Thread Level Speculation (as chair) and Intermediate Representation (as co-organizer). The thematic quarter on compilation (see Section 9.1.2) was presented in HIPEAC info 35 (July 2013), the HIPEAC quarterly newsletter (http://www.hipeac.net/content/hipeacinfo-35-july-2013) and the keynotes on HPC languages (third event) recognized as an HIPEAC event.

8.4. International Initiatives

8.4.1. Inria International Partners

8.4.1.1. Declared Inria International Partners

- Compsys and, in particular Fabrice Rastello, has a regular collaboration with P. Sadayappan from Ohio State University (USA). This year, this collaboration led to several results, see Sections 6.2 , 6.4 , 6.5 , and 6.6 .
- Fabrice Rastello and Laure Gonnord have a regular collaboration with Fernando Magno Quintao Pereira from the University of Mineas Gerais (Brazil). This year, this collaboration led to several results, see Sections 6.1 and 6.3 . Compsys also hosted Raphael Ernani Rodrigues, from the group of F. Pereira, who made part of his master in Lyon supervised by Laure Gonnord and Christophe Alias.
- Compsys and, in particular Christophe Alias, has a regular collaboration with S. Rajopadhye from Colorado State University (CSU). Guillaume Iooss is preparing a PhD through a PhD convention between Ecole normale supérieure de Lyon and Colorado State University, co-advised by Christophe Alias and Sanjay Rajopadhye. In 2013, Guillaume Iooss spent part of the summer at CSU, joined by Christophe Alias for a week. Paul Feautrier and Fabrice Rastello also made regular visits at Colorado State University in the previous years. This year, this collaboration led to several results, see Sections 6.10 , 6.11 , and 6.13 .

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Invited Researchers

Fernando Magno Quintão Pereira is visiting Fabrice Rastello for 1.5 month in early 2014. The goal of his visit is to work on dynamic analysis and cloning for loop transformations (so called hybrid compilation).

8.5.1.2. Internships

Raphael Ernani Rodrigues made part of his master Internship in Lyon in June/July 2013 under the supervision of Laure Gonnord and Christophe Alias. He worked on synthesizing preconditions that (may) ensure termination. We are currently pursuing the collaboration with him and his supervisor in Brazil, Fernando Magno Quintao Pereira (Univ. Mineas Gerais).

8.5.2. Visits to International Teams

Fabrice Rastello visited the group of P. Sadayappan (OSU) during two months, in June-July 2013, in addition to shorter stays. He worked on dynamic analysis and generalized tiling.

Alexandre Isoard did an internship at Xilinx, during 2.5 months, from June to September 2013, under the supervision of Stephen Neuendorffer, working on exploring polyhedral tools for Xilinx HLS tool.

CONTRAINTES Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

- The OSEO BioIntelligence coordinated by Dassault-Systèmes, with EPI Orpailleur, Sobios, Aureus pharma, Ipsen, Pierre Fabre, Sanofi-Aventis, Servier, Bayer CropScience, INSERM, Genopole Evry (2009-2014).
- ANR Investissement Avenir Iceberg project (2011-2016) "From population models to model populations", 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 Blanc Net-WMS-2 (2011-2015) on "constraint optimization in Wharehouse Management Systems", coordinated by F. Fages, with N. Beldiceanu, Ecole des Mines de Nantes, EPI TASC, and Abder Aggoun, KLS optim.
- ANR Cosinus Syne2arti project (2010-2013) coordinated by Grégory Batt, with Oded Maler, CNRS Verimag, Dirk Drasdo, EPI Bang, and Ron Weiss, MIT.
- ANR Blanc BioTempo project (2010-2014) coordinated by Anne Siegel, CNRS IRISA Rennes, with Ovidiu Radulescu, U. Montpellier, Irina Rusu, U. Nantes.
- AE REGATE (2008-2013) on the "REgulation of the GonAdoTropE axis", coordinated by Frédérique Clément, SISYPHE, with E. Reiter, INRA Tours, J.P. Françoise, Univ. Paris 6, B. Laroche Orsay, P. Michel Centrale Lyon, N. Ayache ASCLEPIOS, A. Goldbeter, ULB Bruxelles.
- AE COLAGE (2008-2013) on the "control of growth and aging in *E. coli* using synthetic biology approaches", coordinated by H. Berry, COMBINING, with F. Taddei, A. Lindner, INSERM Necker, H. de Jong, D. Ropers, IBIS, H. Geiselmann, Grenoble Univ., J.-L. Gouzé, and M. Chaves, COMORE.
- GENCI (2009-) attribution of 300000 computation hours per year on the Jade cluster of 10000 processors of GENCI 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: march 2010 - march 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 Associate Teams

8.3.1.1. TISHOM

Title: Artificial tissue homeostasis: combining synthetic and computational biology approaches

Inria principal investigator: Grégory Batt

International Partner (Institution - Laboratory - Researcher):

Massachusetts Institute of Technology (United States) - Weiss Lab

Duration: 2012 - 2014

See also: TISHOM

Cell-based gene therapy aims at creating and transplanting genetically-modified cells into a patient in order to treat an illness. Ideally, actively-growing cells are used to form a self-maintaining tissue in the patient, thus permanently curing the disease. Propelled forward by the development of stem cell biology, this research domain has recently attracted significant interest. Still, before any real therapeutic use, many important issues need to be addressed. In particular, one should guarantee tissue homeostasis, that is, that the size of the newly-introduced tissue remains within admissible bounds.

Using a synthetic biology approach, we propose to reprogram mammalian cells so as to enforce tissue homeostasis. The proposed design relies on growth control and cell-cell communication mechanisms. The design and tuning of such engineered tissues are particularly challenging. Indeed, the correct functioning of the system depends on its specific molecular implementation. To relate cell population behavior with molecular details, extensive modelling work and in-depth in silico analysis are needed. Therefore, a tight integration between dry lab and wet lab efforts will be essential for the success of the project.

8.4. International Research Visitors

8.4.1. Internships

Hui-Ju Katherine Chiang (from Jul 13 until Sep 13) on program compilation in biochemical reaction networks.

8.4.2. Visits to International Teams

Grégory Batt: one week with the Weiss lab at MIT

François Bertaux: two weeks with the Weiss lab at MIT

Xavier Duportet: 3 months and 1 week with the Weiss lab at MIT

DREAMPAL Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. IRCICA project " Smart Cities"

Smart Cities is an interdisciplinary project, internal of IRCICA (http://www.ircica.univ-lille1.fr/), in collaboration with the laboratory of Civil Engineering of Lille I. It builds on the expertise of several teams hosted by IRCICA (RF networks, sensors, high-performance and real-time embedded systems computing, pattern recognition). The scientific problem, we tackle within this project, is to develop an intelligent platform for managing accidents and incidents in the drinking water and wastewater. In this platform, a permanent dialogue M2M (machine to machine) between servers, embedded systems (laptops, smartphones, tablets, ...), smart cameras, and sensors, will detect and solve problems in real time.

Scientific problems relate to the study of the possibility of linking objects (cameras , sensors, servers ...) all together, with a standardized mixed network (radio frequency wifi and internet). DreamPal is responsible for implementing the part of the hardware platform for high performance dedicated to intelligent video applications using the HoMade softcore. This work involves the processing of data , analysis of video images, the use of these data, and the integration of embedded reconfigurable components (on Xilinx Zynq 7000 board) as well as the existing RF network cards. It uses the video data acquisition to apply algorithms to detect such an anomaly on the water in a part of the building, or abnormal number of people in a given area, or any information about a specific person such as the recognition of face, the nature of motion. The work done during this year usefully supplements our platform by developing video modules dedicated to intelligent surveillance .

8.2. International Initiatives

We have a strong ongoing collaboration with Univ. Iasi, Romania, which includes (but is not limited to) the co-supervision of the PhD of Andrei Arusoaie. Collaboration topics include language-independent techniques for analysis of programs, and their specialization to the languages designed in the Dreampal project (HiHope, HoMade assembler and machine code).

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Prof. Dorel Lucanu, Assist. Prof./ Stefan Ciobaca, and PhD student Andrei Arusoaie from Univ. Iasi (Romania) visited us in July 2013. We initiated work on language-independent program-verification techniques and on the formal definitions of the HiHope and HoMade assembler languages, as well as on the formally proved correctness of compilation between these languages.

8.3.2. Internships

Kanwarjeet Dhaliwal made his internship in the Dreampal team from May to July 2013. He worked on the formal semantics of the parallel version of Hihope, and also made a preliminary work to compile Hihope to the Kalray's MPPA platform. This work was partially funded by Kalray (http://www.kalray.eu).

8.3.3. Visits to International Teams

In June 2013, Rabie Ben Atitallah and Wissem Chouchene visited Michael Huebner, Professor and Chair for Embedded Systems in Information Technique (ESIT) at the Ruhr-University of Bochum. The objective is to establish a new collaboration in the field of 3D FPGA next generation.

In October 2013, Andrei Arusoaie visited the team of Prof. Grigore Roşu at the University of Illinois at Urbana Champaign, where he worked on implementing the symbolic domains used in our language-independent symbolic execution and verification tool. He benefitted from the guest team's expertise on symbolic domains.

INDES Project-Team

7. Partnerships and Cooperations

7.1. National initiatives

7.1.1. ANR DEFIS PWD

The PWD project (for "Programmation du Web diffus") has been funded by the ANR Défis programme for 4 years, starting November 2009. The partners of this project are the teams INDES (coordinator), LIP6 at University Pierre et Marie Curie and PPS at University Denis Diderot.

7.1.2. FUI X-Data

Broadly available big and open data open new perspectives in terms of use and applications. The X-Data project aims at validating this claim by using actual data sets for building realistic applications. The goal is to combine a large variety of data sets coming from different partners (Data Publica, Orange, EDF, La Poste, social networks, ...) to build innovative applications. The Indes team designs and implements new programming language constructs that help programming these applications.

7.1.3. MEALS

The MEALS project (Mobility between Europe and Argentina applying Logics to Systems), IRSES program, started October 1st (2011), and will end September 30th, 2015. The project goals cover three aspects of formal methods: specification (of both requirement properties and system behavior), verification, and synthesis. The Indes members are involved in the task of Security and Information Flow Properties (WP3). The partners in this task include University of Buenos Aires, University of Cordoba, Inria (together with Catuscia Palamidessi, Kostas Chatzikokolakis, Miguel Andrés) and University of Twente.

7.2. European initiatives

7.2.1. FP7 Projects

Program: RAPP

Title: Robot App Store

Collaborator: Inria Coprin

Abstract: RAPP is a 36 months pan-european FP7 project, started in December 2013. Hop is used in the development of prototypes of the Coprin Ang rollator transfer device, for mobility assistance and activity monitoring.

7.2.2. Collaborations in European Programs, except FP7

Program: ICT Cost Action IC1201

Program acronym: BETTY

Project title: Behavioural Types for Reliable Large-Scale Software Systems

Duration: October 2012 - October 2016

Coordinator: Simon Gay, University of Glasgow

Other partners: Several research groups, belonging to 22 european countries

Abstract: The aim of BETTY is to investigate and promote behavioural type theory as the basis for new foundations, programming languages, and software development methods for communication-intensive distributed systems. Behavioural type theory encompasses concepts such as interfaces, communication protocols, contracts, and choreography.

PAREO Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

We participate at the LORIA project entitled “Combining deduction engines into SMT”.

7.2. 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).

7.3. International Research Visitors

7.3.1. Internships

Anisia Maria Magdalena Tudorescu

Subject: Integrating SMT solvers into Spike

Date: from Mar 2013 until May 2013

Institution: West Timisoara University (Romania)

Cosay Gurkay Topaktas

Subject: Property Based Testing

Date: from Feb 2013 until Jun 2013

Institution: Erasmus Mundus MSc in Dependable Software Systems

Fellype Vedovato Martins

Subject: Generation of Terms

Date: from Jun 2013 until Sept 2013

Institution: Mines-Nancy, 2nd year student

TASC Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- AGIRA project (LigéRO) *Teaching optimization project*.

8.2. National Initiatives

- Development of IBEX with Jordan Ninin and Luc Jaulin from ENSTA Bretagne, Bertrand Neveu from ENPC PariTech, and Gilles Trombettoni from Lirmm.
- Work on a conference and journal paper on optimization problems with Mohamed Siala, PhD student at LAAS, Toulouse.
- Collaboration with F. Pachet and P. Roy, Sony music, Paris.

8.3. International Initiatives

8.3.1. Inria Associate Teams

Inria Associated Team Bananas

- Partners: Inria-Lorraine, PUCV (Chili), UTFSM (Chili), Univ. Angers (LERIA), Univ. Nantes (TASC).
- Duration: 2012-2014.
- Topics: Autonomous constraint solving, SMT solvers.
- Budget: 15 KEuros per year for the project.

8.3.2. Inria International Partners

8.3.2.1. Informal International Partners

- SICS, Sweden: Work on the *global constraint catalog* and on *scalable constraints* with Mats Carlsson.
- Uppsala University, Sweden: Work on automata and dedicated filtering algorithms for some constraint patterns with the ASTRA group of Pierre Flener.
- JFLI, Japan: Work with Philippe Codognet.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Helmut Simonis (4C): work on model learning and work on learning constraints in the context of EDF, three months.

8.4.2. Visits to International Teams

- N. Beldiceanu, 4C Cork Ireland: work on *learning generic models* and work on *learning constraints in the context of EDF* with H. Simonis.
- N. Beldiceanu, Uppsala University and SICS: work on *automata and constraints* with P. Flener and J. Pearson and on *learning generic models* with M. Carlsson.
- Eric Monfroy, Univ. Austral de Chile, Valparaiso, Chile: work on autonomous search with B. Crawford and R. Soto.

ESPRESSO Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

Program: ANR

Project acronym: VeriSync

Project title: Vérification formelle d'un générateur de code pour un langage synchrone

Duration: Nov. 2010 - Oct. 2013

Coordinator: IRIT

Other partners: IRIT

URL: http://www.irit.fr/Verisync/

Abstract:

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

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

7.1.2. Competitivity Clusters

Program: FUI

Project acronym: P

Project title: Project P

Duration: March 2011 - Sept. 2015

Coordinator: Continental Automotive France

Other partners: 19 partners (Airbus, Astrium, Rockwell Collins, Safran, Thales Alenia Space, Thales Avionics...)

URL: http://www.open-do.org/projects/p/

Abstract:

The aim of project P is 1/ to aid industrials to deploy model-driven engineering technology for the development of safety-critical embedded applications, 2/ to contribute on initiatives such as OPEES [23] and CESAR [22] to develop support for tools inter-operability, and 3/ to provide state-of-the-art automated code generation techniques from multiple, heterogeneous, system-levels models. The focus of project P is the development of a code generation toolchain starting from domain-specific modeling languages for embedded software design and to deliver the outcome of this development

as an open-source distribution, in the aim of gaining an impact similar to GCC for general-purpose programming, as well as a kit to aid with the qualification of that code generation toolchain.

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

7.1.3. CORAC

Program: CORAC

Project acronym: CORAIL

Project title: Composants pour l'Avionique Modulaire Étendue

Duration: July 2013 - May 2017

Coordinator: Thales Avionics

Other partners: Airbus, Dassault Aviation, Eurocopter, Sagem...

URL: http://www.corac-ame.com/

Abstract:

The CORAIL project aims at defining components for Extended Modular Avionics. The contribution of project-team ESPRESSO is to define a specification method and to provide a generator of multi-task applications.

7.2. International Initiatives

7.2.1. Inria Associate Teams

7.2.1.1. POLYCORE

Title: Models of computation for embedded software design of multi-core architectures

Inria principal investigator: Jean-Pierre Talpin

International Partner :

Virginia Tech Research Laboratories, Arlington (United States)

Embedded Systems Group, Teschnische Universität Kaiserslautern (Germany)

Duration: 2011 - 2013

See also: http://www.irisa.fr/espresso/Polycore

Anyone experienced with multi-threaded programming would recognize 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 necessary for safe execution of such code. 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 French tools based on the synchronous programming models. Unfortunately, software generated in those contexts usually operate in a time-triggered execution model. Such models are simpler but less efficient than multi-threaded software on multi-core processors. Normally they run on multiple processors communicating over a time-triggered bus. Hence the execution is less efficient than it could be. While time-triggered programming model simplifies code generation, we feel that multi-rate event driven execution model is much more efficient. Code synthesis for such execution model must be thoroughly investigated. The multi-threaded software generation is inspired by a recent shift in the hardware design paradigms from single-core to multi-core processors. This shift has brought parallel and concurrent programming to the desktop and embedded arena. In the desktop market, most processors

now being sold are multi-core, and very soon this trend might conquer the embedded world as well. 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 dataflow paradigm: Polychrony.

7.2.2. Inria International Partners

7.2.2.1. The University of Hong Kong, Emerging Technologies Institute

Title: Virtual prototyping of embedded software architectures

Inria principal investigator: Jean-Pierre Talpin

International Partner :

The University of Hong Kong - Emerging Technologies Institute - John Koo

Embedded software architectures are modeling objects at the crossing of several design viewpoints: the physical environment, the embedded software and the hardware architecture. These viewpoints present different perceptions of time: continuous and discrete, event-based and clock-based. They are further represented by high-level models that significantly alter this perception: in the model of the environment, evolution over time is represented by differential equations whose resolution alters discrete simulation time; in the model of the embedded software, hardware/operating-system events are sampled by periodic reaction loops; in the model of the hardware, instruction clock time is usually approximated by coarser periods or transactions. Providing a mathematical framework, verification and synthesis tools, to understand, compose and orchestrate them would prove invaluable to system architects. The architect operates from design focus point around which all components of the system under design—software, middleware, hardware and environment—need to be analyzed, profiled, composed, simulated, validated. It is the aim of our project to propose a formal design methodology to that purpose.

7.2.2.2. Beihang University, Institute of Computer Architectures

Title: Certifiable development of a synchronous compiler for multi-core platforms

Inria principal investigator: Jean-Pierre Talpin

International Partner :

Beihang University, China - Institute of Computer Architectures - Kai Hu

The synchronous paradigm is a widely accepted approach for the design of safety-critical applications, such as digital circuits or embedded software. The well-defined notions of time and causality at specification-level provide a simple way to model, analyze and verify systems. The synchronous programming paradigm is made popular because of its role at the joint point of 1) computer science and language design, 2) control theory and reactive systems, and 3) microelectronic (synchronous) circuit design. It provides a sound semantic background with a notion of discrete instants and successive reactions, together with high-level structuring primitives which help defining subthreads whose activations (defined by signals or clocks) model over/sub-sampling. Exploiting the semantic independence of various computations to allow the generation of concurrent, potentially distributed code from synchronous and polychronous specifications is a notoriously difficult subject. It amounts to determining which part of the system-wide synchronization specific to the synchronous model can be removed while preserving the specified functionality. In this context, the objective of the proposed project consists in the design of a certifiable compiler from a synchronous language to a multicore platform. However, even if the compilation of endochronous systems to a sequential architecture has been widely studied for twenty years, targeting multicore architectures is more recent and exploiting weak endochrony has not yet been deeply explored. Three main points will be addressed: the architecture of a compiler of weakly-endochronous programs to a virtual parallel machine; the formal verification of some of these compilation steps as well as the formal modeling of the target; the study of multicore platforms, of their synchronization primitives and the implementation of the virtual machine on such a platform.

7.2.3. Participation In other International Programs

7.2.3.1. USAF Office for Scientific Grant FA8655-13-1-3049

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

Inria principal investigator: Jean-Pierre Talpin

International Partner :

Virginia Tech Research Laboratories, Arlington (United States)

Embedded Systems Group, Teschnische Universität Kaiserslautern (Germany)

Duration: 2013 - 2016

See also: http://www.irisa.fr/espresso/Polycore

The aim of the USAF OSR Grant FA8655-13-1-3049 is to support collaborative research entitled "Co-Modeling of safety-critical multi-threaded embedded software for multi-core embedded platforms" between Inria project-team ESPRESSO, the VTRL Fermat Laboratory and the TUKL embedded system research group, under the program of the Polycore associate-project.

7.3. International Research Visitors

7.3.1. Visits to International Teams

- Jean-Pierre Talpin was awarded a visiting researcher grant by the Chinese Academy of Science. In this context, he visited the Shenzhen Institutes of Advanced Technology and the University of Hong Kong in January, July and August, and Beihang University in November and December.
- In the context of the associate project Polycore, Jean-Pierre Talpin visited Virginia Tech Research Laboratories, Arlington, in April and October.

S4 Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

...

8.2. National Initiatives

8.2.1. Synchronics: Language Platform for Embedded System Design

Participants: Albert Benveniste, Benoît Caillaud.

Large scale initiative funded by INRIA. *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 contributions to Synchronics in 2012 are:

- A journal paper [] presenting the non-standard semantics for hybrid systems and its applications to the semantics and compilation of hybrid modeling languages. Details can be found in Section .
- Inputs to the latest evolution of the Modelica language, related to state machines and a clock calculus.
- A study of modular code generation techniques for reactive synchronous programming languages, based on an interface theoretic approach [], []. See for further details.

8.3. European Initiatives

8.3.1. FP7 Projects

8.3.1.1. DALI

Type: COOPERATION

Defi: ICT for Health, Ageing Well, Inclusion and Governance

Instrument: Specific Targeted Research Project

Objectif: ICT for Ageing and Wellbeing

Duration: November 2011 - October 2014

Coordinator: ___COORDINATOR___???

Partner: ___DEPARTEMENT???___, ___INSTITUTION???___ (Italy)

Inria contact: Axel Legay

Abstract: ___RESUME???___

8.3.2. Collaborations in European Programs, except FP7

8.3.3. Collaborations with Major European Organizations

8.4. International Initiatives

8.4.1. Inria Associate Teams

8.4.2. Inria International Partners

8.4.2.1. Declared Inria International Partners

8.4.2.2. Informal International Partners

8.4.3. Inria International Labs

8.4.4. Participation In other International Programs

8.4.4.1. ___SIGLE???___

Program: International joint supervision of PhD agreement

Title: Contrôle de l'opacité dans les systèmes distribués à flots de tâches basés sur le partage de documents structurés

Inria principal investigator: Eric BADOUEL

International Partner (Institution - Laboratory - Researcher):

University Cheikh Anta Diop of Dakar (Senegal) - Eric BADOUEL

Duration: Dec 2010 - Dec 2013

See also: ___URL???___

___ABSTRACT???___

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Internships

8.5.2. Visits to International Teams

TRIO Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. BGLE DEPARTS

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo, Cristian Maxim.

The project DEPARTS started on October 1st, 2012, but for administrative reasons the kick-off meeting was only on April, 2013. This project is funded by the national funding program BGLE. TRIO team proposes solutions for probabilistic component-based models and a PhD thesis will start early 2014. Such solution allows designers to unify in the same framework probabilistic scheduling techniques and compositional guarantees that have different levels of criticality. The schedulability analysis presented in [12], [6] are the bases of our future contributions.

7.2. European Initiatives

7.2.1. FP7 Projects

7.2.1.1. PROARTIS

Type: COOPERATION

Defi: Embedded Systems Design

Instrument: Specific Targeted Research Project

Objectif: Embedded Systems Design

Duration: February 2010 - July 2013

Coordinator: Barcelona Supercomputing Center (Spain)

Inria contact: L. Cucu-Grosjean

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo, Dorin Maxim and Cristian Maxim.

TRIO team participates to PROARTIS which is a STREP project within the FP7 call and it started on February 2010. It has six partners: Barcelona Supercomputing, University of York, University of Padova, Inria and Airbus. The overarching objective of the PROARTIS project is to facilitate a probabilistic approach to timing analysis. The PROARTIS approach concentrates on proving that pathological timing cases can only arise with negligible probability, instead of struggling to eradicate them, which is arguably not possible and could severely degrade performance. This is a major turn from previous approaches that seek analyzability by predicting with cycle accuracy the state of hardware and software through analysis.

The PROARTIS project facilitates the production of analysable CRTE systems on advanced hardware platforms with features such as memory hierarchies and multi core processors.

This project ended July 2013.

7.2.1.2. PROXIMA

Type: COOPERATION

Defi: Mixed-Criticality Systems

Instrument: Integrated Project

Objectif: Development of probabilistic approaches for mixed-criticality systems on multi-core and many-core platforms

Duration: October 2013 - September 2016

Coordinator: Barcelona Supercomputing Center (Spain)

Inria contact: Liliana Cucu-Grosjean

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo, Dorin Maxim and Cristian Maxim.

PROXIMA project started on October 1st, 2013 with a kick-off meeting in November 2013.

The PROXIMA hypothesis is that probabilistic analysis techniques can provide efficient (tractable) and effective (tight) analysis of the temporal behaviour of complex mixed-criticality applications on novel multicore and manycore platforms. Solid research results from the FP7 STREP PROARTIS project underpin this claim. The concept is based on using probabilistic analysis techniques to derive safe and tight bounds on the temporal behaviour of applications, reflecting requirements on failure rates commensurate with their criticality. PROXIMA defines architectural paradigms that break the causal dependence in the timing behaviour of execution components at hardware and software level that can give rise to pathological cases, and reduces that risk to quantifiable small levels. Only modest changes will be needed to this end in the hardware and software components beneath the application (processing cores, interconnects, memory hierarchies and controllers, real-time operating system, middleware, compilers).

7.2.2. Collaborations in European Programs, except FP7

7.2.2.1. European Network of Excellence (NOE) High Performance Embedded Architectures and Compilation (HiPEAC)

Participant: Olivier Zendra.

The TRIO team is involved in the HiPEAC 3 (High Performance Embedded Architecture and Compilation) European Network of Excellence (NoE). Olivier Zendra was initiator and leader in this context of a cluster of European Researchers “Architecture-aware compiler solutions for energy issues in embedded systems” from mid-2007 to mid-2009. A STREP proposal tentatively titled "RuSH2LEAP: Runtime Software-Hardware interactions to Lower Energy And Power" was written at the beginning of 2013, mostly in the context of this network of excellence, for submission in Call ICT 2013.10, challenge 3.4 Advanced computing, embedded and control systems. The proposal passed all thresholds, but failed to be funded.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

Rob Davis (University of York) has continued to visit TRIO within the UK Seedcorn Grant that covers his visits in Nancy. This collaboration allowed to successfully apply for a FP7 IP project as well as an Inria International Chair that will start in 2014 within AOSTE (team that Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo and Cristian Maxim had joined before the end of 2013).

AOSTE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. CIM PACA Design Platform

Participants: Robert de Simone, Ameni Khecharem, Carlos Gomez Cardenas, Emilien Kofman.

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 active in the Design Platform (one of three platforms), of which Inria is a founding member. This provides opportunities for interactions with local companies, leading indirectly to more formal collaborations at times. Phase 3 of the CIM PACA programme should be launched in 2014, and was subject of extensible preparation at the end of 2013.

The ANR HOPE project 8.2.1.2 is conducted under the auspices of the CIM PACA Design Platform, which also hosts prototype and commercial software products contributed by project members (Synopsys, Docea Power, and Magillem, see 8.2.1.2). Similarly, the CLISTINE FUI project was recently accepted, and supported by the platform.

8.2. National Initiatives

8.2.1. ANR

8.2.1.1. HeLP

Participants: Carlos Gomez Cardenas, Ameni Khecharem, Robert de Simone, Jean-Vivien Millo.

The ANR HeLP project dealt with joint modeling of functional behavior and energy consumption for the design of low-power heterogeneous SoCs. Partners were ST Microelectronics and Docea Power (SME) as industrial; Inria, UNS (UMR LEAT), and VERIMAG (coordinator) as academics. Our goal in this project was twofold: first, combine SoC modeling with temporal behavior and logical time with energy/power modeling as extra annotations on MARTE models; second, link the modeling abilities of MARTE with those of the domain-specific standard IP-XACT.

The project ended in April 2013, with some of its findings taken up and extended in the more recent ANR project HOPE.

8.2.1.2. HOPE

Participants: Carlos Gomez Cardenas, Ameni Khecharem, Emilien Kofman, Robert de Simone.

The ANR HOPE project focuses on hierarchical aspects for the high-level modeling and early estimation of power management techniques, with potential synthesis in the end if feasible.
The PhD defense of Carlos Gomez Cardenas was held in Dec 2013 [16], in strong connection with the project (as a follow-up of HeLP).
Although this project was officially started in November, it was in part postponed due to the replacement of a major partner (Texas Instruments) by another one (Intel). Current partners are CNRS/UNS UMR LEAT, Intel, Synopsys, Docea Power, Magillem, and ourselves.

8.2.1.3. GeMoC

Participants: Matias Vara Larsen, Julien Deantoni, Frédéric Mallet.

This project is admistratively handled by CNRS for our joint team, on the UMR I3S side. Partners are Inria (Triskell EPI), ENSTA-Bretagne, IRIT, Obeo, Thales TRT.

The project focuses on the modeling of heterogeneous systems using Models of Computation and Communication for embedded and real-time systems, described using generic means of MDE techniques (and in our case the MARTE profile, and most specifically its Time Model, which allows to specify precise timely constraints for operational semantic definition).

8.2.2. FUI

8.2.2.1. FUI P

Participants: Abderraouf Benyahia, Dumitru Potop Butucaru, Yves Sorel.

The goal of project P is to support the model-driven engineering of high-integrity embedded real-time systems by providing an open code generation framework able to verify the semantic consistency of systems described using safe subsets of heterogeneous modeling languages, then to generate optimized source code for multiple programming (Ada, C/C++) and synthesis (VHDL, SystemC) languages, and finally to support a multi-domain (avionics, space, and automotive) certification process by providing open qualification material. Modeling languages range from behavioural to architectural languages and present a synchronous and asynchronous semantics (Simulink/Matlab, Scicos, Xcos, SysML, MARTE, UML),
See also: http://www.open-do.org/projects/p/
Partners of the project are: industrial partners (Airbus, Astrium, Continental, Rockwell Collins, Safran, Thales), SMEs (AdaCore, Altair, Scilab Enterprise, STI), service companies (ACG, Aboard Engineering, Atos Origins) and research centers (CNRS, ENPC, Inria, ONERA).

8.2.2.2. FUI PARSEC

Participants: Dumitru Potop Butucaru, Thomas Carle, Zhen Zhang, Yves Sorel.

The PARSEC Project aims at providing development tools for critical real-time distributed systems requiring certification according to the most stringent standards such as DO-178B (avionics), IEC 61508 (transportation) or Common Criteria for Information Technology Security Evaluation. The approach proposed by PARSEC provides an integrated toolset that helps software engineers to meet the requirements associated to the certification of critical embedded software. Partners of the project are: Alstom, Thales, Ellidiss, OpenWide, Systerel, CEA, InriaS, Telecom ParisTech.
See also: http://www.systematic-paris-region.org/sites/default/files/exports/projets/fichiers/ProjetPARSEC_BookSystematic2012.pdf.

8.2.2.3. FUI CLISTINE

Participants: Robert de Simone, Amin Oueslati, Emilien Kofman.

This contract has just been accepted, with a kick-off meeting in Dec 2013. Partners are SynergieCAD (coordinator), Avantis, Optis, and the two EPIs Aoste and Nachos. The goal is to study the feasibility of building a low-cost, low-power "supercomputer", reusing ideas from SoC design, but this time with out-of-chip network "on-board", and out-of-the-shelf processor elements organized as an array. The network itself should be time predictable and highly parallel (far more than PCI-e for instance).

8.2.3. Investissements d'Avenir

8.2.3.1. DEPARTS

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo, Cristian Maxim.

This project is funded by the BGLE Call (*Briques Logicielles pour le Logiciel Embarqué* of the national support programme *Investissements d'Avenir*. Formally started on October 1st, 2012, but the kick-off meeting was only held on April, 2013 for administrative reasons. Initially this contract was handled by the TRIO team in Nancy, but at this end of TRIO moved to Aoste Rocquencourt with the people involved. Research will target solutions for probabilistic component-based models, and a Ph.D. thesis will start early 2014 on this topic. The goal is to allow designers to unify in a common framework probabilistic scheduling techniques with compositional assume/guarantee contracts that have different levels of criticality. Our contribution is based on the schedulability analysis presented in [39].

8.3. European Initiatives

8.3.1. FP7 Projects

8.3.1.1. PROXIMA

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo, Cristian Maxim.

Type: COOPERATION
Defi: Mixed-Criticality Systems
Instrument: Integrated Project
Objectif: Development of probabilistic approaches for mixed-criticality systems on multi-core and many-core platforms
Duration: October 2013 - September 2016
Coordinator: Barcelona Supercomputing Center (Spain)
Inria contact: Liliana Cucu-Grosjean PROXIMA started on October 1st, 2013 with a kick-off meeting in November 2013.

The project claims that probabilistic analysis techniques can provide efficient (tractable) and effective (tight) analysis of the temporal behaviour of complex mixed-criticality applications, while running on novel multicore and manycore platforms. Solid research results from the former FP7 STREP PROARTIS project sustain this claim. The concept is based on using probabilistic analysis techniques to derive safe and tight bounds on the temporal behaviour of applications,. Such bounds should reflect requirements on failure rates commensurate with their criticality.
PROXIMA defines architectural paradigms that break causal dependence in the timing behaviour of execution components at hardware and software level that can give rise to pathological cases. The risk is then reduced to quantifiably small levels. The changes needed in the hardware and software components beneath the application (processing cores, interconnects, memory hierarchies and controllers, real-time operating system, middleware, compilers) remain modest.

8.3.2. Collaborations in European Programs, except FP7

8.3.2.1. ARTEMIS PRESTO

Participants: Frédéric Mallet, Arda Goknil, Julien Deantoni, Marie-Agnès Peraldi Frati, Robert de Simone, Jean-Vivien Millo.

Type: ARTEMIS
Project title: PRESTO
Duration: April 2011 - March 2014
Coordinator: Miltech (Greece)
Others partners: TELETEL S.A. (Greece), THALES Communications (France), Rapita Systems Ltd. (United Kingdom), VTT (Finland), Softeam (France), THALES (Italy), MetaCase (Finland), Inria (France), University of LâAquila (Italy), MILTECH HELLAS S.A (Greece), PragmaDev (France), Prismtech (United Kingdom), Sarokal Solutions (Finland).
See also: http://www.cesarproject.eu/
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.

8.4. International Initiatives

8.4.1. Inria Associate Teams

8.4.1.1. DAESD

Title: Distributed/Asynchronous and Embedded/synchronous Systems Development

Inria principal investigator: Robert de Simone (Aoste) / Eric Madelaine (Oasis)

International Partner (Institution - Laboratory - Researcher):

East China Normal University (China) - SEI-Shone - Robert De Simone

Duration: 2012 - 2014

See also: https://team.inria.fr/DAESD/

The development of concurrent and parallel systems has traditionally been clearly split in two different families: distributed and asynchronous systems on one hand, now growing very fast with the recent progress of the Internet towards large scale services and clouds; embedded, reactive, or hybrid systems on the other hand, mostly of synchronous behaviour. The frontier between these families has attracted less attention, but recent trends, e.g. in industrial systems, in Cyber-Physical systems (CPS), or in the emerging Internet of Things, give a new importance to research combining them.
The aim of the DAESD associate team is to combine the expertise of the Oasis and Aoste teams at Inria, the SEI-Shone team at ECNU-Shanghai, and to build models, methods, and prototype software tools inheriting from synchronous and asynchronous models. We plan to address modelling formalisms and tools, for this combined model; to establish a method to analyze temporal and spatial consistency of embedded distributed real-time systems; to develop scheduling strategies for multiple tasks in embedded and distributed systems with mixed constraints.
A dedicated Spring School was organized this year in Shanghai (April 27-30th), with participation of Robert de Simone and Frédéric Mallet from Aoste.

8.4.2. Inria International Labs

8.4.2.1. LIAMA

The DAESD associated-team goals have been extended to a LIAMA project named HADES (Heterogeneous Asynchronous Distributed / Embedded Synchronous), again with the SEI-Shone lab of ECNU Shanghai. The kick-off meeting was held next to the thematic Spring School (see 8.4.1.1), in presence of Chinese and French officials.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Internships

Franco Pestarini

Subject: Threads scheduling on multicore processors

Date: from Feb 2013 until Jul 2013

Institution: Universidad National de Rosario (Argentina)

CONVECS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. FSN (Fonds national pour la Société Numérique)

8.1.1.1. OpenCloudware

Participants: Rim Abid, Hugues Evrard, Frédéric Lang, Gwen Salaün [correspondent], Lina Ye.

OpenCloudware [10] is a project funded by the FSN. The project is led by France Telecom / Orange Labs (Meylan, France) and involves 18 partners (among which Bull, OW2, Thalès, Inria, etc.). OpenCloudware aims at providing an open software platform enabling the development, deployment and administration of cloud applications. The objective is to provide a set of integrated software components for: (i) modelling distributed applications to be executed on cloud computing infrastructures; (ii) developing and constructing multi-tier virtualized applications; and (iii) deploying and administrating these applications (PaaS platform) possibly on multi-IaaS infrastructures.

OpenCloudware started in January 2012 for three years and nine months. The main contributions of CONVECS to OpenCloudware (see § 6.5.3) are the formal specification of the models, architectures, and protocols (self-deployment, dynamic reconfiguration, self-repair, etc.) underlying the OpenCloudware platform, the automated generation of code from these specifications for rapid prototyping purposes, and the formal verification of the aforementioned protocols.

8.1.1.2. Connexion

Participants: Hubert Garavel [correspondent], Frédéric Lang, Raquel Oliveira.

Connexion [11] (*COntrôle commande Nucléaire Numérique pour l'EXport et la rénovatION*) is a project funded by the FSN, within the second call for projects "*Investissements d'Avenir — Briques génériques du logiciel embarqué*". The project, led by EDF and supported by the *Pôles de compétitivité* Minalogic, Systematic, and *Pôle Nucléaire Bourgogne*, involves many industrial and academic partners, namely All4Tech, Alstom Power, ArevA, Atos Worldgrid, CEA-LIST, CNRS/CRAN, Corys Tess, ENS Cachan, Esterel Technologies, Inria, LIG, Predict, and Rolls-Royce. Connexion aims at proposing and validating an innovative architecture dedicated to the design and implementation of control systems for new nuclear power plants in France and abroad.

Connexion started in April 2012 for four years. In this project, CONVECS will assist another LIG team, IIHM, in specifying human-machines interfaces formally using the LNT language and in verifying them using CADP (see § 6.5.6).

8.1.2. Competitivity Clusters

8.1.2.1. Bluesky for I-Automation

Participants: Hubert Garavel, Fatma Jebali, Jingyan Jourdan-Lu, Frédéric Lang, Eric Léo, Radu Mateescu [correspondent].

Bluesky for I-Automation is a project funded by the FUI (*Fonds Unique Interministériel*) within the *Pôle de Compétitivité* Minalogic. The project, led by Crouzet Automatismes (Valence), involves the SMEs (*Small and Medium Enterprises*) Mootwin and VerticalM2M, the LCIS laboratory of Grenoble INP, and CONVECS. Bluesky aims at bringing closer the design of automation applications and the Internet of things by providing an integrated solution consisting of hardware, software, and services enabling a distributed, Internet-based design and development of automation systems. The automation systems targeted by the project are networks of programmable logic controllers, which belong to the class of GALS (*Globally Asynchronous, Locally Synchronous*) systems.

[10] http://www.opencloudware.org
[11] http://www.cluster-connexion.fr

Bluesky started in September 2012 for three years. The main contributions of CONVECS to Bluesky (see § 6.5.4) are the definition of GRL, the formal pivot language for describing the asynchronous behaviour of logic controller networks, and the automated verification of the behaviour using compositional model checking and equivalence checking techniques.

8.1.3. Other National Collaborations

Additionally, we collaborated in 2013 with the following Inria project-teams:

- OASIS (Inria Sophia-Antipolis – Méditerranée): Eric Madelaine and Ludovic Henrio,
- TRISKELL (Inria Rennes – Bretagne Atlantique): Kevin Corre and Axel Legay,
- MEXICO (Inria Saclay – Île-de-France): Alban Linard.

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

- Gaëlle Calvary and Sophie Dupuy-Chessa (LIG, Grenoble),
- Fabrice Kordon and Lom Messan Hillah (LIP6, Paris),
- Alexandre Hamez and Jérôme Hugues (ISAE, Toulouse),
- Noël De Palma and Fabienne Boyer (LIG, Grenoble),
- Xavier Etchevers (Orange Labs, Meylan),
- Matthias Güdemann (Systerel, Aix-en-Provence),
- Meriem Ouederni (IRIT, Toulouse),
- Pascal Poizat (LIP6, Paris).

H. Garavel, F. Lang, and R. Oliveira attended two training days on the Scade and Scade Display software (given by Luc Coyette, Esterel Technologies) on March 6 and 24, 2013.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. SENSATION

Participants: Hubert Garavel [correspondent], Radu Mateescu, Wendelin Serwe.

SENSATION [12] (*Self ENergy-Supporting Autonomous computaTION*) is a European project no. 318490 funded by the FP7-ICT-11-8 programme. It gathers 9 participants: Inria (TRISKELL and CONVECS project-teams), Aalborg University (Denmark), RWTH Aachen and Saarland University (Germany), University of Twente (The Netherlands), GomSpace (Denmark), and Recore Systems (The Netherlands). The main goal of SENSATION is to increase the scale of systems that are self-supporting by balancing energy harvesting and consumption up to the level of complete products. In order to build such Energy Centric Systems, embedded system designers face the quest for optimal performance within acceptable reliability and tight energy bounds. Programming systems that reconfigure themselves in view of changing tasks, resources, errors, and available energy is a demanding challenge.

SENSATION started on October 1st, 2012 for three years. CONVECS contributes to the project regarding the extension of formal languages with quantitative aspects, studying common semantic models for quantitative analysis, and applying formal modeling and analysis to the case studies provided by the industrial partners.

The case study on rescaling video for handheld devices, proposed initially by STMicroelectronics, was abandoned in 2013 after the departure of this partner from the project. Therefore, we oriented our efforts on the EnergyBus case study (see § 6.5.5), in collaboration with Saarland University.

[12] http://sensation-project.eu/

8.2.2. Collaborations with Major European Organizations

The CONVECS project-team is member of the FMICS (*Formal Methods for Industrial Critical Systems*) working group of ERCIM [13]. R. Mateescu is currently the chairman of the FMICS working group and H. Garavel is member of the FMICS board, in charge of dissemination actions.

H. Garavel was appointed to a new Working Group within Informatics Europe: "*Parallel Computing (Supercomputing) Education in Europe: State-of-Art*". This is a relatively small working group (about 10 people) with the following missions: to show the need for urgent changes in higher education in the area of computational sciences, to compose a survey of the current landscape of parallel computing and supercomputing education in Europe with respect to different universities and countries, and to prepare a set of recommendations on how to bring ideas of parallel computing and supercomputing into higher educational systems of European countries.

8.2.3. Other European Collaborations

In addition to our partners in aforementioned contractual collaborations, we had scientific relations in 2013 with several European universities and research centers, including:

- Saarland University (Alexander Graf-Brill and Holger Hermanns),
- RWTH Aachen (Joost-Pieter Katoen),
- Oxford University (Ernst-Moritz Hahn and Marta Kwiatkowska),
- University of Birmingham (Dave Parker),
- Technical University of Eindhoven (Anton Wijs),
- University of Twente (Marieke Huisman and Jaco van de Pol),
- University of Málaga (Francisco Duran and Ernesto Pimentel).

Our partnership with Saarland University was sustained by the Humboldt Forschungspreis received by H. Garavel, who continued his regular visits to Saarland University.

8.3. International Initiatives

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.

8.3.1. Other International Collaborations

We had sustained scientific relations with Tevfik Bultan (University of California at Santa Barbara, USA).

We also had scientific exchanges with Gianfranco Ciardo (University of California at Riverside, USA).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Loïg Jezequel (Technical University of München, Germany) visited us on March 4–6, 2013. He gave a talk entitled "*Distributed Cost-Optimal Planning*" on March 4, 2013.
- Zhen Zhang (University of Utah, USA) visited us from September 1st to December 31, 2013.
- The annual CONVECS seminar was held in Col de Porte (France) on November 18–20, 2013. The following invited scientists attended the seminar:
  - Jérôme Hugues (Institute for Space and Aeronautics Engineering, Toulouse) gave on November 18, 2013 a talk entitled "*Model-Based, Model Checking: the Missing Bits*".

[13] http://fmics.inria.fr

- Loïg Jezequel (Technical University of München, Germany) gave on November 19, 2013 a talk entitled "*Computation of Summaries using Net Unfoldings*".
- Xavier Etchevers (Orange Labs, Meylan, France) gave on November 19, 2013 a talk entitled "*VAMP: Self-Deployment of Arbitrary Applications in the Cloud*".
- Fabrice Kordon (LIP6, Paris) gave on November 20, 2013 a talk entitled "*Verification Approaches for Distributed Systems in LIP6/MoVe*".
- Zhen Zhang (University of Utah, USA) gave on November 20, 2013 a talk entitled "*Modeling a Fault-Tolerant Wormhole Routing Algorithm using LNT*".

Hycomes Team

6. Partnerships and Cooperations

6.1. Regional Initiatives

- Ayman Aljarbooh's PhD is partially funded by a ARED grant of the Brittany Regional Council.
- Benoît Caillaud is participating to the S3PM project of the CominLabs excellence laboratory [10]. This project focuses on the computation of surgical procedural knowledge models from recordings of individual procedures, and their execution [7]. The objective is to develop an enabling technology for procedural knowledge based computer assistance of surgery. In this project, we demonstrate its potential added value in nurse and surgeon training.

6.2. National Initiatives

Program:« Briques génériques du logiciel embarqué » (Embedded Software Generic Building-Blocks)

Project acronym: Sys2soft

Project title: Physics Aware Software

Duration: June 2012 – April 2016

Coordinator: Dassault Systèmes (France)

Other partners: Thales TGS / TRT / TAS, Alstom Transport, Airbus, DPS, Obeo, Soyatec

Abstract: The Sys2soft project aims at developping methods and tools supporting the design of embedded software interacting with a complex physical environment. The project advocates a methodology where both physics and software are co-modeled and co-simulated early in the design process and embedded code is generated automatically from the joint physics and software models. Extensions of the Modelica language with synchronous programming features are being investigated, as a unified framework where interacting physical and software artifacts can be modeled.

6.3. European Initiatives

6.3.1. Collaborations in European Programs, except FP7

Program: ITEA2

Project acronym: Modrio

Project title: Model Driven Physical Systems Operation

Duration: September 2012 – November 2015

Coordinator: EDF (France)

Other partners: ABB (Sweden), Ampère Laboratory / CNRS (France), Bielefeld University (Germany), Dassault Systèmes (Sweden), Dassault Aviation (France), DLR (Germany), DPS (France), EADS (France), Equa Simulation (Sweden), IFP (France), ITI (Germany), Ilmenau University (Germany), Katholic University of Leuven (Belgium), Knorr-Bremse (Germany), LMS (France and Belgium), Linköping University (Sweden), MathCore (Sweden), Modelon (Sweden), Pöry (Finland), Qtronic (Germany), SICS (Sweden), Scania (Sweden), Semantum (Finland), Sherpa Engineering (France), Siemens (Germany and Sweden), Simpack (Germany), SKF (Sweden), Supmeca (France), Triphase (Belgium), University of Calabria (Italy), VTT (Finland), Vattenfall (Sweden), Wapice (Finland).

[10] http://www.cominlabs.ueb.eu/projects/

Abstract: Modelling and simulation are efficient and widely used tools for system design. But they are seldom used for systems operation. However, most functionalities for system design are beneficial for system operation, provided that they are enhanced to deal with real operating situations. Through open standards the benefits of sharing compatible information and data become obvious: improved cooperation between the design and the operation communities, easier adaptation of operation procedures wrt. design evolutions. Open standards also foster general purpose technology. The objective of the ITEA 2 MODRIO project is to extend modelling and simulation tools based on open standards from system design to system operation.

6.4. International Initiatives

6.4.1. Informal International Partners

Beyond the Modrio and Sys2soft collaborative projects, we have an informal but sustained collaboration with the Dassault Systèmes team developping the Dymola tool, located in Lund, Sweden, and with the DLR in Munich, Germany, which are both prominent actors of the Modelica association. This collaboration has allowed us to have an impact on the recent evolution of the Modelica language: Version 3.3 of the language integrates several of our contributions related to the introduction of language constructs inherited from synchronous programming languages [11].

[11] See acknowledgements in section E.1.3, page 261 of https://www.modelica.org/documents/ModelicaSpec33.pdf

MUTANT Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. INEDIT

Title: Interactivity in the Authoring of Time and Interactions

Project acronym: INEDIT

Type: ANR Contenu et Interaction 2012 (CONTINT)

Instrument: ANR Grant

Duration: September 2012 - September 2015

Coordinator: IRCAM (France)

Other partners: Grame (Lyon, France), LaBRI (Bordeaux, France).

Abstract: The INEDIT project aims to provide a scientific view of the interoperability between common tools for music and audio productions, in order to open new creative dimensions coupling *authoring of time* and *authoring of interaction*. This coupling allows the development of novel dimensions in interacting with new media. Our approach lies within a formal language paradigm: An interactive piece can be seen as a virtual interpreter articulating locally synchronous temporal flows (audio signals) within globally asynchronous event sequence (discrete timed actions in interactive composition). Process evaluation is then to respond reactively to signals and events from an environment with heterogeneous actions coordinated in time and space by the interpreter. This coordination is specified by the composer who should be able to express and visualize time constraints and complex interactive scenarios between mediums. To achieve this, the project focuses on the development of novel technologies: dedicated multimedia schedulers, runtime compilation, innovative visualization and tangible interfaces based on augmented paper, allowing the specification and realtime control of authored processes. Among posed scientific challenges within the INEDIT project is the formalization of temporal relations within a musical context, and in particular the development of a GALS (Globally Asynchronous, Locally Synchronous) approach to computing that would bridge in the gap between synchronous and asynchronous constraints with multiple scales of time, a common challenge to existing multimedia frameworks.

8.1.2. Other National Initiatives

The team participated to the CLASYCO network on DSL for simulation, supported by the RNSC (réseau national des systèmes complexes).

Jean-Louis Giavitto participates to the SynBioTIC ANR Blanc project (with IBISC, University of Evry, LAC University of Paris-Est, ISC - Ecole Polytechnique).

8.2. International Initiatives

8.2.1. Inria International Partners

8.2.1.1. Informal International Partners

Miller Puckette (UCSD), David Wessel (UC Berkeley), Edward Lee (UC Berkeley), Shlomo Dubnov (UCSD).

8.3. International Research Visitors

Dr. Roger Dannenberg (Carnegie Mellon University) was invited by MuTant in May 2013, where he took part in Arshia Cont's HDR defense, José Echeveste's mid-term PhD defense, and gave a public seminar in the MuTant Seminars in Real-time Multimedia Computing series.

Dr. Shlomo Dubnoc (University of California San Diego) was invited by MuTant in August 2013 for ongoing collaborative work and to take part in the International Conference on Geometric Science of Information 2013, Special Session on *Audio and Music* organized by MuTant member Arshia Cont.

Masahiko Sakai visited MuTant for two weeks in August 2013. He is a professor at the University of Nagoya and director of the Sakabe/Sakai computer science laboratory of the department of computer science and mathematical informatics of Nagoya University.

Dr. Edward Lee and Dr. David Wessel (UC Berkeley) visited MuTant for discussions on future collaborations with MuTant around Cyber-Physical Systems.

PARKAS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

ANR WMC project (program “jeunes chercheuses, jeunes chercheurs”), 2012–2016, 200 Keuros. F. Zappa Nardelli is the main investigator.

ANR Boole project (program “action blanche”), 2009-2014.

ANR Partout (program “defis”), 2009-2012. Louis Mandel and Marc Pouzet.

ANR CAFEIN, 2013-2015. Marc Pouzet.

Action d’envergure Synchronics, 2008-2012. The action was driven by Alain Girault (Inria, PopArt, Grenoble) and Marc Pouzet (Inria, Parkas, Paris-Rocquencourt), to focus on “langages for embedded systems”. This has been instrumental in driving our new research on hybrid system modelers.

8.1.2. Competitivity Clusters

FUI project OpenGPU, 2008–2012.

8.1.3. Investissements d’avenir

Sys2Soft contract (Briques Génériques du Logiciel Embarqué). Partenaire principal: Dassault-Systèmes, etc. Inria contacts are Benoit Caillaud (HYCOMES, Rennes) and Marc Pouzet (PARKAS, Paris).

ManycoreLabs contract (Briques Génériques du Logiciel Embarqué). Partenaire principal: Kalray. Inria contacts are Albert Cohen (PARKAS, Paris) and Alain Darte (COMPSYS, Lyon).

8.1.4. Others

Marc Pouzet is scientific advisor for the Esterel-Technologies/ANSYS company.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. TETRACOM

Type: CAPACITIES

Defi: Alternative Paths to Components and Systems

Instrument: Coordination and Support Action

Objectif: Advanced Computing, embedded and Control systems

Duration: September 2013 – August 2016

Coordinator: Rainer Leupers

Partner: RWTH Aachen (Germany)

Inria contact: Albert Cohen

Abstract: coordination action to support bilateral technology transfer partnerships (TTPs); prototype of future H2020 transfer instruments.

8.2.1.2. COPCAMS

Type: ARTEMIS

Defi: Alternative Paths to Components and Systems

Instrument: ASP

Objectif: NC

Duration: April 2013 – March 2016

Coordinator: Christian Fabre

Partner: CEA Leti (Grenoble)

Inria contact: Albert Cohen

Abstract: cognitive/smart cameras enabled by hardware accelerators, including manycore processors (STHORM platform of ST) and GPUs.

8.2.2. Collaborations in European Programs, except FP7

8.2.2.1. MODRIO

Duration: December 2012 - December 2014

Coordinator: EDF

Partner: Dassault-Systèmes, EDF, Institut Francais du Pétrole, DLR (Munich, Germany), LMS-Imagine, Inria.

Inria contact: Benoit Caillaud (HYCOMES, Rennes); Marc Pouzet (PARKAS, Paris)

8.3. International Initiatives

8.3.1. Inria Associate Teams

8.3.1.1. POLYFLOW

Title: Polyhedral Compilation for Data-Flow Programming Languages

Inria principal investigator: Albert Cohen

International Partner (Institution - Laboratory - Researcher):

IISc Bangalore (India) - Department of Computer Science and Automation - Albert Cohen

Duration: 2013 - 2016

See also: http://polyflow.gforge.inria.fr

Polyhedral techniques for program transformation are now used in several proprietary and open source compilers. However, most of the research on polyhedral compilation has focused on imperative languages such as C, where computation is specified in terms of statements with zero or more nested loops and other control structures around them. Graphical data-flow languages, where there is no notion of statements or a schedule specifying their relative execution order, have so far not been studied using a powerful transformation or optimization approach. These languages are extremely popular in system analysis, modeling and design, in embedded reactive control. They also underline the construction of many domain-specific languages and compiler intermediate representations. The copy and execution semantics of data-flow languages impose a different set of challenges. We plan to bridge this gap by studying techniques that could enable extraction of a polyhedral representation from data-flow programs, transform them, and synthesize them from their equivalent polyhedral representation.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

We have regular invited professors in the PARKAS team:

- In 2012, one month (June/July), Prof. Stephen Edwards (Columbia Univ., New York, USA).
- In 2013, one month (June), Prof. Mary Sheeran from (Chalmers Univ., Sweden).

8.4.1.1. Internships

Pankaj Prateek, Anirudh Kumar, and Pankaj More, students at IIT Kanpur, India, worked in the Parkas team under the supervision of Francesco Zappa Nardelli from 4th May, 2013 to 23 July, 2013.

Guillaume Chelfi, student at Telecom Paris and the MPRI program, under the supervision of Francesco Zappa Nardelli and Marc Pouzet, from 1st of March, 2013, to 31st July, 2013. Guillaume Chelfi worked on the formal verification of the translation of synchronous programs to sequential code.

Louis Mandel supervised the 5-months MPRI Internship of Louis Jachiet from April to August. Louis Jachiet worked on the static scheduling of ReactiveML programs.

Albert Cohen supervised the 3-months Internship of Vincent Thiberville, 3rd year student at École Polytechnique, from April to June. Vincent conducted experimental studies and proposed enhanced methods to support array-based computations in the Heptagon synchronous language.

8.4.2. Visits to International Teams

October, Louis Mandel spent 2 weeks in the team of Vijay Saraswat at IBM T.J. Watson. He worked on the type system of the X10 language.

SPADES Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR Projects

8.1.1.1. PiCoq (ANR project)

Participants: Barbara Petit, Jean-Bernard Stefani.

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

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

The project partners include Inria (CELTIQUE and SPADES teams), LIP (PLUME team), and Université de Savoie. The project runs from November 2010 to October 2014.

8.1.1.2. REVER (ANR project)

Participants: Barbara Petit, Jean-Bernard Stefani.

The REVER project aims to develop semantically well-founded and composable abstractions for dependable distributed computing on the basis of a reversible programming model, where reversibility means the ability to undo any program execution and to revert it to a state consistent with the past execution. The critical assumption behind REVER is that by combining reversibility with notions of compensation and modularity, one can develop systematic and composable abstractions for dependable programming.

The REVER work program is articulated around three major objectives:

- To investigate the semantics of reversible concurrent processes.
- To study the combination of reversibility with notions of compensation, isolation and modularity in a concurrent and distributed setting.
- To investigate how to support these features in a practical (typically, object-oriented and functional) programming language design.

The project partners are Inria (FOCUS and SPADES teams), Université de Paris VII (PPS laboratory), and CEA (List laboratory). The project runs from December 2011 to November 2015.

8.2. International Initiatives

8.2.1. Inria Associate Teams

8.2.1.1. RIPPES

Title: RIgorous Programming of Predictable Embedded Systems

Inria principal investigator: Alain Girault

International Partner (Institution - Laboratory - Researcher):

University of California Berkeley (USA) – EECS Department, PTOLEMY group – Prof. Edward Lee.

University of Auckland (New Zealand) – ECE Department – Prof. Partha Roop.

Duration: January 2013 – December 2015

See also: https://wiki.inria.fr/rippes/Main_Page

The RIPPES associated team gathers the SPADES team from Inria Grenoble, the Ptolemy group from UC Berkeley (EECS Department), and the Embedded Systems Research group from U. of Auckland (ECE Department). The planned research seeks to reconcile two contradictory objectives of embedded systems, more predictability and more adaptivity. We propose to address these issues by exploring two complementary research directions: (1) by starting from a classical concurrent C or Java programming language and enhancing it to provide more predictability, and (2) by starting from a very predictable model of computation (SDF) and enhancing it to provide more adaptivity.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

- January and February 2013: Ismail Assayad (Ass. Prof. U. Casablanca) visited Inria Grenoble to work on multi-criteria optimisation and scheduling for embedded system.
- March 2013: Eugene Yip (PhD student, U. Auckland) visited Inria Grenoble to work on the semantics of the FOREC PRET programming language (RIPPES associated team).
- March 2013: Hokeun Kim (PhD student, UC Berkeley) visited Inria Grenoble to work on the RIPPES associated team.
- March 2013: Partha Roop (Senior Lecturer, U. Auckland) visited Inria Grenoble to work on the FOREC PRET programming language (RIPPES associated team).
- July 2013: Eugene Yip (PhD student, U. Auckland) visited Inria Grenoble to work on the semantics of the FOREC PRET programming language (RIPPES associated team).
- July 2013: Matthew Kuo (PhD student, U. Auckland) visited Inria Grenoble to work on tickpad memories for PRET programs (RIPPES associated team).
- December 2013: Chris Shaver (PhD student, UC Berkeley) visited Inria Grenoble to work on parametric data-flow models of computation (RIPPES associated team).

8.3.2. Visits to International Teams

- Vagelis Bebelis visited the University of California Berkeley (USA) in October 2013 to work on a parametric dataflow models of computation and on its implementation within the Ptolemy II framework.

8.3.3. Inria International Partners

8.3.3.1. Informal International Partners

We have a long lasting informal collaboration with Prof. Ivan Lanese (U. Bologna, Italy) on component programming and reversability. He visits the team regularly.

We have a long lasting informal collaboration with Prof. Ismail Assayad (U. Casablanca, Morocco) and Prof. Hamoudi Kalla (U. Batna, Algeria) on fault-tolerant embedded systems, multi-criteria optimization, reliability, and power consumption. They both visit the team regularly.

FORMES Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. Tsinghua Grant

contract: Tsinghua National Laboratory for Information Science and Technology, Cross-discipline Foundation grant 2011-9

title: An Intensional Logical Framework and Its Implementation

Participants: Jean-Pierre Jouannaud, Jianqi Li

duration: 2011 - 2012

Amount: 100,000 RMB

7.1.2. NSFC Grant

contract: National Science Foundation of China grant 61272002

title: The meta-theories of higher-order rewriting and their proof automation: toward the next generation theorem prover

PIs: Jean-Pierre Jouannaud, Jianqi Li

duration: 2013-2016

Amount: 600,000 RMB

7.2. International Initiatives

7.2.1. Inria International Partners

7.2.1.1. Declared Inria International Partners

The FORMES project has been held since the beginning at Tsinghua University, Beijing, China. Tsinghua University is a founding member of LIAMA laboratory.

7.2.1.2. Informal International Partners

The FORMES project has also collaborated with:

- Pr John Koo at Shenzhen Institute of Advanced Technology, until August 2013.
- the Institute of Software of the Chinese Academy of Science where Frédéric Blanqui has been kindly hosted between July 2012 and August 2013.

7.2.2. Inria International Labs

FORMES is one of the LIAMA projects.

7.2.3. Participation In other International Programs

LIAMA is a member of the AURA network: Association of Units of Research in Asia.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

FORMES project member Jean-Pierre Jouannaud organized jointly with Pr Ming Gu the LIAMA-Tsinghua Software Day, where the following scientists reported on their research:

- Pr Edmund Clarke, from Carnegie Mellon.
- Erik Hagersten from University of Uppsala.
- Marc Pouzet from University Pierre et Marie Curie.

7.3.1.1. Internships

- *Jiaxiang Liu*
  - Subject: Diagramatic Confluence,
  - Date: from Jul 2013 to Dec 2013,
  - Institution: Ecole Polytechnique
- *Antoine Rouquette*
  - Subject: Upgrade of SimSoC simulator,
  - Date: from September 2012 to August 2013,
  - Institution: Shenzhen Institutes of Advanced Technology
- *Shenpeng Wang*
  - Subject: Approximately Timed Simulation of PowerPC e200z,
  - Date: from March 2012 to May 2013,
  - Institutions: Tsinghua University and Shenzhen Institutes of Advanced Technology

SECSI Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- ANR programme blanc CPP ("Confidence, Probability, and Proofs"), 2009-April 2013. Partners: LSV (scientific leader), CEA LIST (co-leader), Inria (Comète, Parsifal), Ecole Supérieure d'Electricité (L2S, SSE). External partners: Safran, Dassault Systèmes.

  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.

- ANR VERSO program ProSe ("Proofs of Security"), 2010-2014. Partners: Inria (Cascade, leader; Cassis), LSV, Verimag.

  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.

- ANR JCJC project VIP, 2012-2015. Awarded to Stéphanie Delaune.

  The aim of this project is to formally analyze modern applications in which privacy plays an important role. Many applications having an important societal impact are concerned by privacy, e.g. electronic voting, electronic auction protocols, RFID tags, safety critical application in vehicular ad hoc networks, routing protocols in mobile ad hoc networks, etc. Moreover, each application comes with its own specificities. E.g. e-voting protocols often rely on complex cryptographic primitives, some routing protocols rely on recursive tests, and so on. In mobile ad hoc networks, taking into account mobility issues is also an important challenge.

  Because security protocols are notoriously difficult to design and analyse, formal verification techniques are extremely important. However, nearly all studies focus on trace-based security properties, and thus to not allow one to analyse privacy-type properties that play an important role in many modern applications. Moreover, the envisioned applications have some specificities that prevent them to be modelled in an accurate way with existing verification tools.

  The goal of this project is to design verification algorithms to analyse privacy-type properties on several applications having an important societal impact. The project is accompanied by an effort in case studies and application domains which will allow at the end of the project an assessment of the pragmatic potential both in terms of modelling and effective analysis. More details are available on the web page of the project: http://www.lsv.ens-cachan.fr/Projects/anr-vip/.

- Inria-DGA contract, on evaluation of the Orchids tool. This is a 3-year contract, starting in April 2013, on the evaluation and improvement of the Orchids intrusion detection tool. The actual contents of the contract is not public.

7.2. International Initiatives

7.2.1. Inria International Partners

7.2.1.1. Informal International Partners

- Mark D. Ryan, U. Birmingham
- Alwen Tiu, Australian National University
- Achim Jung, U. Birmingham
- Frédéric Mynard, Georgia Southern University
- Roberto Segala, U. Verona
- Dominique Unruh, U. Tallinn

7.2.2. Participation In other International Programs

- Inria Project Lab CAPPRIS (Collaborative Action on the Protection of Privacy Rights in the Information Society). Member: Stéphanie Delaune.

  The goal of CAPPRIS is to provide solutions to enhance the privacy protection in the Information Society. The targeted applications are Online Social Networks, Location Based Services, and Electronic Health Record Systems.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

- Dominique Unruh, Tallinn, 1 month, January 2013.
- Mark Ryan, Birmingham, 2 weeks, July 2013.
- Achim Jung, Birmingham, 1 month, April-May 2013.

7.3.1.1. Internships

Stéphanie Delaune et David Baelde co-supervised the following master student:

- Lucca Hirschi, ENS Lyon, “Réduction d’ordre partiel pour les propriétés d’équivalence”, 2013.

Jean Goubault-Larrecq supervised the following L2 student:

- Jean-Philippe Lachance, U. Laval, Québec, “Evaluation automatique de la complexité de détection des signatures Orchids”, 2013.

ABSTRACTION Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

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. We set out to develop a generic static analyzer based on abstract interpretation for the C language, along with a number of advanced abstract domains and domain combination operators, and prove the soundness of this analyzer using the Coq proof assistant. Likewise, we will continue our work on the CompCert C formally-verified compiler, the first realistic C compiler that has 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. FP7 Projects

8.2.1.1. MemCad

Type: IDEAS

Defi: Design Composite Memory Abstract Domains

Instrument: ERC Starting Grant

Objectif: Design Composite Memory Abstract Domains

Duration: October 2011 - September 2016

Coordinator: Inria (France)

Partner: None

Inria contact: Xavier Rival

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 to 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. Informal International Partners

Research on Kappa and its applications involves several close international partners:

- Vincent Danos (University of Edinburgh, UK);
- Walter Fontana (Harvard Medical School, US);
- Hein Koeppl and Tatjana Petrov (ETH Zürich, SW);
- Jonathan Hayman and Glynn Winskel (Cambridge, UK).

Research on abstract domains for memory states involves the group of Bor-Yuh Evan Chang (University of Colorado at Boulder, Colorado, USA).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Bor-Yuh Evan Chang visited the team from June to August 2013, as part of his collaboration with Xavier Rival.

8.4.1.1. Internships

Abdellatif Atki is a student at École Polytechnique (Palaiseau, France). He performed his M1 internship from April 2013 to July 2013 under the supervision of Antoine Miné on the Two variables per inequality abstract domain [27].

Matthias Bry is a student at École Polytechnique (Palaiseau, France). He performed his M1 internship from April 2013 to July 2013 under the supervision of Antoine Miné on analysis of concurrent programs [28].

Huisong Li is a master student at the Institute of Software, at the Chinese Accademy of Sciences (Beijing, China) and is doing a research internship under the supervision of Xavier Rival.

8.4.2. Visits to International Teams

Xavier Rival visited the ROSAEC Team in Seoul National University (team of Professor Kwangkeun Yi).

CELTIQUE Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

The Celtique team collaborates with DGA-MI, a research laboratory belonging to the French army, and located in Rennes. The collaboration has several facets.

- We run a joint bi-monthly seminar on Security and Formal Methods. This seminar attracts attendance from academia and industry.
- DGA-MI is funding a PhD thesis, supervised jointly, on code obfuscation.
- Colas Le Guernic, a DGA-MI researcher, is external collaborator of Celtique on our activities on analysis of binary code.

7.2. National Initiatives

7.2.1. The PiCoq ANR project

Participants: Alan Schmitt, Petar Maksimovic.

Process calculi, Verification, Proof Assistants

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

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

The project partners include Inria, LIP, and Université de Savoie. The project runs from November 2010 to October 2014.

7.2.2. The ANR VERASCO project

Participants: Sandrine Blazy, Delphine Demange, Vincent Laporte, André Oliveira Maroneze, David Pichardie.

Static program analysis, Certified static analysis

The VERASCO project (2012–2015) is funded by the call ISN 2011, a program of the Agence Nationale de la Recherche. It investigates the formal verification of static analyzers and of compilers, two families of tools that play a crucial role in the development and validation of critical embedded software. It is a joint project with the Inria teams ABSTRACTION, GALLIUM, The VERIMAG laboratory and the Airbus company.

7.2.3. The ANR Binsec project

Participants: Frédéric Besson, Sandrine Blazy, Pierre Wilke.

Binary code, Static program analysis

The Binsec project (2013–2017) is founded by the call ISN 2012, a program of the Agence Nationale de la Recherche. The goal of the BINSEC project is to develop static analysis techniques and tools for performing automatic security analyses of binary code. We target two main applicative domains: vulnerability analysis and virus detection.

Binsec is a joint project with the Inria CARTE team, CEA LIS, VERIMAG, EADS IW and VUPEN SECURITY. ABSTRACTION, The VERIMAG laboratory and the Airbus company.

7.2.4. Labex COMIN Labs Seccloud project

Participants: Frédéric Besson, Nataliia Bielova, Thomas Jensen, Alan Schmitt, Martin Bodin.

The SecCloud project, started in 2012, will provide a comprehensive language-based approach to the definition, analysis and implementation of secure applications developed using Javascript and similar languages. Our high level objectives is to enhance the security of devices (PCs, smartphones, ect.) on which Javascript applications can be downloaded, hence on client-side security in the context of the Cloud. We will achieve this by focusing on three related issues: declarative security properties and policies for client-side applications, static and dynamic analysis of web scripting programming languages, and multi-level information flow monitoring.

This is a joint project with Supelec Rennes and Ecole des Mines de Nantes.

7.3. International Initiatives

7.3.1. Inria International Partners

7.3.1.1. Informal International Partners

A strong collaboration is ongoing with researchers from Imperial College (UK) in the setting of the JSCert project (http://jscert.org/). This project aims at really understanding JavaScript by building models of ECMAScript semantics in the Coq proof assistant, and certifying automated logical reasoning tools built on those semantics. We are closely working with Philippa Gardner and Sergio Maffeis. This collaboration has resulted in a large Coq development including a formal semantics for JavaScript and a certified JavaScript interpreter. These results are described in our POPL 2014 paper [24].

In 2013, Martin Bodin, Thomas Jensen, and Alan Schmitt visited Imperial College twice. Daiva Naudziuniene, a PhD student of Philippa Gardner, also did a one month internship in the Celtique team in the setting of this collaboration.

David Pichardie was on sabbatical in 2012, in Jan Vitek's group at Purdue University, Indiana, USA. The strong collaboration is still ongoing, and an Associate Team proposal for 2014-2016 has been submitted in 2013 as part of an Inria International program. The JCert project research aims at verifying the compilation of concurrent managed languages, following the previous outcomes of the informal collaboration – a new memory model for concurrent Java that is more suitable to formal verification [26], as well as refinement-based proof methodology (under submission) that allows to reason compositionally about the atomicity of low-level concurrent code fragments. If the proposal is accepted, David Pichardie would be the Inria principal investigator of the JCert project, and Delphine Demange, Thomas Jensen, and Vincent Laporte will also be active participants.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

7.4.1.1. Internships

Patricio Palladino

Subject: Protection from Web Tracking: Analysis of web browser fingerprints

Date: from Mar 2013 until Apr 2013

Institution: University of Buenos Aires (Argentina)

7.4.2. Visits to International Teams

David Pichardie took a sabbatical year and visited Greg Morrisett's group at Harvard University, Cambridge, USA in 2013. During this sabbatical, he worked on the DARPA SAFE project with Harvard University and UPenn University [17].

DEDUCTEAM Exploratory Action

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR Locali

We are coordinators of the ANR-NFSC contract Locali with the Chinese Academy of Sciences. This year we organized the first Locali workshop in Beijing.

7.1.2. ANR BWare

We are members of the ANR *BWare*, which started on September 2012 (David Delahaye is the national leader of this project). The aim of this project is to provide a mechanized framework to support the automated verification of proof obligations coming from the development of industrial applications using the *B* method. The methodology used in this project consists in building a generic platform of verification relying on different theorem provers, such as first order provers and SMT solvers. We are in particular involved in the introduction of Deduction modulo in the first order theorem provers of the project, i.e. *Zenon* and *iProver*, as well as in the backend for these provers with the use of *Dedukti*.

7.1.3. ANR Tarmac

We are members of the ANR Tarmac, coordinated by Pierre Valarcher, on models of computation.

7.2. International Initiatives

7.2.1. Informal International Partners

Deducteam and the KWARC research group (Jacobs University, Germany), led by Michael Kohlhase, have organized a common workshop in Paris on the 12 of April. This workshop has led to the two tools dk2MMT and MMT2dk, and another workshop is planned on the 2014 year. See the program at http://www.cri.ensmp.fr/people/hermant/deducteam/2013/kwarc-dedukti.html or the webpage of the seminars.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

Hermann Haeusler, Bruno Bruno Lopes and Cecilia Englander, from the University PUC Rio have visited Deducteam.

Ying Jiang from the Institute of software of the Chinese Academy of Sciences has visited Deducteam.

7.3.2. Visits to International Teams

Gilles Dowek has visited the University PUC Rio and the Institute of software of the Chinese Academy of Sciences.

GALLIUM Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR projects

8.1.1.1. BWare

Participants: Damien Doligez, Fabrice Le Fessant, Luca Saiu.

The "BWare" project (2012-2016) is coordinated by David Delahaye at Conservatoire National des Arts et Métiers and funded by the *Ingénierie Numérique et Sécurité* programme of *Agence Nationale de la Recherche*. BWare is an industrial research project that aims to provide a mechanized framework to support the automated verification of proof obligations coming from the development of industrial applications using the B method and requiring high guarantees of confidence.

8.1.1.2. Paral-ITP

Participant: Damien Doligez.

The "Paral-ITP" project (2011-2014) is coordinated by Burkhart Wolff at Université Paris Sud and funded by the *Ingénierie Numérique et Sécurité* programme of *Agence Nationale de la Recherche*. The objective of Paral-ITP is to investigate the parallelization of interactive theorem provers such as Coq and Isabelle.

8.1.1.3. Verasco

Participants: Jacques-Henri Jourdan, Xavier Leroy.

The "Verasco" project (2012-2015) is coordinated by Xavier Leroy and funded by the *Ingéniérie Numérique et Sécurité* programme of *Agence Nationale de la Recherche*. The objective of this 4-year project is to develop and formally verify a static analyzer based on abstract interpretation, and interface it with the CompCert C verified compiler.

8.1.2. FSN BGLE projects

8.1.2.1. ADN4SE

Participants: Damien Doligez, Jael Kriener.

The "ADN4SE" project (2012-2016) is coordinated by the Sherpa Engineering company and funded by the *Briques Génériques du Logiciel Embarqué* programme of *Fonds national pour la Société Numérique*. The aim of this project is to develop a process and a set of tools to support the rapid development of embedded software with strong safety constraints. Gallium is involved in this project to provide tools and help for the formal verification in TLA+ of some important aspects of the PharOS real-time kernel, on which the whole project is based.

8.1.2.2. CEEC

Participants: Thomas Braibant, Xavier Leroy.

The "CEEC" project (2011-2014) is coordinated by the Prove & Run company and also involves Esterel Technologies and Trusted Labs. It is funded by the *Briques Génériques du Logiciel Embarqué* programme of *Fonds national pour la Société Numérique*. The CEEC project develops an environment for the development and certification of high-security software, centered on a new domain-specific language designed by Prove & Run. Our involvement in this project focuses on the formal verification of a C code generator for this domain-specific language, and its interface with the CompCert C verified compiler.

8.1.3. FUI projects

8.1.3.1. Richelieu (FUI)

Participants: Michael Laporte, Fabrice Le Fessant.

The "Richelieu" project (2012-2014) is funded by the *Fonds unique interministériel* (FUI). It involves Scilab Enterprises, U. Pierre et Marie Curie, Dassault Aviation, ArcelorMittal, CNES, Silkan, OCamlPro, and Inria. The objective of the project is to improve the performance of scientific programming languages such as Scilab's through the use of VMKit and LLVM.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. DEEPSEA

Type: IDEAS

Instrument: ERC Starting Grant

Duration: June 2013 - May 2018

Coordinator: Umut Acar

Partner: Inria

Inria contact: Umut Acar

Abstract: the objective of project DEEPSEA is to develop abstractions, algorithms and languages for parallelism and dynamic parallelism, with applications to problems on large data sets.

8.3. International Initiatives

8.3.1. Inria International Labs

Fabrice Le Fessant visited CIRIC (Center of Excellence on TIC, created by Inria in Chile) during two weeks. He gave several lectures on OCaml: a presentation at StarTechConf'2013, a presentation at University Adolfo Ibañez, and a presentation and a lecture at University of Chile.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Olin Shivers, professor at Northeastern University (Boston), visited the Gallium team from July 2013 to December 2013. He worked on static analysis and intermediate representations for functional programming languages.

8.4.1.1. Internships

Robbert Krebbers

Subject: formal semantics for the C language

Date: from Jan 2013 until Mar 2013

Institution: Radboud University (Netherlands)

MARELLE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- We participated in 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 the question of precision in floating-point arithmetic and to provide formal proofs on this topic. This project was completed in October 2013.

7.2. European Initiatives

7.2.1. FP7 Projects

7.2.1.1. FORMATH

Type: COOPERATION

Defi: Future and Emerging Technologies

Instrument: Specific Targeted Research Project

Objectif: FET-Open: Challenging Current Thinking

Duration: March 2010 - August 2013

Coordinator: University of Göteborg (Sweden)

Partners: Radboud University Nijmegen, (the Netherlands), University of La Rioja, (Spain).

Site: http://wiki.portal.chalmers.se/cse/pmwiki.php/ForMath/ForMath

Inria contact: Y. Bertot

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.

7.3. International Initiatives

7.3.1. Informal International Partners

We interact regularly with the team of Prof. Thierry Coquand at University of Göteborg and Chalmers University in Sweden and the team of Prof. Julio Rubio at Universidad de La Rioja in spain.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Amy Felty, professor at the University of Ottawa, Doug Howe, professor at Carleton University in Canada, are visiting from September 2013 to Summer 2014.

7.4.1.1. Internships

- Florent Bréhard, student at École Normale Supérieure, worked from June to August 2013 on *homotopy type theory*. In particular, he produced a proof of equivalence between various presentations of spheres, at all dimensions.
- Antoine Grospellier, student at École Normale Supérieure, worked from June to August 2013 on integrating automatic proof tools for first order logic in the Coq system.

7.4.2. Visits to International Teams

- Yves Bertot spent three months From January 15th to April 15th, 2013 at Institute for Advanced Study, Princeton, where he was invited to participate to the special year on *Homotopy Type Theory*.

MEXICO Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. DIM/LSC TECSTES - 2011-052D

In this DIGITEO project (No. 6024), Hernán Ponce de Léon, Delphine Longuet (ParisSud) and Stefan Haar cooperate on the subject of conformance testing for concurrent systems, using Event Structures. The project started on September 1, 2011 and is scheduled to end on August 31, 2014.

7.1.2. LOCOREP

In the DIGITEO project LoCoReP (No. 2010-043D), Aiswarya Cyriac, Paul Gastin, and Benedikt Bollig worked on temporal logics for the specification and verification of concurrent recursive programs. The project started on September 1, 2010 and ended on August 31, 2013.

7.2. IRT

7.2.1. SystemX

Participants: Simon Theissing, Stefan Haar.

We participate in the project MIC on multi-modal transport systems with in the IRT *System X*, with academic partners UPMC, IFSTTAR and CEA, and several industrial partners including Alstom (project leader), COSMO and Renault.

7.3. National Initiatives

7.3.1. ANR project IMPRO

Participants: Thomas Chatain, Stefan Haar, Serge Haddad.

The Project ANR **ImpRo** ANR-2010-BLAN-0317 involves *IRCCyN* (Nantes), *IRISA* (Rennes), *LIP6*(Paris), *LSV* (Cachan), *LIAFA* (Paris) and *LIF* (Marseille). It addresses issues related to the practical implementation of formal models for the design of communication-enabled systems: such models abstract away from many complex features or limitations of the execution environment. The modeling of *time*, in particular, is usually idealized, with infinitely precise clocks, instantaneous tests or mode communications, etc. Our objective is thus to study to what extent the practical implementation of these models preserves their good properties. We aim at a generic mathematical framework to reason about and measure implementability, and then study the possibility to integrate implementability constraints in the models. A particular focus is on the combination of several sources of perturbation such as resource allocation, the distributed architecture of applications, etc. We also study implementability through control and diagnosis techniques, and apply the developed methods to a case study based on the AUTOSAR architecture, a standard in the automotive industry.

7.4. European Initiatives

7.4.1. FP7 Projects

7.4.1.1. Hycon2

Type: COOPERATION

Defi: Engineering of Networked Monitoring and Control Systems

Instrument: Network of Excellence

Objectif: Engineering of Networked Monitoring and Control systems

Duration: September 2010 - August 2014

Coordinator: CNRS

Partner: ETH Zürich, TU Berlin, TU Delft and many others.

Inria contact: C. Canudas de Wit

Abstract: Hycon2 aims at stimulating and establishing a long-term integration in the strategic field of control of complex, large-scale, and networked dynamical systems. It focuses in particular on the domains of ground and aerospace transportation, electrical power networks, process industries, and biological and medical systems.

7.4.1.2. Univerself: realizing autonomics for Future Networks

Type: COOPERATION

Defi: The Network of the Future

Instrument: Integrated Project

Objectif: The Network of the Future

Duration: September 2010 - August 2013

Coordinator: Alcatel Lucent (France)

Partner: UTwente, AL Ireland, AL Germany, VTT (Finland), U. of Piraeus, FT, Telecom Italia, NU of Athens, Fraunhofer, Interdic. Institue for Broadband Technology, Telefonica, Thales, Nec Europe, U. of Surrey, UCL, IBBT (Belgium)

Inria contact: E. Fabre

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.

7.5. International Initiatives

7.5.1. Inria International Partners

7.5.1.1. Informal International Partners

1. The CMI (Chennai Mathematical Institute) is a long-standing partner of our team. The project *Île de France/Inde* in the *ARCUS* program from 2008 to 2011 has allowed several exchange visits between Cachan and Chennai, organizations of ACTS workshops with french and indian researchers in Chennai, internships in Cachan, and two theses in *co-tutelle* (Akshay Sundararaman, defended in 2010) and Aiswarya Cyriac (thesis in progress).

   Currently, Paul Gastin is co-head (with Madhavan Mukund) of the CNRS International Associated Laboratory (LIA) INFORMEL (INdo-French FORmal Methods Lab, http://projects.lsv.ens-cachan.fr/informel/) . This LIA was created in January 2012 by an agreement between CNRS, ENS Cachan, University Bordeaux 1 on the french side and the Chennai Mathematical Institute, the Institute of Mathematical Sciences of Chennai, and the Indian Institute of Science of Bangalore on the Indian side.

2. We have been exchanging visits for several years between *MExICo* and the DISCO team (Lucia Pomello and Luca Bernardinello) at University Milano-Bicocca, Italy.
3. Exchanges are frequent with Rolf Hennicker from LMU and Javier Esparza at TUM, both in Munich, Germany.
4. With the computer science and electrical engineering departments at Newcastle University, UK

7.5.2. Participation In Other International Programs (non-Inria)

Benedikt Bollig, Aiswarya Cyriac, and Benjamin Monmege are participating in LeMon, a joint Procope project with LIAFA, (Paris) and the University of Lübeck, supported by EGIDE/DAAD. The aim of the project is to develop techniques for the inference of systems that deal with infinite data domains.

7.6. International Research Visitors

7.6.1. Visits of International Scientists

- Monika Heiner, Professor at University of Cottbus/Germany, visited *MExICo*from September 15 through October 15, 2013.
- Estibaliz Fraca, PhD student from Zaragossa, visited *MExICo*from november 2012 trough February 2013.
- From 7 to 19 January 2013, Paul Gastin and Aiswarya Cyriac (LSV) visit K. Narayan Kumar and Madhavan Mukund at CMI Chennai. They studied verification problems for concurrent and recursive multi-threaded programs.
- 13 May to 1 June 2013: Madhavan Mukund (CMI) visits LSV, IRISA.
- 8 to 29 June K. Narayan Kumar (CMI) visits LSV, LaBRI. The study verification problems for concurrent and recursive multi-threaded programs was pursued.
- 16 June to 30 June 2013: Saivasan Prakash (CMI) visits LSV and LIAFA. Discussions with Ahmed Bouajjani on Verification of networks of Communicating Recursive Processes. Joint work with M.F.Atig (Uppsala) and manuscript based on this work is under preparation.
- 25 May to 20 July 2013: Bharat Adsul (IIT Bombay) visits LSV and LaBRI to work on cascade products of asynchronous automata.

7.6.1.1. Internships

Gonzalo Amadio

Subject: Diagnosis of Stochastic Systems

Date: from Apr 2013 until Jul 2013

Institution: Universidad National de Rosario (Argentina)

Siddharth Krishna

Subject: Multiple Context Free Grammars

Date: from May 19, 2013 until June 15, 2013

Institution: Chennai Mathematical Institute, India

7.6.2. Visits to International Teams

- Thomas Chatain visited
  - Lucia Pomello and Luca Bernardinello at University of Milano-Bicocca for one week in February 2013,
  - Humboldt Universität Berlin for the KOSMOS-Workshop (November 28-30, 2013)
- 4 to 19 December 2013: Paul Gastin and Aiswarya Cyriac (LSV) visit CMI. With K. Narayan Kumar, they completed the study of verification problems via split-width for concurrent recursive multi-threaded programs (a paper is in preparation). With Madhavan Mukund, they started working on statistical analysis of asynchronous systems.

- Stefan Haar visited
    1. Technische Universitä Berlin in for five days in March 2013 and three days in November 2013 for seminar talks and technical cooperation,
    2. Humboldt Universität Berlin for the KOSMOS-Workshop (Nov. 28-30)
    3. University of Newcastle (UK) June 10-12 and Sep.16-20,
    4. Bucarest Polytechnic (RO) May 29 to June 1, giving a course on verification within the *CAN'TI* summer school, and
    5. University of Cordoba (Argentina) as an invited professor, from Oct 27 to Nov 1.
- Serge Haddad
- Hernán Ponce de Léon visited University of Cordoba (Argentina) for two weeks in October/November.
- César Rodríguez visited Victor Khomenko at the University of Newcastle for one week in May.
- Stefan Schwoon visited the group of Javier Esparza at the Technical University of Munich for two weeks in February.

PARSIFAL Project-Team

7. Partnerships and Cooperations

7.1. European Initiatives

7.1.1. FP7 Projects

7.1.1.1. Proofcert

Participants: Hichem Chihani, Quentin Heath, Dale Miller [correspondant], Fabien Renaud.

Title: ProofCert: Broad Spectrum Proof Certificates

Duration: January 2012 - December 2016

Type: IDEAS

Instrument: ERC Advanced Grant

Coordinator: Dale Miller

Abstract: There is little hope that the world will know secure software if we cannot make greater strides in the practice of formal methods: hardware and software devices with errors are routinely turned against their users. The ProofCert proposal aims at building a foundation that will allow a broad spectrum of formal methods—ranging from automatic model checkers to interactive theorem provers—to work together to establish formal properties of computer systems. This project starts with a wonderful gift to us from decades of work by logicians and proof theorist: their efforts on logic and proof has given us a *universally accepted* means of communicating proofs between people and computer systems. Logic can be used to state desirable security and correctness properties of software and hardware systems and proofs are uncontroversial evidence that statements are, in fact, true. The current state-of-the-art of formal methods used in academics and industry shows, however, that the notion of logic and proof is severely fractured: there is little or no communication between any two such systems. Thus any efforts on computer system correctness is needlessly repeated many time in the many different systems: sometimes this work is even redone when a given prover is upgraded. In ProofCert, we will build on the bedrock of decades of research into logic and proof theory the notion of *proof certificates*. Such certificates will allow for a complete reshaping of the way that formal methods are employed. Given the infrastructure and tools envisioned in this proposal, the world of formal methods will become as dynamic and responsive as the world of computer viruses and hackers has become.

7.1.2. Collaborations in European Programs, except FP7

7.1.2.1. STRUCTURAL: ANR blanc International

Participants: Kaustuv Chaudhuri, Nicolas Guenot, Willem Heijltjes, Stefan Hetzl, Novak Novakovic, François Lamarche, 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: SYSTEMTIC Paris région)

This project is a consortium of four partners, two French and two Austrian, who are all 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 Goedel'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. International Initiatives

7.2.1. Inria Associate Teams

7.2.1.1. RAPT

Participants: Kaustuv Chaudhuri [correspondant], Dale Miller, Yuting Wang, Olivier Savary-Bélanger.

Title: Applying Recent Advances in Proof Theory for Specification and Reasoning

Inria principal investigator: Kaustuv Chaudhuri

International Partner:

Institution: McGill University (Canada)

Laboratory: School of Computer Science

Researcher: Prof. Brigitte Pientka

International Partner:

Institution: University of Minnesota (United States)

Laboratory: Department of Computer Science and Engineering

Researcher: Prof. Gopalan Nadathur

International Partner:

Institution: Carnegie Mellon University (United States)

Laboratory: Department of Computer Science

Researcher: Prof. 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 (eg, 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.

7.2.2. Inria International Partners

7.2.2.1. PHC Procope: From Proofs to Counterexamples for Programming

Participants: Kaustuv Chaudhuri, Nicolas Guenot, Willem Heijltjes, Lutz Straßburger.

Title: From Proofs to Counterexamples for Programming

Duration: 01/01/2012 – 31/12/2013

German Partner: University of Bonn, Institute for Computer Science (Department III)

Finding counterexamples is an endeavor which is as important as proving theorems. But while the latter has seen a huge amount of research effort—we have nowadays a large quantity of tools for automated and interactive theorem proving—the former has mainly been neglected by proof theorists. One of the reasons is that finding counterexamples or countermodels has been considered a model theoretical activity, rather than a proof theoretical one. Only recently, researchers have begun to explore the well-known duality between "proof search" and "search for countermodels" in a purely proof theoretical way. The main objective of this collaboration is to develop the necessary proof theory for automatically generating such counterexamples in a more general setting.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

Chuck Liang (Professor from Hofstra University, NY, USA) visited for three weeks in May and June and another week in December.

Gopalan Nadathur (Professor from the University of Minnesota) visited for two weeks in May and June.

Elaine Pimentel (Associate Professor, UFRN, Brazil) for four weeks in June and July.

7.3.2. Internships

Olivier Savary-Bélanger (Masters, McGill University, Canada), supervised by Kaustuv Chaudhuri

7.3.3. Visits to International Teams

Fabien Renaud visited Gopalan Nadathur in Minneapolis for two weeks in February.

Dale Miller visited Alwen Tiu at the Australian National University in Canberra, Australia for onc week in May 2013.

Dale Miller visited Christof Benzmüller for one week in February.

PI.R2 Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

Pierre-Louis Curien (coordinator), Yves Guiraud and Philippe Malbos are members of the three-years Focal project of the IDEX Sorbonne-Paris-Cité, started in June 2013. This project, giving the support for the PhD grant of Cyrille Chenavier, concerns the interactions between higher-dimensional rewriting and combinatorial algebra with researchers from LAGA (Univ. Paris 13)

Pierre-Louis Curien (coordinator), Yves Guiraud and Philippe Malbos are members of the four-years Cathre ANR project, accepted in 2013, to begin in January 2014. This project will investigate the general theory of higher-dimensional rewriting, the development of a general-purpose library for higher-dimensional rewriting, and applications in the fields of combinatorial algebra, combinatorial group theory and theoretical computer science.

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

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

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

6.2. European Initiatives

6.2.1. FP7 Projects

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

6.2.2. Collaborations in European Programs, except FP7

Pierre-Louis Curien, Yves Guiraud and Philippe Malbos are collaborators of the Applied and Computational Algebraic Topology (ACAT) networking programme of the European Science Foundation.

6.3. International Initiatives

6.3.1. Inria Associate Teams

Title: Proof theory and functional programming languages (SEMACODE)

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: http://www.pps.univ-paris-diderot.fr/~saurin/EA-SEMACODE

6.3.2. Inria International Partners

We are setting up a partnershiop with the University of Wroclaw (our interlocutors are D. Biernacki and M. Biernacka).

6.3.3. Participation In other International Programs

Pierre-Louis Curien participates to the ANR International French-Chinese project LOCALI (coordinated by Gilles Dowek), and to a MathAmSud project in algebraic operads with the university of Talca (Chile).

6.3.4. Other international cooperations

MIT (Adam Chlipala, Jason Gross).

6.4. International Research Visitors

6.4.1. Visits of International Scientists

Beta Ziliani (MPI, Saarbrücken) visited πr^2 and PPS for a week in January to collaborate with Yann Régis-Gianas and Matthieu Sozeau.

Zena Ariola visited πr^2 and PPS for the whole academic year 2012-2013 with SEMACODE associate team to collaborate with Pierre-Louis Curien, Hugo Herbelin and Alexis Saurin. Her two PhD students joined for shorter terms (Paul Downen from November 2012 to July 2013 and Luke Maurer, being funded by the INTERNSHIP program – see below – from March 2013 to July 2013).

Marco Gaboardi visited πr^2 and PPS in for 10 days in may and again in december 2013 to collaborate with Alexis Saurin.

Olivier Danvy visited πr^2 and PPS in the fall 2013.

Fernando Ferreira (Univ. of Lisbon) and Ulrich Kohlenbach visited πr^2, hosted by Jaime Gaspar.

6.4.2. Internships

Participant: Luke Maurer.

Subject: Foundation for lazy languages

Date: from Mar 2013 until Jul 2013

Institution: University of Oregon (United States)

6.4.3. Visits to International Teams

Pierre Boutillier visited MSP group at the university of Strathclyde for a month in March 2013.

Hugo Herbelin visited Thomas Streicher at the University of Darmstadt in May 2013.

Hugo Herbelin visited the Institute of Cybernetics in Tallinn, Estonia in September and October 2013.

Pierre-Louis Curien visited IAS for 3 weeks in March, towards the end of the Special Year on Univalent Foundations. Matthieu Sozeau visited Vladimir Voevodsky at the IAS in Princeton for 15 days in May 2013.

SUMO Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

ANR VACSIM: Validation of critical control-command systems by coupling simulation and formal analysis, 2011-2014, web site
Partners: EDF R&D, Dassault Systèmes, LURPA, I3S, LaBRI, and Inria SUMO.
The project aims at developing both methodological and formal contributions for the simulation and validation of control-command systems. SUMO contributes to quantitative analysis and its application to testing, monitoring of timed systems, and verification of communicating timed automata.

ANR Ctrl-Green: Autonomic management of green data centers, 2011-2014
Partners: UJF/LIG, INPT/IRIT, Inria SUMO, EOLAS, Scalagent.
This project aims at developing techniques for the automatic optimal management of reconfigurable systems in the context of data centers using discrete controller synthesis methodology applied in the synchronous paradigm.

ANR ImpRo: Implementability and Robustness of Timed Systems, 2010-2014, web site
Partners: IRCCyN, LIP6, LSV, LIAFA, LIF, and Inria SUMO.
This project 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 good properties that are satisfied by idealized models. Within IMPRO, members of SUMO mainly focus on robustness issues for timed models (timed automata, timed Petri nets,...), and diagnosis.

ANR STOCH-MC: Model-Checking of Stochastic Systems using approximated algorithms, 2014-2018.
Led by SUMO.
Partners: Inria Project Team CONTRAINTES (Rocquencourt), LaBRI (Bordeaux), and LIAFA (Paris).
The aim of STOCH-MC is to perform model-checking of large stochastic systems, using controlled approximations. Two formalisms will be considered: Dynamic Bayesian Networks, which represent compactly large Markov Chains; and Markov Decision Processes, allowing non deterministic choices on top of probabilities.

8.1.2. National informal collaborations

We collaborate with Yliès Falcone (VaSCO - LIG) on the enforcement of timed properties and Tristan Le Gall (CEA) on the control of distributed systems.

We collaborate with Arnaud Sangnier (LIAFA) on the parameterized verification of probabilistic systems.

8.2. European Initiatives

8.2.1. FP7 Projects

Participant: Éric Fabre.

Univerself is a FP7 IP, with 19 partners, among which Alcatel-Lucent, Orange Labs, Thales Comunications, Telefonica, Telecom Italia as industrial partners. It lasted from Sept. 2010 to Nov. 2013. See also http://www.univerself-project.eu/ Univerself aimed at developing self-management methods for telecommunication networks, regardless of technological boundaries (wireless, wireline, services) and at providing tools for their integrability and acceptability. The focus was first on the development of network empowerment methods (NEM), that address specific needs in automating management functions, for example power tuning in SONs (Self-Organizing Networks), network and/or service diagnosis, vulnerability detection and correction, knowledge acquisition and elaboration, optimal resource usage and allocation, etc. A second set of results was on a methodology to deploy and coordinate such NEMs, through a Universal Management Framework (UMF).

8.3. International Initiatives

8.3.1. Inria Associate Teams

DISTOL (web site) is a joint project between the SUMO Team at Inria Rennes, the LogicA team at IRISA Rennes, the Chennai Mathematical Institute, the Institute of Mathematical Sciences at Chennai and the National University of Singapore.

The DISTOL project (Distributed systems, stochastic models and logics) aims at gathering researchers from Inria Rennes, two institutes in Chennai, India (CMI and IMSC) and National University of Singapore, working on formal modeling and verification of distributed systems. This project covers four main research directions. Each of these directions rely on specific and complementary competences:

- Robustness and time issues in distributed systems models (Members of SUMO consider this problem with the Chennai Mathematical Institute)
- Applications of formal models & techniques to Web Services (Members of SUMO consider this problem with the Chennai Mathematical Institute)
- Quantitative verification for distributed systems (Members of SUMO consider this problem with researchers at NUS)
- Unification of Control Theory of Distributed Systems (This part is mainly addressed by the LOGICA team in collaboration with the Institute of Mathematical Sciences)

8.3.2. Inria International Partners

8.3.2.1. Declared Inria International Partners

Éric Badouelis member of the team ALOCO (Architecture logicielle à Composants) of LIRIMA lab (Laboratoire international de recherche en informatique et mathématiques appliquées). LIRIMA is an african lab with headquarters in Yaoundé (Cameroun) partially funded by Inria. Within the team ALOCO, Éric collaborates on artifact-centric business process models.

8.3.2.2. Informal International Partners

We collaborate with Thomas Brihaye (UMONS, Brihaye) on the verification of stochastic timed systems.

We collaborated with Laurie Ricker (Mount Allison University, Canada) and Thierry Massart (ULB,Belgium) on the control of distributed systems.

8.3.3. Participation in other International Programs

Several researchers of the SUMO team are members of the LIA Informel. The Indo-French Formal Methods Lab is a CNRS International Associated Laboratory fostering the scientific collaboration between India and France in the domain of formal methods and applications to the verification of complex systems.

The research within LIA Informel focuses on theoretical foundations of games, automata, and logics, three important tools in formal methods. Members of Informel work on the verification of safety-critical systems, with an emphasis on quantitative aspects (time, cost, energy, etc.), concurrency, control, and security protocols.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

S. Akshay from IIT Bombay visited the SUMO team one week in autumn.

Luca Bernardinello, professor at the University of Milano Bicocca (Italy).

Thomas Brihaye, professor at Mons University (Belgium), spent one month in SUMO team as ISTIC (University Rennes 1) invited professor.

Georges-Edouard Kouamou, junior professor at ENSP Yaoundé (Cameroun).

Madhavan Mukund, from the Chennai Mathematical Institute, visited SUMO in May 2013 and was part of Loïc Hélouët's habilitation jury. He also stayed one week in autumn.

Laurie Ricker (Mount Allison University) visited us during for 2 weeks in March 2013.

8.4.1.1. Internships

Shibashis Guha, PhD student at IIT Delhi, spent two months in SUMO team, supervised by Nathalie Bertrand.

Baptiste Lefebvre (L3 student, ENS Ulm), was an intern from June to Aug. 2013, on the experimental evaluation of an enhanced graceful shutdown method for the OSPF routing protocol, supervised by Éric Fabre.

Raphael Struk (L3 student, ENS Rennes), did an internship supervised by Blaise Genest and Loïc Hélouët.

TOCCATA Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. 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 [100], [68][35], [45]. This is sorely needed to ease the verification of numerical applications, especially those involving advanced mathematics.

Partners: LIX (Palaiseau), University Paris 13

8.2. National Initiatives

8.2.1. ANR BWare

Participants: Sylvain Conchon, Évelyne Contejean, Jean-Christophe Filliâtre, Andrei Paskevich, Claude Marché.

This is a research project funded by the programme "Ingénierie Numérique & Sécurité" of the ANR. It is funded for a period of 4 years and started on September 1, 2012. http://bware.lri.fr.

It is an industrial research project that aims to provide a mechanized framework to support the automated verification of proof obligations coming from the development of industrial applications using the B method and requiring high guarantees of confidence. The methodology used in this project consists in building a generic platform of verification relying on different theorem provers, such as first-order provers and SMT solvers. The variety of these theorem provers aims at allowing a wide panel of proof obligations to be automatically verified by the platform. The major part of the verification tools used in BWare have already been involved in some experiments, which have consisted in verifying proof obligations or proof rules coming from industrial applications [107]. This therefore should be a driving factor to reduce the risks of the project, which can then focus on the design of several extensions of the verification tools to deal with a larger amount of proof obligations.

The partners are: Cedric laboratory at CNAM (CPR Team, project leader); Inria teams Gallium, Deducteam and Asap; Mitsubishi Electric R&D Centre Europe, the ClearSy company that develops and maintains *Atelier B* and the OCamlPro start-up.

8.2.2. ANR Verasco

Participants: Guillaume Melquiond [contact], Sylvie Boldo, Arthur Charguéraud, Claude Marché.

This is a research project funded by the programme "Ingénierie Numérique & Sécurité" of the ANR. It is funded for a period of 4 years and started on January 1st, 2012. http://verasco.imag.fr

The main goal of the project is to investigate the formal verification of static analyzers and of compilers, two families of tools that play a crucial role in the development and validation of critical embedded software. More precisely, the project aims at developing a generic static analyzer based on abstract interpretation for the C language, along with a number of advanced abstract domains and domain combination operators, and prove the soundness of this analyzer using the *Coq* proof assistant. Likewise, it will keep working on the CompCert C formally-verified compiler, the first realistic C compiler that has been mechanically proved to be free of miscompilation, and carry it to the point where it could be used in the critical software industry.

Partners: teams Gallium and Abstraction (Inria Paris-Rocquencourt), Airbus avionics and simulation (Toulouse), IRISA (Rennes), Verimag (Grenoble).

8.2.3. Systematic: Hi-Lite

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

The Hi-Lite project (http://www.open-do.org/projects/hi-lite/) is a project in the SYSTEMATIC Paris Region French cluster in complex systems design and management http://www.systematic-paris-region.org.

Hi-Lite is a project aiming at popularizing formal methods for the development of high-integrity software. It targets ease of adoption through a loose integration of formal proofs with testing and static analysis, that allows combining techniques around a common expression of specifications. Its technical focus is on modularity, that allows a divide-and-conquer approach to large software systems, as well as an early adoption by all programmers in the software life cycle.

Our involvements in that project include the use of the Alt-Ergo prover as back-end to already existing tools for SPARK/ADA, and the design of a verification chain for an extended SPARK/ADA language to verification conditions, via the Why3 VC generator.

The results of that project are the basis of SPARK2014, the next generation of the SPARK.

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

8.3. European Initiatives

8.3.1. FP7 Projects

Project acronym: ERC Deepsea

Project title: Parallel dynamic computations

Duration: Jun. 2013 - Jun. 2018

Coordinator: Umut A. Acar

Other partners: Carnegie Mellon University

Abstract:

The objective of this project is to develop abstractions, algorithms and languages for parallelism and dynamic parallelism with applications to problems on large data sets. Umut A. Acar (affiliated to Carnegie Mellon University and Inria) is the principal investigator of this ERC-funded project. The other researchers involved are Mike Rainey (Inria, Gallium team), who is full-time on the project, and Arthur Charguéraud (Inria, Toccata team), who works 40% of his time to the project. Project website: http://deepsea.inria.fr/.

8.3.2. Collaborations in European Programs, except FP7

Project acronym: JsCert

Project title: Certified JavaScript

Duration: Oct. 2011 - ...

Other partners: Imperial College and Inria Rennes – Bretagne Atlantique (Celtique project).

Abstract: This project aims at providing a formal semantics to the JavaScript language. It is joint work with Philippa Gardner, Sergio Maffeis, Gareth Smith, Daniele Filaretti and Daiva Naudziuniene from Imperial College, Alan Schmitt and Martin Bodin from Inria Rennes – Bretagne Atlantique, and Arthur Charguéraud from Inria Saclay –Île-de-France. Project website: http://jscert.org.

8.4. International Initiatives

8.4.1. Inria International Partners

8.4.1.1. Informal International Partners

- S. Conchon, A. Mebsout and F. Zaidi (VALS group, LRI) collaborate with S. Krstic and A. Goel (Intel Strategic Cad Labs in Hillsboro, OR, USA), in particular around the development of the SMT-based model checker Cubicle (see above). This collaboration is partly supported by an academic grant by Intel.

8.4.2. Participation In other 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 Summer School “Imagine the future in ICT”.

VERIDIS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. Inria Development Action VeriT

Participants: Pablo Dobal, Pascal Fontaine.

Inria funds this project (started in 2011) to support the development of the SMT solver veriT (see section 5.1), including added expressiveness, improved efficiency and code stability, and interfaces with tools that embed veriT as a backend solver. The project is coordinated by Pascal Fontaine and also includes Inria Rennes (Celtique) and Sophia Antipolis (Marelle). Federico Dobal has been hired in 2012 on a position funded by this project and has in particular contributed to improvements in the code of the solver as well as of the testing platform that allows us to detect bugs and the impact of changes on the performance of the tool. He has also contributed to the maintenance of the deltaSMT tool, which has been used by several other teams of SMT developers for debugging SMT solvers.

8.2. European Initiatives

8.2.1. FP7 project MEALS

Type: PEOPLE

Instrument: International Research Staff Exchange Scheme

Objective: Exchange of scientists between Europe and Argentina

Duration: October 2011 - September 2015

Coordinator: Holger Hermanns, Universität des Saarlandes (Germany)

Partner: Universidad de Buenos Aires, Universidad Nacional de Córdoba, Universidad Nacional de Rio Cuarto, Instituto Tecnológico Buenos Aires

Inria contact: Castuscia Palamidessi

Abstract: The MEALS project funds exchanges between scientists in Europe (Saarland University, RWTH Aachen, TU Dresden, Inria, Imperial College, Univ. of Leicester, TU Eindhoven); it is structured in five work packages (Quantitative Analysis of Concurrent Program Behaviour, Reasoning Tasks for Specification and Verification, Security and Information Flow Properties, Synthesis in Model-based Systems Engineering, Foundations for the Elaboration and Analysis of Requirements Specifications). Our team mainly cooperates with the group led by Carlos Areces in Córdoba, as well with Diego Garbervetsky in Buenos Aires, within work package 2. In 2013, the project funded visits by Luciana Benotti, Rodrigo Castaño, Raúl Fervari, and Guillaume Hoffmann.

8.2.2. Cooperation with TU Wien, Austria

Participants: Pascal Fontaine, Stephan Merz.

This project – from January 2012 to December 2013 – fosters bilateral cooperation with the team headed by Prof. Alexander Leitsch at TU Vienna. It focuses on aspects of proof production and proof compression in automated reasoning. It is headed by Bruno Woltzenlogel Paleo of TU Wien, who was formerly a post-doctoral researcher in VeriDis until March 2011, and Pascal Fontaine. The project is funded by the Amadeus Programme of the Partenariat Hubert Curien and the Österreichischer Austausch Dienst.

The project funded the traveling costs for the participants for four one-week workshops in Vienna and Nancy. In particular, the third workshop was affiliated to Tableaux 2013 and was open to the participants of Tableaux; it attracted around 40 participants. The final workshop of the project took place in November 2013 in Vienna.

The discussions involved many aspects on proofs and allowed to improve some aspects of proof production in SMT, as well as several proof handling tools (e.g. Skeptik), developed among others at TU Wien. The web page gives more information on this project.

8.2.3. Cooperation with NUI Maynooth, Ireland

Participant: Dominique Méry.

The project *Building Reliable Systems: Software Refinement meets Software Verification* is a one-year project funded by PHC Ulysses. The academic Irish partner is Dr Rosemary Monahan of NUI Maynooth. The verification of software requires the specification of preconditions and postconditions as well as other properties of the code. These properties are expressed as annotations providing a detailed understanding of how the software is implemented. In program verification, the annotation process is often done *a posteriori*, with verification tools used to check that annotations are sound according to the semantics of the program. Determining the correct annotations to provide a complete specification is difficult, especially when specifying invariant properties of the code. *A priori* techniques for developing correct software are based on the correct-by-construction paradigm. The refinement-based approach is such a technique, providing for the construction of a correct program through the step-by-step refinement of an initial high-level model of the software. In this way, the program specification is developed alongside the code, discharging the conditions that need to be proved. We focus on combining these two software engineering techniques, to benefit from the strengths of both. We have proposed a framework [18] for integrating a representation of the *a posteriori* paradigm, namely Spec#, and a representation of the *a priori* paradigm, namely Event B. This integration induces a methodology which bridges the gap between software modeling and program verification in the software development life cycle.

8.3. International Initiatives

8.3.1. Participation In International Programs

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

Participants: David Déharbe, Pablo Dobal, Pascal Fontaine, Stephan Merz.

VeriDis has a close working relationship with a team at Universidade Federal do Rio Grande de Norte (UFRN), Brazil, and more specifically with Prof. David Déharbe. Pascal Fontaine visited Natal in early 2013. 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. Our cooperation was also supported by the Inria-CNPq project SMT-SAVeS from 2010 throughout early 2013.

A new STIC AmSud project has been approved that will start in 2014 and involves a team at the University of Córboba in Argentina, the team at UFRN, and VeriDis. It is again centered on SMT, with a particular focus on quantifiers and modal logic [21].

8.4. International Research Visitors

8.4.1. Visits of International Scientists

David Déharbe from UFRN (Natal, Brazil) joined the VeriDis team in Nancy for a one-year sabbatical that started in August 2013.

Josef Widder from TU Vienna, Austria, spent 6 weeks in Nancy in October and November 2013 as an Inria invited researcher. Together with Stephan Merz, he worked on the formalization of parameterized model checking techniques for fault-tolerant distributed algorithms in a proof assistant.

Mike Poppleton from the University of Southampton and Hoang Thai Son from ETHZ spent a week in our group for developing techniques to integrate fairness in Event B models, on the basis of the work published at IFM 2013 [17].

8.4.1.1. Internships

Luis Esteban Campostrini

Subject: Formal Verification of Distributed Algorithms

Date: from May until October, 2013

Institution: Universidad National de Rosario (Argentina)

Joint supervision with Martin Quinson (AlGorille team)

Anisia Maria Magdalena Tudorescu

Subject: Integrating SMT solvers into Spike

Date: from March 2013 until May 2013

Institution: West Timisoara University (Romania)

Joint supervision with Christophe Ringeissen (Cassis team) and Sorin Stratulat (Pareo team)

Paula Chocrón

Subject: Non-disjoint combination for SMT solvers: sharing a fragment of arithmetic

Date: from September 2013 until December 2013

Institution: University of Buenos Aires (Argentina)

Joint supervision with Christophe Ringeissen (Cassis team)

CARTE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- The team was a funding parter in ANR Complice (Implicit Computational Complexity, Concurrency and Extraction), ref.: ANR-08-BLANC-0211-01, that ended in april 2013 and whose aim was to extend the results of ICC to other paradigms (process languages, ...) and take benefice of proof extraction techniques in order to synthesize resoure certificates. This ANR should be followed by a new ANR submission (ANR Elica proposal) involving Paris 7 PPS team, Paris 13 LCC team, ENS Lyon Plume team and Bologna Inria team Focus.
- The team is a funding parter in ANR Binsec, whose aim is to fill part of the gap between formal methods over executable code on one side, and binary-level security analyses currently used in the security industry. Two main applicative domains are targeted: vulnerability analysis and virus detection. Two other closely related applications will also be investigated: crash analysis and program deobfuscation.
- Emmanuel Jeandel is a member of ANR Blanche ANR-09-BLAN-0164 (EMC: *Emerging Phenomena in Computation Models*), that ended in April 2013.

8.1.2. PEPS

- Simon Perdrix is a member of a PEPS INS2I "Information et Communication Quantique: Cryptographie et Calcul Quantiques Distribués." with partners in Telecom ParisTech and other labs.
- Mathieu Hoyrup is principal investigator of a PEPS INS2I "Approches Topologiques de l'Information et de la Calculabilité", with Emmanuel Jeandel and Laurent Bienvenu (CNRS, LIAFA).

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. FI-WARE

Title: Morphus

Type: COOPERATION

Defi: PPP FI: Technology Foundation: Future Internet Core Platform

Instrument: Integrated Project (IP)

Objectif: PPP FI: Technology Foundation:Future Internet Core Platform

Duration: September 2011 - May 2014

Coordinator: Telefonica (Spain)

Other Partners: Thales, SAP, Inria

Inria contact: Olivier Festor

Abstract: See also: http://www.fi-ware.eu/. 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 for building a true foundation for the Future Internet.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

The team has an informal partnership with Pr. James Royer (University of Syracuse) and PhD. Norman Danner (Wesleyan University) on the study of program higher order complexity (an Inria associated team proposal has been submitted on this domain). On the Implicit Computational Complexity part, the team has strong contacts with Universita di Torino (Pr Simona Ronchi Della Rocca), Dundee University(PhD Marco Gaboardi), Universita di Bologna (Pr Simone Martini and PhD Ugo Dal Lago).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Subramanian Kumbakonam Govindarajan, professor in Universiti Sains Malaysia, was visiting Carte team in february. He works on computational models and Parikh matrices.

Neil Jones, professor in the University of Copenhagen, visited Carte team for one month in March. He is currently working on program transformation and program obfuscation, which have obvious applications to Computer Virology.

8.4.2. Visits to International Teams

Mathieu Hoyrup visited Universidad Andres Bello in Santiago de Chile during february. He worked there with Cristobal Rojas on extending the results [22] from functions to relations.

CASSIS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- Franche-Comté Region project SyVAD (SysML Verification and Validation), coordinated by Fabrice Bouquet, duration: 3 years, started in September 2011. This project focuses on the SysML models for the validation and verification of the micro-systems, in particular for distributed micro airduct. The project associates several team of FEMTO-ST institute.

8.2. National Initiatives

8.2.1. ANR

- 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 EPI Prosecco and EPI 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.
- ANR OSEP *Online and offline model-based testing of SEcurity Properties*, duration: 2 years, started in November 2011 and ended in November 2013. The goal of this project was to apply online and offline model-based testing approaches for security testing of cryptographic components and software radio case studies, used as a black boxes. This approach had to be compatible with our previous offline approaches to increase the number of artefacts that can be shared. So, we developed new algorithms to allow online testing, and a dedicated tool called MBeeTle. This project was an opportunity to reuse the results of the ANR TASCCC project, and to complete these approaches with security properties expressed in TOCL. This project involved the DGA and Smartesting.

8.2.2. Competitivity Clusters

- 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 will provide a methodology and tools based on open source components.

- Project "Investissement d'Avenir - Développement de l'Econimie Numérique" DAST (Dynamic Application Security Testing), duration: 2 years, starting in September 2012. The goal of this project is to generate automatically the tests to prevent vulnerabilities. We have proposed an automated model-based vulnerability testing approach, that focuses on Criss-Site Scripting vulnerabilities in web applications. It relies on a behavioral model that describes the web application and a set of security test patterns formalizing ways to detect the vulnerabilities. This partnership includes NBSystem, Smartesting (coordinator), Thales, Trusted-Labs and Inria CASSIS.

8.3. European Initiatives

8.3.1. FP7 Projects

- Nessos is a Network of Excellence on Engineering Secure Future Internet Software Services and Systems in FP7-ICT (starting in October 2010 for a period of 42 months). Nessos has 12 partners and aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. Partner Inria is involved through project-teams Arles, Triskell and Cassis. Cassis will focus on developping tools for service security verification and testing tasks.
- ProSecure (2011-2016) [9]— ERC Starting Grant Project on Provably secure systems: foundations, design, and modularity. This long-term project aims at developing provably secure systems such as security protocols. The goal is to propose foundations for a careful analysis and design of large classes of up-to-date protocols. To achieve this goal, we foresee three main tasks. First, we plan to develop general verification techniques for new classes of protocols that are of primary interest in nowadays life like e-voting protocols, routing protocols or security APIs. Second, we will consider the cryptographic part of the primitives that are used in such protocols (encryption, signatures, ...), obtaining higher security guarantees. Third, we aim at proposing modular results both for the analysis and design of protocols. Véronique Cortier is the leader of the project.

8.4. International Initiatives

8.4.1. Inria Associate Teams

BANANAS [10]*Automated design and autonomous control of hybrid solver cooperations*. In order to tackle large scale instances and intricate problem structures, sophisticated solving techniques have been developed, combined, and hybridized to provide efficient solvers. A common idea to get more efficient and robust algorithms consists in combining several resolution paradigms in order to take advantage of their respective assets. Autonomous Search is a very attractive approach for designing adaptive systems with the capability of improving its solving performance by selecting and adapting its search strategies to the problem at hand. The main goal of the project is to apply the Autonomous Search approach to hybrid solver cooperations, by automating the selection and the cooperation of solvers, by tuning the cooperation parameters, and by adapting the cooperation during solving. The international partners are Technical University Federico Santa Maria, Valparaíso (Chile) — Department of Computer Science — Carlos Castro and Eric Monfroy; University of Chile (Chile) — Center for Mathematical Modeling — Jorge Amaya. The Inria principal investigator is Christophe Ringeissen.

8.4.2. Inria International Partners

- Collaboration with Bogdan Warinschi (Bristol University) on soundness of symbolic models w.r.t. cryptographic ones.
- Collaboration with Mark Ryan's group (University of Birmingham) on the formal analysis of e-voting protocols.
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction.

[9] http://www.loria.fr/~cortier/ProSecure.html
[10] http://www.loria.fr/~ringeiss/CHILI/bananas

- Collaboration with Hanifa Boucheneb's group (Ecole Polytechnique de Montréal) on model-checking of collaborative systems.
- Collaboration with John Mullins's group (Ecole Polytechnique de Montréal) on information hiding.

8.4.3. Participation in International Programs

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.

French-Canadian project on *Automata for Hiding and Disclosing Information*, in the framework of the CFQCU program. We collaborate with the CRAC team at the Ecole Polytechnique de Montréal, Canada, and the MoVe team/LIP6 at the UPMC, Paris, France.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Myrto Arapinis (University of Edinburgh), one week in January 2013, two weeks in November 2013
- Florian Boehl (KIT University), one week in January 2013
- Luigi Grillo (Università di Catania), two weeks in April 2013
- Dominique Unruh (Tallin University), one week in February 2013
- Bogdan Warinschi (University of Bristol), one week in January 2013
- Paliath Narendran (SUNY Albany), one month in June-July 2013
- David Bouchard and Kim Gero (SUNY Albany), one week in September 2013
- Christoph Sprenger and Binh Nguyen (ETH Zürich) three days in April 2013

8.5.1.1. Internships

We have supervised the following internships.

Anisia Maria Magdalena Tudorescu

Subject: Integrating SMT solvers into Spike

Supervisors: Pascal Fontaine (project-team Veridis), Sorin Stratulat, and Christophe Ringeissen

Date: from Mar 2013 until May 2013

Institution: West Timisoara University (Romania)

Gisela-Carla Rossi

Subject: Formal Methods for Secure Service Composition

Supervisors: Walid Belkhir and Michaël Rusinowitch

Date: from Jun 2013 until Dec 2013

Institution: National University of Cordoba (Argentina)

Paula Chocrón

Subject: Non-disjoint combination for SMT solvers: sharing a fragment of arithmetic

Supervisors: Pascal Fontaine (project-team Veridis) and Christophe Ringeissen

Date: from Sep 2013 until Nov 2013

Institution: University of Buenos Aires (Argentina)

Gemma Puig-Quer

Subject: New protocols for private e-voting

Supervisors: David Galindo-Chacon and Véronique Cortier

Date: from Sep 2013 until Mar 2014

Institution: UPC Barcelona (Spain)

In addition, Steve Kremer has supervised the following students from the École des Mines de Nancy:

- Othmane El Omri, Analysis of a peer-to-peer E-wallet protocol (from Jul 2013 to Sep 2013)
- Pierre Lepeudry, Formalizing some combinatorial attacks in security protocols (from Sep 2013 to Jan 2014)

and Véronique Cortier and Cyrille Wiedling have supervised a group of three students from the École des Mines de Nancy on the implementation of a secure key management system on smartcards: Arnaud Kéranguéven, Hadrien Chastant, and Othmane El Omri (from Oct 2012 to June 2013).

8.5.2. Visits to International Teams

- Olga Kouchnarenko, August 2013 (10 days), Ecole Polytechnique de Montréal (the CRAC team), Canada, visit funded by the Conseil franco-québécois de coopération universitaire" (CFQCU).

COMETE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR projects

7.1.1.1. ANR-09-BLAN-0169-01

- **Project acronym:** PANDA
- **Project title:** Analysis of Parallelism and Distribution
- **Duration:** October 2009 - March 2013
- **URL:** http://lipn.univ-paris13.fr/~mazza/Panda/
- **Coordinator:** Catuscia Palamidessi, Inria Saclay
- **Other PI's and partner institutions:** Dale Miller, EPIs Parsifal at Inria Saclay. Emmanuel Haucourt, CEA Saclay. Damiano Mazza, Pôle Parisien (ENS Cachan, Paris VII and Paris XIII). Emmanuel Godard, Pôle Méditerranéen (ENS Lyon and the University of Marseille). Jean Souyris, Airbus.
- **Abstract:** The aim of PANDA is to bring together different mathematical models of parallel and concurrent computation (geometric models, rewriting theory, higher category theory, stochastic processes), along with theoretical frameworks for static analysis (spatial logics, proof construction), in order to guide the development of software tools that meet industrial needs of program specification and verification (in particular, fault detection of parallel programs involved in avionics).

7.1.1.2. ANR-09-BLAN-0345-02

- **Project acronym:** CCP
- **Project title:** Confidence, Proof and Probabilities
- **Duration:** October 2009 - March 2013
- **URL:** http://www.lix.polytechnique.fr/~bouissou/cpp/
- **Coordinator:** Jean Goubault-Larrecq, ENS Cachan
- **Other PI's and partner institutions:** Catuscia Palamidessi, Inria. Olivier Bouissou, CEA LIST. Gilles Fleury, Supelec SSE. Michel Kieffer, Supelec L2S.
- **Abstract:** 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.

7.1.2. Large-scale initiatives

- **Project acronym:** CAPPRIS
- **Project title:** Collaborative Action on the Protection of Privacy Rights in the Information Society
- **Duration:** October 2011 - September 2015
- **URL:** https://cappris.inria.fr/
- **Coordinator:** Daniel Le Metayer, Inria Grenoble
- **Other partner institutions:** The project involves four Inria research centers (Saclay, Saphia-Antipolis, Rennes and Grenoble), CNRS-LAAS, Eurecom and the university of Namur. Besides computer scientists, the consortium also includes experts in sociology and in law, thus covering the complementary areas of expertise required to reach the objectives.

- **Abstract:** The goal of this project is to study the challenges related to privacy in the modern information society, trying to consider not only the technical, but also the social and legal ones, and to develop methods to enhance the privacy protection.

7.2. European Initiatives

7.2.1. FP7 Projects

7.2.1.1. MEALS

Program: FP7-PEOPLE-2011-IRSES

Project acronym: MEALS

Project title: Mobility between Europe and Argentina applying Logic to Systems

Duration: October 2011 - September 2015

URL: http://www.meals-project.eu/

Coordinator: Holger Hermans, Saarland University, Germany

Coordinator for the Inria sites: Catuscia Palamidessi, Inria Saclay

Other partner institutions: Rheinisch-Westfälische Technische Hochschule Aachen, Germany. Technische Universität Dresden, Germany. Inria, France. Imperial College of Science, Technology and Medicine, UK, University of Leicester, UK. Technische Universiteit Eindhoven, NL. Universidad Nacional de Cordoba, AR. Universidad de Buenos Aires, AR. Instituto Tecnologico de Buenos Aires, AR. Universidad Nacional de Rio Cuarto, AR.

Abstract: In this project we focus on three aspects of formal methods: specification, verification, and synthesis. We consider the study of both qualitative behavior and quantitative behavior (extended with probabilistic information). We aim to study formal methods in all their aspects: foundations (their mathematical and logical basis), algorithmic advances (the conceptual basis for software tool support) and practical considerations (tool construction and case studies).

7.3. International Initiatives

7.3.1. Inria Associate Teams

7.3.1.1. PRINCESS

Title: Protecting privacy while preserving data access

Inria principal investigator: Catuscia Palamidessi

International Partners:

Geoffrey Smith, Florida International University (United States)

Andre Scedrov, University of Pennsylvania (United States)

Duration: 2013 - 2016

URL: http://www.lix.polytechnique.fr/comete/Projects/Princess/

Abstract: PRINCESS is an Inria associated team focusing on the protection of privacy and confidential information. In particular, we study the issues related to the leakage of confidential information through public observables.

We aim at developing a meaningful notion of measure in order to quantify the leakage of information, and to design mechanisms to limit the amount of leakage, without interfering too severely with the utility of the information that is meant to be disclosed.

The main topics currently investigated are quantitative information flow, where we are developing a decision-theoretic approach, and differential privacy, where we are developing an extension which lifts the basic notion of privacy meant for databases to arbitrary domains.

7.3.2. Inria International Partners

7.3.2.1. Informal International Partners

- **Charles Carroll Morgan,** Professor, University of New South Wales
- **Moreno Falaschi,** Professor, University of Siena
- **Mario Ferreira Alvim Junior,** Assistant Professor, Federal University of Minas Gerais
- **Annabelle Mciver,** Associate Professor, Macquarie University
- **Carlos Olarte,** Associate Professor, Universidad Javeriana Cali

7.3.3. Participation In other International Programs

7.3.3.1. PACE

- **Program:** ANR Blanc International
- **Project title:** Beyond plain Processes: Analysis techniques, Coinduction and Expressiveness
- **Duration:** January 2013 - December 2016
- **URL:** http://perso.ens-lyon.fr/daniel.hirschkoff/pace/
- **Coordinator:** Daniel Hirschkoff , Ecole Normale Supérieure de Lyon
- **Other PI's and partner institutions:** Catuscia Palamidessi, Inria Saclay. Davide Sangiorgi, University of Bologna (Italy). Yuxi Fu, Shanghai Jiao Tong University (China).
- **Abstract:** This project objective is to enrich and adapt these methods, techniques, and tools to much broader forms of interactive models, well beyond the realm of "traditional" processes.

7.3.3.2. LOCALI

- **Program:** ANR Blanc International
- **Project title:** Logical Approach to Novel Computational Paradigms
- **Duration:** October 2011 - September 2015
- **URL:** http://lcs.ios.ac.cn/~locali2013/
- **Coordinator:** Gilles Dowek, Inria Rocquencourt
- **Other PI's and partner institutions:** Catuscia Palamidessi, Inria Saclay. Thomas Erhard, Paris VII. Ying Jiang , Chinese Academy of Science in Beijin (China).
- **Abstract:** This project aims at exploring the interplays between logic and sequential/distributed computation in formalisms like the lambda calculus and the π calculus. Going back to the fundamentals of the definitions of these calculi, the project plans to design new programming languages and proof systems via a logical approach.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

- **Nikita Borisov,** Associate Professor, University of Illinois at Urbana-Champaign, from Nov 2013 until Dec 2013
- **Moreno Falaschi,** Professor, University of Siena, from Sep 2013 until Sep 2013
- **Mario Ferreira Alvim Junior,** Assistant Professor, Federal University of Minas Gerais, from Nov 2013 until Dec 2013
- **Fabio Gadducci,** Associate Professor, University of Pisa, from Jun 2013 until Aug 2013
- **Dominik Luecke,** Postdoc, from Apr 2013 until Apr 2013
- **Annabelle Mciver,** Associate Professor, Macquarie University, from Dec 2013 until Dec 2013
- **Charles Carroll Morgan,** Professor, University of New South Wales, from Dec 2013 until Dec 2013

- **Carlos Olarte,** Associate Professor, Universidad Javeriana Cali, from June 2013 until Jul 2013
- **Camilo Rueda,** Professor, Universidad Javeriana Cali, from Nov 2013 until Dec 2013
- **Vladimiro Sassone,** Professor, University of Southampton, from Apr 2013 until May 2013
- **Mauricio Toro Bermudez,** Postdoc, University of Cyprus, from Jun 2013 until Jun 2013

7.4.2. Internships

7.4.2.1. Xiao Wang

- **Duration:** From May 2013 until August 2013
- **Subject:** Differential privacy and applications of privacy protection in location-based services
- **Institution:** LIX, Ecole Polytechnique

7.4.2.2. Fernán Martinelli

- **Duration:** From September 2012 until March 2013
- **Subject:** Computation of bounds on the information flow
- **Institution:** University of Rio Cuarto, Argentina
- **Support:** FP7 project MEALS

7.4.3. Visits to International Teams

Catuscia Palamidessi visited the team of Andre Scedrov and Benjamin Pierce at the University of Pennsylvania. July 2013.

DICE Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Dice is involved in a regional project of the Rhône-Alpes region, ARC6 "Innovative Services for Social Networks", with Telecom Saint Etienne.

8.2. National Initiatives

8.2.1. ANR

Dice is involved in two new ANR projects, to start at the end of 2013,

- C3PO, on Collaborative Creation of Contents and Publishing using Opportunistic networks, with LT2C Telecom Saint-Etienne, INSA LYON, IRISA, ChronoCourse, et Ecole des Mines de Nantes.
- Socioplug, Social Cloud over Plug Networks, Enabling Symmetric Access to Data and Preserving Privacy, with LINA / Université de Nantes, Université de Rennes 1, INSA Lyon.

8.3. European Initiatives

8.3.1. FP7 Projects

Dice is involved in the CSA project "Big data roadmap and cross-disciplinarY community for addressing socieTal Externalities (BYTE)", Objective ICT-2013.4.2 Scalable data analytics (c) Societal externalities of Big Data roadmap.

PRIVATICS Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Privamov'

Title: Privamov'

Type: Labex IMU.

Duration: September 2013 - 2015.

Coordinator: LIRIS.

Others partners: EVS-ITUS, Inria Urbanets.

Abstract: The objective of this project is to provide researchers the IMU community traces of urban mobility allowing further their research and validate their assumptions and models. Indeed , many communities need to know the modes of urban transport : sociologists, philosophers , geographers, planners or computer scientists. If these traces are an important feature for researchers or industrial, they are more for users who have helped to build: attacks jeopardize the privacy of users. Anonymization techniques developed within the project will make available to the greatest number of these traces, while ensuring that the entire process (from collection to data analysis) will be made in respect of the privacy of users involved.

7.1.2. SCCyPhy

Title: SCCyPhy

Type: Labex Persyval.

Duration: September 2013 - 2015.

Coordinator: Institut Fourier.

Others partners: Inria MOAIS, Verimag, CEA/LETI, LIG, GIPSA-Lab, TIMA.

Abstract: A main motivation of this action-team is to provide a structure to the Grenoble community in computer security and cryptography in the spirit of the PERSYVAL-lab Labex. Our emphasize, within the PCS workpackage, is around complementary areas of research with high impact for science and technology, with the following target applications: embedded systems (including smartphones and sensors network), at both software and hardware levels, distributed architectures (including "cloud" and "sky"), privacy and protection of information systems against cyberattacks of various origins.

7.2. National Initiatives

7.2.1. ANR

7.2.1.1. BIOPRIV

Title: Application of privacy by design to biometric access control.

Type: ANR.

Duration: April 2013 - March 2017.

Coordinator: Morpho (France).

Others partners: Morpho (France), Inria (France), Trusted Labs (France).

See also: http://planete.inrialpes.fr/biopriv/.

Abstract: The objective of BIOPRIV is the definition of a framework for privacy by design suitable for the use of biometric technologies. The case study of the project is biometric access control. The project will follow a multidisciplinary approach considering the theoretical and technical aspects of privacy by design but also the legal framework for the use of biometrics and the evaluation of the privacy of the solutions.

7.2.1.2. BLOC

Title: Analysis of block ciphers dedicated to constrained environments.

Type: ANR.

Duration: October 2013 - September 2015.

Coordinator: INSA-Lyon (France).

Others partners: CITI Laboratory XLIM Laboratory, University of Limoges, Inria Secret, CryptoExperts (PME).

See also: http://bloc.project.citi-lab.fr/.

Abstract: BLOC aims at studying the design and analysis of block ciphers dedicated to constrained environments. The four milestones of BLOC are: security models and proofs, cryptanalysis, design and security arguments and performance analyzes and implementations of lightweight block ciphers. The aims of the project are the following ones: Security models and proofs Cryptanalysis Design C library of lightweight block ciphers We also aim at providing at the end of the project a lightweight block cipher proposal.

7.2.1.3. pFlower

Title: Parallel Flow Recognition with Multi-Core Processor.

Type: ANR.

Duration: March 2011 - September 2014.

Coordinator: LISTIC Université de Savoie.

Others partners: ICT-CAS Insititute of Computing Technology (China), LISTIC Université de Savoie.

Abstract: The main objective of this project is to take advantage of powerful parallelism of multi-thread, multi-core processors, to explore the parallel architecture of pipelined-based flow recognition, parallel signature matching algorithms.

7.2.2. Other

7.2.2.1. MOBILITICS

Title: MOBILITICS

Type: joint project.

Duration: January 2012 - Ongoing.

Coordinator: CNIL.

Others partners: CNIL.

Abstract: Platform for mobile devices privacy evaluation. This project strives to deploy an experimental mobile platform for studying and analyzing the weaknesses of current online (smartphone) applications and operating systems and the privacy implications for end-users. For instance, one of the objectives is to understand trends and patterns collected when they are aimed at obtaining general knowledge that does not pertain to any specific individual. Examples of such tasks include learning of commuting patterns, inference of recommendation rules, and creation of advertising segments.

7.2.2.2. MOBILITICS

Title: MOBILITICS

Type: joint project.

Duration: January 2012 - Ongoing.

Coordinator: CNIL.

Others partners: CNIL.

Abstract: Platform for mobile devices privacy evaluation. This project strives to deploy an experimental mobile platform for studying and analyzing the weaknesses of current online (smartphone) applications and operating systems and the privacy implications for end-users. For instance, one of the objectives is to understand trends and patterns collected when they are aimed at obtaining general knowledge that does not pertain to any specific individual. Examples of such tasks include learning of commuting patterns, inference of recommendation rules, and creation of advertising segments.

Inria Mobilitics (2011-2012): as a joint national project with CNIL (the French national committee of Information freedom).

Collaborative Action CAPRIS (2011-2014): the Collaborative Action on the Protection of Privacy Rights in the Information Society (CAPRIS), is an Inria national project, which goal is to tackle privacy-related challenges and provide solutions to enhance the privacy protection in the Information Society. His main tasks are the identification of existing and future threats to privacy, and the design of appropriate measures to assess and quantify privacy.

7.3. European Initiatives

7.3.1. FP7 Projects

7.3.1.1. PRIPARE

Title: Preparing industry to privacy-by-design by supporting its application in research.

Type: COOPERATION (ICT).

Instrument: Support Action (SA).

Duration: October 2013 - September 2015.

Coordinator: Trialog (France).

Others partners: American University of Paris (France), Atos (Spain), Fraunhofer SIT (Germany), Galician Research and Development Center in Advanced Telecommunications (Spain), Inria (France), KU Leuven (Belgium), Trialog (France), Trilateral Research (UK), Universidad Politecnica de Madrid (Spain), University of Ulm (Netherlands), Waterford Institute of Technology (UK).

Abstract: the general goal of PRIPARE is to facilitate the application of privacy by design. To this aim, PRIPARE will support the practice of privacy by design by the ICT research community (to prepare for industry practice) and foster risk management culture through educational material targeted to a diversity of stakeholders. The project will specify a privacy by design software and systems engineering methodology combining a multidisciplinary expertise involving legal, engineering and business viewpoints. The project will also provide best practices material and educational material focusing on risk management of privacy for different target audiences (general public, policy makers, users, ICT students and professional). The project will also pave the way for future research by identifying gaps and providing recommendations for a research agenda for privacy by design.

7.3.1.2. PARIS

Title: Privacy preserving infrastructure for surveillance.

Type: COOPERATION (ICT).

Instrument: Specific Targeted Research Project (STREP).

Duration: January 2013 - December 2015.

Coordinator: Trialog (France).

Others partners: AIT (Austria), Inria (France), KU Leuven (Belgium), Trialog (France), Universidad de Malaga (Spain), Université de Namur (Belgium), Thales (France), Visual Tools (Spain).

See also: http://www.paris-project.org/.

Abstract: PARIS will define and demonstrate a methodological approach for the development of surveillance infrastructure which enforces the right of citizens for privacy, justice and freedom and takes into account the evolving nature of such rights (e.g. aspects that are acceptable today might not be acceptable in the future), and the social and ethical nature of such rights (e.g. perception of such rights varies). The methodological approach will be based on two pillars, first a theoretical framework for balancing surveillance and data protection which fully integrates the concept of accountability, and secondly an associated process for the design of surveillance systems which takes from the start privacy (i.e. Privacy by Design) and accountability (i.e. Accountability by Design).

7.3.2. Collaborations in European Programs, except FP7

7.3.2.1. FI-WARE

Title: Future Internet Ware.

Type: COOPERATION (ICT).

Defi: PPP FI: Technology Foundation: Future Internet Core Platform.

Instrument: Integrated Project (IP).

Duration: May 2011 - April 2014.

Coordinator: Telefonica. (Spain)

Others partners: SAP (Germany), IBM (Israel, Switzerland), Inria (France), 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).

See also: 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.

7.4. International Initiatives

7.4.1. Inria International Labs

Title: Secure and Private Distributed Data Storage and Publication in the Future Internet

Inria principal investigator: Claude Castelluccia

International Partners (Institution - Laboratory - Researcher):

University of California Berkeley (United States) - Electrical Engineering and Computer Science Department - Edward Lee

University of California Irvine (United States) - Donald Bren School of Information and Computer Sciences - Gene Tsudik

Duration: 2012 - 2014

See also: http://planete.inrialpes.fr/cloudy-associated-team/

Cloud computing is a form of computing where general purpose clients (typically equipped with a web browser) are used to access resources and applications managed and stored on a remote server. Cloud applications are increasingly relied upon to provide basic services like e-mail clients, instant messaging and office applications. The customers of cloud applications benefit from outsourcing the management of their computing infrastructure to a third-party cloud provider. However, this places the customers in a situation of blind trust towards the cloud provider. The customer has to assume that the "cloud" always remains confidential, available, fault-tolerant, well managed, properly backed-up and protected from natural accidents as well as intentional attacks. An inherent reason for today's limitations of commercial cloud solutions is that end users cannot verify that servers in the cloud and the network in between are hosting and disseminating tasks and content without deleting, disclosing or modifying any content. This project seeks to develop novel technical solutions to allow customers to verify that cloud providers guarantee the confidentiality, availability and fault-tolerance of the stored data and infrastructure.

7.5. International Research Visitors

7.5.1. Visits to International Teams

Mohamed Ali Kaafar, spending a sabbatical at NICTA Australia in Sydney (since February 2012)

Subject: Online Privacy Enhancing Technologies: measuring the risks and designing countermeasures

PROSECCO Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. ProSe

Title: ProSe: Security protocols : formal model, computational model, and implementations (ANR VERSO 2010.)

Other partners: Inria/Cascade, ENS Cachan-Inria/Secsi, LORIA-Inria/Cassis, Verimag.

Duration: December 2010 - December 2014.

Coordinator: Bruno Blanchet, Inria (France)

Abstract: The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the symbolic level, in which messages are terms; the computational level, in which messages are bitstrings; the implementation level: the program itself.

8.1.2. FUI

8.1.2.1. Pisco

Title: PISCO

Partners: Bull, Cassadian, CEA, CS, Saferiver, Serpikom, Telecom Paristech

Duration: January 2013 - December 2014.

Coordinator: Liliana Calabanti, Bull (France)

Abstract: The goal of the project is to develop a prototype of a new secure applicance based on a virtual machine architecture accessing an HSM. The role of PROSECCO is to contribute to the analysis of security http://www.systematic-paris-region.org/en/projets/pisco

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. CRYSP

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

Type: IDEAS ()

Instrument: ERC Starting Grant (Starting)

Duration: November 2010 - October 2015

Coordinator: Karthikeyan Bhargavan, Inria (France)

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

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

- K. Bhargavan, A. Pironti, and A. Delignat-Lavaud work closely with Microsoft Research in Cambridge, Redmond, Silicon Valley, and Bangalore (C. Fournet, N. Swamy, M. Abadi, P. Naldurg)
- G. Steel and R. Bardou work closely with University of Venice, Italy (R. Foccardi).
- G. Bana works closely with Keio University Japan
- E-I. Bartzia works closely with IMDEA Madrid (P-Y. Strub)

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Pierre-Malo Denielou (Lecturer, Royal Holloway, University of London) visited us for two months as professeur invité.
- Sergio Maffeis (Imperial College, London) visited us as part of an ongoing collaboration.
- Cédric Fournet (Researcher, Microsoft Researcher) visited us as part of an ongoing collaboration.

8.4.2. Visits to International Teams

- Alfredo Pironti visited Microsoft Research Cambridge (UK) several times, as part of a long-term collaboration
- Gergely Bana visited Keio University (Japan), ICT Lisbok (Portugal), and Queen Mary University of London in Nov 2013
- Benjamin Smyth visited Toshiba, Japan and Univesity of Birmingham (UK)