RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2014

Section Partnerships and Cooperations

Edition: 2015-06-01

ARIC Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

The PhD grant of Valentina Popescu is funded by Région Rhône-Alpes through the ARC6 programme.

8.2. National Initiatives

8.2.1. ANR HPAC Project

Participants: Claude-Pierre Jeannerod, Nicolas Louvet, Clément Pernet, Nathalie Revol, 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.

8.2.2. ANR DYNA3S Project

Participants: Guillaume Hanrot, Gilles Villard.

Dyna3s is a four year ANR project that started in October 2013. The Web page of the project is http://www.liafa.univ-paris-diderot.fr/dyna3s/. It is headed by Valérie Berthé (U. Paris 7) and involves also the University of Caen.

The aim is to study algorithms that compute the greatest common divisor (gcd) from the point of view of dynamical systems. A gcd algorithm is considered as a discrete dynamical system by focusing on integer input. We are mainly interested in the computation of the gcd of several integers. Another motivation comes from discrete geometry, a framework where the understanding of basic primitives, discrete lines and planes, relies on algorithm of the Euclidean type.

8.2.3. ANR FastRelax Project

Participants: Nicolas Brisebarre, Guillaume Hanrot, Vincent Lefèvre, Jean-Michel Muller, Bruno Salvy, Serge Torres, Silviu Filip, Sébastien Maulat.

FastRelax stands for "Fast and Reliable Approximation". It is a four year ANR project started in October 2014. The web page of the project is http://fastrelax.gforge.inria.fr/. It is headed by B. Salvy and involves AriC as well as members of the Marelle Team (Sophia), of the Mac group (LAAS, Toulouse), of the Specfun and Toccata Teams (Saclay), as well as of the Pequan group in UVSQ and a colleague in the Plume group of LIP.

The aim of this project is to develop computer-aided proofs of numerical values, with certified and reasonably tight error bounds, without sacrificing efficiency. Applications to zero-finding, numerical quadrature or global optimization can all benefit from using our results as building blocks. We expect our work to initiate a "fast and reliable" trend in the symbolic-numeric community. This will be achieved by developing interactions between our fields, designing and implementing prototype libraries and applying our results to concrete problems originating in optimal control theory.

8.2.4. 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.

8.3. 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. 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

- PICS CANTaL (Cryptography, Algorithmic Number Theory and Lattices). This is a collaborative project involving several AriC members (Nicolas Brisebarre, Guillaume Hanrot, Fabien Laguillaumie, Adeline Langlois and Damien Stehlé), and collaborators in several Australian universities: Christophe Doche (Macquarie University), Igor Shparlinski (UNSW) and Ron Steinfeld (Monash University). It was funded by the International office of the CNRS, for 2012, 2013 and 2014.
- IEEE P1788 working group for the standardization of interval arithmetic. We contributed to the creation in 2008 of this working group http://grouper.ieee.org/groups/1788/ and Nathalie Revol chairs this group since its creation. In 2014, the final draft text has been approved upon by the working group in June. The rest of the year was devoted to editorial polishing, before submitting the text to the "Sponsor ballot", which constitutes the final step and should be completed in 2015. The annual in-person meeting, chaired by Nathalie Revol, took place at the end of the SCAN 2014 conference in Würzburg, Germany, the 26 September.

  Vincent Lefèvre actively participated in various discussions, either in the mailing-list or in small subgroups.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Many colleagues from all other the world visit us regularly for seminars and collaborations. We list only long visits here.

Jie Chen (assistant professor at ECNU, China) visited us for a month, in November. He collaborated with Fabien Laguillaumie, Benoît Libert and Damien Stehlé on functional encryption.

Jung Hee Cheon (professor at SNU, South Korea) and Changmin Lee (PhD student at SNU, South Korea) visited us for a month, in August. They collaborated with Damien Stehlé on the approximate greatest common divisor problem and its applications in homomorphic cryptography.

8.4.1.1. Internships

Mihai-Ioan Popescu (ENS de Lyon) did a Master 1 internship from May to July, under the supervision of Damien Stehlé. He worked on heuristic algorithms for short lattice vector enumeration.

François Colas (U. Grenoble) did a Master 2 internship from March to June, under the supervision of Damien Stehlé. He worked on lattice-based homomorphic encryption.

Catalin Cocis (ENS de Lyon) did a Master 2 internship from February to June under the supervision of Fabien Laguillaumie. He worked on the implementation of multilinear maps.

Laura Chira (Technological U. of Cluj, Romania) did an L3 Summer internship from July to September 2014. This internship was supervised by Benoît Libert and devoted to the implementation of pseudo-random functions based on hard algorithmic problems in lattices.

Thomas Grégoire (ENS de Lyon) did a Master 2 internship from February to June under the supervision of Nicolas Brisebarre. He designed some tools for the certified approximation of functions in various orthogonal bases.

Saurabh Yadav (2nd year student, Indian Institute of Technology Delhi, India) did a Summer internship supervised by Benoît Libert in July and August 2014. The goal was to study and survey the applications of a cryptographic primitive built on top of multi-linear maps and called “indistinguishability obfuscation.”

CARAMEL Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

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

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

Participants: Cyril Bouvier, Nicholas Coxon, Jérémie Detrey, Pierrick Gaudry, Laurent Grémy, 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 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. Four meetings have taken place already: in Nancy on December 14, 2012 (kick-off), in Palaiseau on June 19, 2013, in Montpellier on November 12-13, 2013, and in Nancy in June 18-19, 2014.

8.2. International Research Visitors

8.2.1. Visits of International Scientists

- Masahiro Ishii is a visiting PhD student from the Nara Institute of Science and Technology, Nara (Japan), from February 2014 until February 2015. His PhD supervisors are Atsuo Inomata and Kazutoshi Fujikawa. Locally, he is supervised by Jérémie Detrey and Pierrick Gaudry.

CASCADE Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives with Industrials

- **ANR ARPEGE PRINCE: Proven Resilience against Information leakage in Cryptographic Engineering.**
  Participants: Michel Ferreira Abdalla, Sonia Belaid, Fabrice Ben Hamouda, Alain Passelègue, David Pointcheval.

  From December 2010 to May 2015.
  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.
- **ANR INS SIMPATIC: SIM and PAiring Theory for Information and Communications security.**
  Participants: Angelo de Caro, Houda Ferradi, David Pointcheval, Olivier Sanders, Damien Vergnaud.

  From February 2013 to July 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.
- **FUI CryptoComp.**
  Participants: Rafael Del Pino, Vadim Lyubashevsky.

  From October 2014 to September 2017.
  Partners: CEA, UVSQ, CryptoExperts, Dictao, XLIM, ViAccess Orca, CNRS, Bertin Technologies, KalRay, Gemalto
  We aim at studying delegation of computations to the cloud, in a secure way.

6.2. National Collaborations within Academics

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

  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).

- **ANR JCJC CLE: Cryptography from Learning with Errors.**
  Participants: Vadim Lyubashevsky, Pierrick Méaux, Thomas Prest.

  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.
- **ANR JCJC EnBiD: Encryption for Big Data.**
  Participant: Hoeteck Wee.

  From October 2014 to September 2018.
  Partners: Univ. Paris 2, Univ. Paris 8.
  The main objective of this project is to study techniques for efficient and expressive functional encryption schemes. Functional encryption is a novel paradigm for public-key encryption that enables both fine-grained access control and selective computation on encrypted data, as is necessary to protect big, complex data in the cloud.

6.3. European Initiatives

- **SecFuNet: Security for Future Networks.**
  Participants: Michel Ferreira Abdalla, Vadim Lyubashevsky, David Pointcheval.

  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.
- **ICT COST CryptoAction: Cryptography for Secure Digital Interaction**
  Participant: Vadim Lyubashevsky.

  From April 2014 to April 2018.
  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.
- **ERC CryptoCloud: Cryptography for the Cloud.**
  Participants: Michel Ferreira Abdalla, Florian Bourse, Fabrice Ben Hamouda, Geoffroy Couteau, Thomas Peters, David Pointcheval, Hoeteck Wee.

  From June 2014 to May 2019.

6.4. Other Grants

- **Google: Google Research Award.**
  Participant: Hoeteck Wee.

  On the security of TLS. The goal of this project is to initiate a formal cryptographic treatment of new mechanisms and proposals for reducing the latency in the TLS Handshake Protocol and to enhance our cryptographic understanding of the TLS Handshake Protocol.

6.5. International Research Visitors

- Hugo Krawczyk (IBM)
- Serdar Pehlivanoğlu (Zirve University, Turkey)
- Kai-Min Chung (Academia Sinicia, Taiwan)

- Daniel Wichs (Northeastern)
- Mehdi Tibouchi (NTT)
- Vinod Vaikuntanathan (MIT)
- Kenny Paterson (RHUL)
- Tal Malkin (Columbia)
- David Cash (Rutgers)
- Igor Shparlinski
- Zvika Brakerski (Weizmann)
- Elette Boyle (Technion)
- Giuseppe Persiano (Salerno)
- Yuval Ishai (Technion)
- Eike Kiltz (RUB)

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. Collaborations with Major European Organizations

CWI: Cryptography team of Ronald Cramer (Netherlands) organisme 1, labo 1 (pays 1) This team is officially a partner of LIAMA's CRYPT international project.

5.3. International Initiatives

5.3.1. Inria International Labs

- CRYPT is an international project from LIAMA in China, hosted by Tsinghua University in Beijing. It is a joint project between Inria, Tsinghua University, CAS Academy of Mathematics and System Sciences, and CWI (Netherlands).
- Phong Nguyen is the European director of LIAMA.

5.3.2. Inria International Partners

5.3.2.1. Informal International Partners

- Univ. Oklahoma, USA
- Univ. Wisconsin, USA

5.4. International Research Visitors

5.4.1. Visits of International Scientists

Cheng Qi (Univ. Oklahoma, USA)

Mehdi Tibouchi (NTT, Japan)

Guangwu Xu (Univ. Wisconsin, USA)

GALAAD2 Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. GEOLMI

GEOLMI - Geometry and Algebra of Linear Matrix Inequalities with Systems Control Applications - is an ANR project working on topics related to the Geometry of determinantal varieties, positive polynomials, computational algebraic geometry, semidefinite programming and systems control applications.

The partners are LAAS-CNRS, Univ. de Toulouse (coordinator), LJK-CNRS, Univ. Joseph Fourier de Grenoble; Inria Sophia Antipolis Méditerranée; LIP6-CNRS Univ. Pierre et Marie Curie; Univ. de Pau et des Pays de l'Adour; IRMAR-CNRS, Univ. de Rennes.

More information available at http://homepages.laas.fr/henrion/geolmi.

8.1.2. ANEMOS

ANEMOS - Advanced Numeric for ELMs (Edge Localized Mode) : Modeling and Optimized Schemes - is an ANR project devoted to the numerical modelling study of such ELM control methods as Resonant Magnetic Perturbations (RMPs) and pellet ELM pacing both foreseen in ITER. The goals of the project are to improve understanding of the related physics and propose possible new strategies to improve effectiveness of ELM control techniques. The study of spline spaces for isogemetric finite element methods is proposed in this context.

The partners are IRFM, CEA, Cadarache; JAD, University of Nice - Sophia Antipolis; Inria, Bacchus; Maison de la Simulation CEA-CNRS-Inria-University of Orsay- University of Versailles St Quentin.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. TERRIFIC

Title: Towards Enhanced Integration of Design and Production in the Factory of the Future through Isogeometric Technologies

Type: COOPERATION (ICT)

Defi: PPP FoF: Digital factories: Manufactoring design and product lifecycle manage

Instrument: Specific Targeted Research Project (STREP)

Duration: September 2011 - August 2014

Coordinator: SINTEF, Oslo (Norway)

Others partners:

Alenia Aeronautica (Italy); Inria Méditerranée (France); Jozef Kepler universitet, Linz (Austria); JOTNE, Oslo (Norway); MAGNA, Steyr (Austria); Missler Software (France); Siemens AG (Germany); Technische Universität Kaiserslautern (Germany); University of Pavia (Italy).

See also: http://terrific-project.eu

Abstract: The project aims at significant improvement of the interoperability of computational tools for the design, analysis and optimization of functional products. An isogeometric approach is applied for selected manufacturing application areas (cars, trains, aircrafts) and for computer-aided machining. Computer Aided Design (CAD) and numerical simulation algorithms are vital technologies in modern product development, yet they are today far from being seamlessly integrated. Their interoperability is severely disturbed by inconsistencies in the mathematical approaches used. Efficient feedback from analysis to CAD and iterative refinement of the analysis model is a feature of isogeometric analysis, and would be an essential improvement for computer-based design optimization and virtual product development. Our vision is to provide and disseminate tangible evidence of the performance of the isogeometric approach in comparison to traditional ones in four important application areas as well as addressing interoperability and other issues that necessarily arise in a large-scale industrial introduction of isogeometry.

8.3. International Initiatives

8.3.1. Participation In other International Programs

We have a bilateral collaboration between Galaad and the University of Athens-DIT team ERGA, headed by Ioannis Emiris for the period August 2013-August 2014. It is supported by both Inria and the University of Athens.

Title: Algebraic algorithms in optimization

Abstract: In the past decade, algebraic approaches to optimization problems defined in terms of multivariate polynomials have been intensively explored and studied in several directions. One example is the work on semidefinite optimization and, more recently, convex algebraic geometry. This project aims to focus on algebraic approaches for optimization applications in the wide sense. We concentrate on specific tools, namely root counting techniques, the resultant, the discriminant and non-negative polynomials, on which the two teams have extensive collaboration and expertise. We examine applications in convex algebraic geometry as well as to a newer topic for the two teams, namely game theory. A common thread to these approaches is to exploit any (sparse) structure.

We participate to a bilateral collaboration between France and Spain which is supported as a PICS from CNRS. The Spanish partner is the University of Barcelona (J. Burgos, C. D'Andrea, Martin Sombra) and the French partners are The university of Caen (F. Amoroso, M. Weimann), the University of Paris 6 (M. Chardin, P. Philippon) and GALAAD (L. Busé).

Title: Diophantine Geometry and Computer Algebra

Abstract: This project aims at exploring interactions between diophantine geometry and computer algebra by stimulating collaborations between experts in both domains. The research program focus on five particular topics : toric varieties and height, equidistribution, Diophantine geometry and complexity, Factorization of multivariate polynomials by means of toric geometry and study of singularities of toric parameterizations.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Chandrajit Bajaj, professor at University of Austin, Texas, USA, September 14-28.

Nicolàs Botbol, researcher CONICET, University of Buenos Aires, Argentina, March 10-23.

Philippe Trébuchet, LIP6, University of Paris 6, France, May 4-11.

Nelly Villamizar, researcher at RICAM, University of Linz, Austria, February 19-26.

8.4.2. Visits to International Teams

8.4.2.1. Research stays abroad

Evelyne Hubert was invited to participate to the program on *Inverse Moment Problems: the Crossroads of Analysis, Algebra, Discrete Geometry and Combinatorics* at the Institute for Mathematical Science at the National University of Singapore (December 1013 - January 2014).

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. Renewed for 1 year from January 1st 2014 to December 31t 2014
- 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: 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: [56], [33], [48], [52], [62], [61], [12]

8.3.2. ANR TOPDATA

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

- 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 Bourgogne), 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.

- See also: http://geometrica.saclay.inria.fr/collaborations/TopData/Home.html

8.4. European Initiatives

8.4.1. FP7 & H2020 Projects

8.4.1.1. GUDHI

Type: FP7

Instrument: ERC Advanced Grant

Duration: February 2014 - January 2019

Coordinator: Jean-Daniel Boissonnat

Inria contact: Jean-Daniel Boissonnat

Abstract: The central goal of this project is to settle the algorithmic foundations of geometry understanding in dimensions higher than 3. Geometry understanding encompasses a collection of tasks including the approximation and computer representation of geometric structures, and the inference of geometric or topological properties of sampled shapes.

See also https://project.inria.fr/gudhi/

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Pedro Machado Manhães de Castro (Universidade Federal de Pernambuco)

Arijit Ghosh (MPII, Saarbrucken), april, november-december

Antoine Vigneron (KAUST), may

Ramsay Dyer (Johann Bernouilli Institute, University of Groningen), octobre

Kira Vyatkina (Saint Petersburg Academic University), october

Vissarion Fisikopoulos (Université Libre de Bruxelles), november

GRACE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. PEPS PAIP

From late 2012 through 2013, D. 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.

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.

D. Augot engaged in monthly brainstorming meetings with researchers from Inria Paris–Rocquencourt (project-team SMIS), Université Jean Monnet's ADIS and CERDI labs (A. Rallet, A. Bensamoun), and Télécom ParisTech (C. 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 personal data; privacy leaks; and measurements on smartphones.

A one-day conference was held in Paris in December 2014.

8.1.2. PEPS Aije-Bitcoin

Within the group PAIP (Pour une Approche Interdisciplinaire de la Privacy), D. Augot presented the cryptographic and peer-to-peer principles at the heart of the Bitcoin protocol (electronic signature, hash functions, and so on). Most of the information is publicly available: the history of all transactions, evolution of the source code, developers' mailing lists, and the Bitcoin exchange rate. It was recognized by the economists in our group that such an amount of data is very rare for an economic phenomenon, and it was decided to start research on the history of Bitcoin, to study the interplay between the development of protocol and the development of the economical phenomenon.

The project **Aije-Bitcoin** (analyse informatique, juridique et économique de Bitcoin) was accepted as interdisciplinary research for a PEPS (Projet exploratoire Premier Soutien) cofunded by the CNRS and Université de Paris-Saclay. This one-year preliminary program will enable the group to master the understanding of Bitcoin from various angles, allowing more advanced research in the following years.

8.1.3. IDEALCODES

Idealcodes is a two-year Digiteo research project, started in October 2014. The partners involved are the École Polytechnique (X) and the Université de Versailles–Saint-Quentin-en-Yvelines (Luca de Feo, UVSQ). It funds one two-year post-doc, J. Nielsen, working at the boundary between coding theory, cryptography, and computer algebra.

Idealcodes spans the three research areas of algebraic coding theory, cryptography, and computer algebra, by investigating the problem of lattice reduction (and root-finding). In algebraic coding theory this is found in Guruswami and Sudan's list decoding of algebraic geometry codes and Reed–Solomon codes. In cryptography, it is found in Coppersmith's method for finding small roots of integer equations. These topics were unified and generalised by H. Cohn and N. Heninger [36], by considering algebraic geometry codes and number field codes under the deep analogy between polynomials and integers. Sophisticated results in coding theory could be then carried over to cryptanalysis, and vice-versa. The generalized view raises problems of computing efficiently, which is one of the main research topics of Idealcodes.

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). This 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-3: this one-year project aims to find matrices with good diffusion properties over small finite fields, in the spirit of [17]. The principle is to find non-maximal matrices, but with better coefficients and implementation properties. The relevant cryptographic properties to be studied correspond to the weight distribution of the associated code. Since we use Algebraic-Geometry codes, much more powerful techniques can be used for computing these weight distribution, using and improving Duursma's ideas [37].
- Cybersecurity. Inria and DGA contracted for three PhD topics at the national level, one of them involving Grace. Grace started a new PhD, and hired P. Karpman. The topic of this PhD is complementary to the above DIFMAT-3: while DIFMAT-3 provides fundamental methods for dealing with AG codes, in application for diffusion layers in block ciphers, the topic here is to make concrete propositions of block ciphers using these matrices. P. Karpman is coadvised by T. Peyrin (Nanyang Technological University, Singapore), by P.-A. Fouque (Université de de Rennes), and D. Augot.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

PQCRYPTO (Post-Quantum Cryptography) is a proposal which was submitted in 2014 by Tanja Langa (Tu/E), with Inria as a partner. We received in September 2014 the notification that it was accepted. Inria's Secret and Grace project-teams are part of this proposal, whose starting date is March 2015.

8.3.2. Collaborations in European Programs, except FP7 & H2020

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 many new directions in networking, internet, wireless communication systems, and cloud computing. 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. Informal International Partners

- M. Bossert, Institute of Communications Engineering, Ulm Universität.
- S. Galbraith, Department of Mathematics, University of Auckland.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Ruud Pellikaan (Department of Mathematics and Computing Science Eindhoven University of Technology) visited us from April 24th to May 21st.

LFANT Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

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

Participants: Bill Allombert, Karim Belabas, Jean-Marc Couveignes, Andreas Enge, Hamish Ivey-Law, 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.

The ANR organised the conference “Effective moduli spaces and applications to cryptography” in June 2014 as a part of the Centre Henri Lebesgue’s Thematic Semester 2014 “Around moduli spaces”.

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

Participants: Guilhem Castagnos, 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.

D. Robert is a participant in the Task 2 whose role is to give state of the art algorithms for pairing computations, adapted to the specific hardware requirements of the Simpatic Project.

6.2. European Initiatives

6.2.1. FP7 & H2020 Projects

6.2.1.1. ANTICS

Type: FP7

Defi: NC

Instrument: ERC Starting Grant

Objectif: NC

Duration: January 2012 - December 2016

Coordinator: Inria (France)

Inria contact: Andreas Enge

Abstract: Data security and privacy protection are major challenges in the digital world. Cryptology contributes to solutions, and one of the goals of ANTICS (Algorithmic Number Theory in Cryptology) 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.

6.3. International Initiatives

6.3.1. 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, J.-M. Couveignes, T. Ezome, D. Robert and A. Enge. Since Sep. 2014 the coordinator is T. Ezome and the vice-coordinator is D. Robert. The managing team organises the cooperation, schedules meetings, prepares reports, controls expenses, reports to the LIRIMA managing team and administrative staff.

A non-exhaustive list of activities organised or sponsored by Macisa includes

- The Summer school in M'Bour in Senegal with the International Center for Pure and Applied Mathematics (ICPAM/CIMPA), June 2014;
- The Annual Cameroonian workshop on Cryptography, Algebra and Geometry (CRAG), July 2014;
- The visit of Thierry Mefenza (Cameroun), to École Normale Supérieure de Paris for a PhD Thesis with Damien Vergnault, November 2013 and September–November 2014;
- The visit of Hortense Boudjou (Maroua) to work with Abdoul Aziz Ciss (École Polytechnique de Thièse, Sénégal), May – July 2014;
- The visit of Abdoul Aziz Ciss (Dakar) and Tony Ezome (Franceville) to Bordeaux, September 2014.
- Kodjo Kpognon Egadédé defended his PhD thesis in december 2014 under the supervision of Julien Sebag.

The team was evaluated in September 2014 as part of the general LIRIMA evaluation seminar.

6.3.2. Inria International Partners

6.3.2.1. Informal International Partners

The team is used to collaborate with Leiden University through the ALGANT program for PhD joint supervision.

Eduardo Friedman (U. of Chile), long term collaborator of K. Belabas and H. Cohen is a regular visitor in Bordeaux (about 1 month every year).

6.4. International Research Visitors

6.4.1. Visits of International Scientists

- Hartmut Monien, Universität Bonn, Germany. 01/2014;
- Eduardo Friedman, Universidad de Chile, 02/2014;
- Amalia Pizarro-Madariaga, Universidad de Valparaiso, Chile, 04/2014;
- Tony Ezome Mintsa, University of Franceville, Gabon, 04/2014 and 09/2014;
- Alina Dudeanu, École polytechnique fédérale de Lausanne, Switzerland, 05/2014;
- Kamal Khuri-Makdisi, American University of Beirut, Lebanon, 07/2014;
- Abdoul-Aziz Ciss, University of Dakar, 09/2014;
- Dimitar Jetchev, École polytechnique fédérale de Lausanne, Switzerland, 10/2014;

6.4.1.1. Internships

- Ilaria Chillotti (with D. Robert), Université Joseph Fourier, 02/2014–07/2014]
- Gregor Seiler (with A. Enge), Technische Universität Berlin, Germany, 10/2013–03/2014

POLSYS Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- **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).** 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).

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. 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.

7.3. International Initiatives

7.3.1. Inria International Labs

We are involved in the ECCA (Exact/Certifed Computation with Algebraic Systems) Team of LIAMA. Our partners are mainly from the Chinese Academy of Sciences and Beihang Univ. Our research focuses mainly on polynomial system solving and its applications.

7.3.2. Inria Associate Teams

7.3.2.1. QOLAPS

Title: Hybrid Methodologies for Quantifier Elimination, Global Optimization, Linear Algebra and Polynomial System Solving
International Partner (Institution - Laboratory - Researcher):
North Carolina State University (ÉTATS-UNIS)
Duration: 2012 - 2014
See also: http://www-polsys.lip6.fr/QOLAPS/index.html
Reliable and certified computing is a major issue in computer science motivated by huge needs in engineering sciences and in the industry (aeronautics, railway transports, etc.). At the same time, the need for high-performance computational routines is constantly increasing. It is tackled on the one hand by designing asymptotically fast algorithms which often have the feature to be randomized and/or approximate and/or probabilistic and on the other hand by developing high performance implementations. Our goal is to conciliate high-performance computing with certification and/or validation issues. We will mainly focus on algebraic problems, and precisely on linear and non-linear systems of equations and/or inequalities. In this context, hybrid methodologies combining exact and numeric computation are traditionally used in two separate ways: either exact computation is used to analyze the robustness of numerical schemes or numerical computation is used to speed up computations. Our viewpoint is to mix these trends in hybrid methodologies by exploiting the scientific continuum from linear algebra to quantifier elimination and global optimization through Grobner bases computations for polynomial system solving.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Éric Schost, Univ. Western Ontario, Canada.

Nitin Saxena, IIT Kanpur, India.

Danilo Gligoroski, NTNU, Norway.

7.4.1.1. Internships

Ivan Bannwarth

Date: Mar 2014 – Aug 2014

Institution: Université de Versailles – Saint-Quentin-en-Yvelines (France)

Matías Bender

Date: Sep 2014 – Feb 2015

Institution: Universidad de Buenos Aires (Argentine)

Anca Nitulescu

Date: Mar 2014 – Aug 2014

Institution: Université Paris Diderot (France)

Ulrick Severin

Date: Sep 2013 – Mar 2014

Institution: Dassault Systèmes (France)

SECRET Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR BLOC** (10/11 → 09/15)
  Design and Analysis of block ciphers dedicated to constrained environments
  ANR program: Ingénierie numérique et sécurité
  Partners: INSA Lyon, Inria (project-team SECRET), University of Limoges (XLIM), CryptoExperts
  446 kEuros
  http://bloc.project.citi-lab.fr
  The BLOC project aims at providing strong theoretical and practical results in the domain of cryptanalysis and design of block ciphers.
- **ANR KISS** (12/11 → 12/15)
  Keep your personal Information Safe and Secure
  ANR program: Ingénierie numérique et sécurité
  Partners: Inria (project-teams SMIS and SECRET), LIRIS, Gemalto, University of Versailles-St Quentin, 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 → 10/17)
  Cryptography from learning with errors
  ANR program: Jeunes Chercheurs, SIMI2
  Coordinator: Vadim Lyubashevsky (Inria, project-team 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.
- **ANR BRUTUS** (10/14 → 09/18)
  Authenticated Ciphers and Resistance against Side-Channel Attacks
  ANR program: Défi Société de l'information et de la communication
  Partners: ANSSI, Inria (project-team SECRET and project-team MARELLE), Orange, University of Lille, University of Rennes, University Versailles-Saint Quentin
  160 kEuros
  The Brutus project aims at investigating the security of authenticated encryption systems. We plan to evaluate carefully the security of the most promising candidates to the Caesar competition, by trying to attack the underlying primitives or to build security proofs of modes of operation. We target the traditional black-box setting, but also more "hostile" environments, including the hardware platforms where some side-channel information is available.

8.1.2. Others

- **French Ministry of Defense** (10/12 → 09/15)
  Funding for the supervision of Audrey Tixier's PhD.
  30 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

8.2. European Initiatives

8.2.1. Collaborations in European Programs, except FP7 & H2020

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.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Declared Inria International Partners

Title: Discrete Mathematics, Codes and Cryptography

International Partner (Institution): Indian Statistical Institute, Kolkata (India)

Duration: 2014

This collaboration investigates the three following topics: Quantum information and cryptography; Design and maintenance of primitives for symmetric cryptography; Low-cost cryptography designs from coding theory and combinatorics.

8.3.1.2. Informal International Partners

- Otto-von-Guericke Universität Magdeburg, Institut für Algebra und Geometrie (Germany):
  Study of Boolean functions for cryptographic applications
- Nanyang Technological University (Singapore): cryptanalysis of symmetric primitives.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Dimitrios Simos, SBA Research, Vienna, Austria, February 9-15, 2014;
- Marco Tomamichel, University of Sydney, Sydney, Australia, September 30-October 9, 2014;
- Markku-Juhani O. Saarinen, Norwegian University of Science and Technology, Norway, November 8-30, 2014;
- Céline Blondeau, Aalto University, Finland, November 12-13, 2014.

8.4.2. Internships

- Kaushik Chakraborty, ISI Kolkata (India), May 15-June 15, 2014
- Sébastien Duval, Telecom ParisTech, July-December 2014
- Adrien Hauteville, Univ. Limoges, March-August 2014

8.4.3. Visits to International Teams

- Simons Institute for the Theory of Computing, Berkeley, California, February - March, *Quantum Hamiltonian Complexity Program*: A. Chailloux and A. Leverrier;
- Université Catholique de Louvain-la-Neuve, Belgium, visiting Franoȷis-Xavier Standaert, March 10-11: G. Leurent;
- UAB, Barcelona, Spain, visiting Andreas Winter, October 26 - November 4: A. Chailloux;
- Nanyang Technological University, Singapore, visiting Thomas Peyrin, May 19-June 6: G. Leurent.

SPECFUN Project-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

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 Paris-Sud). Participants: A. Mahboubi, C. Tankink, E. Tassi.
Website: http://paral-itp.lri.fr/.

FastRelax (ANR-14-CE25-0018).
Goal: Develop computer-aided proofs of numerical values, with certified and reasonably tight error bounds, without sacrificing efficiency.
Leader: B. Salvy (Inria, ÉNS Lyon). Participants: A. Mahboubi, Th. Sibut-Pinote.
Website: http://fastrelax.gforge.inria.fr/.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Claudio Sacerdoti Coen (associate professor at the University of Bologna) has been visiting three times a week during 2014. During his stays he collaborated with Enrico Tassi and Dale Miller (team Parsifal) on the design and implementation of a λ-Prolog-inspired programming language well suited to express type-inference algorithms and their extensions.

Fabian Immler (PhD candidate, TUM, Munich, Germany) is working on the formal certification of properties of differential systems, using the Isabelle proof assistant. He visited us for three days in December.

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 who moved from the Vegas team to Marne-la-Vallée university in 2013.

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 symbolic or numeric 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 started on March 1st 2014, coordinated by Guillaume Moroz.

In 2014, the project funded 6 months of internship for Olive Chakraborty and the beginning of the postdoc position of Rémi Imbach. We also organized the first meeting on subdivision methods for singular systems in Nantes in December, see the project website SingCAST.

6.2. International Research Visitors

6.2.1. Visits of International Scientists

6.2.1.1. Internships

Olive Chakraborty

Subject: Numerical algorithms for certified topological and geometrical description of singular curves.

Date: Jun-Dec 2014.

Institution: IIT Pilani, India.

ALF Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. Capacités: Projet "Investissement d'Avenir", 1/11/14 to 31/01/2018

Participants: Damien Hardy, Isabelle Puaut.

The project objective is to develop a hardware and software platform based on manycore architectures, and to demonstrate the relevance of these manycore architectures (and more specifically the Kalray manycore) for several industrial applications. The Kalray MPPA manycore architecture is currently the only one able to meet the needs of embedded systems simultaneously requiring high performance, lower power consumption, and the ability to meet the requirements of critical systems (low latency I/O, deterministic processing times, and dependability). The project partners are Kalray (lead), Airbus, Open-Wide, Safran Sagem, IS2T, Real Time ar Work, Dassault Aviation, Eurocopter, MBDA, Supersonic Imagine, ProbaYes, IRIT, Onera, Verimag, Inria, Irisa, Tima and Armines.

8.1.2. Inria Project Lab: Multicore 2013-2016

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.

8.1.3. 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.

8.1.4. 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).

8.1.5. ANR W-SEPT 2012-2015

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.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. 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/dal.

8.2.1.2. HiPEAC3 NoE

Participants: Pierre Michaud, Erven Rohou, André Seznec.

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.

8.2.2. Collaborations in European Programs, except FP7 & H2020

8.2.2.1. 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

Isabelle Puaut is in the management committee of the COST Action TACLe - Timing Analysis on Code-Level (http://www.tacle.eu). She is responsible of Short Term Scientific Missions (STSM) within TACLe.

8.3. International Initiatives

8.3.1. Participation In International Programs

8.3.1.1. UFGM Chair (Brasil)

Program: Cátedras Francesas UFMG

Title: Compiler Support for emerging parallel architectures

Inria principal investigator: Sylvain Collange

International Partner (Institution - Laboratory - Researcher):

Universidade Federal de Minas Gerais (UFMG) - Computer Science Department - Fernando Pereira

Duration: Sep 2014 - Dec 2014

We propose . The project develop compilation techniques for code optimization to speedup applications that run in Graphics Processing Units (GPUs). The objective is to enable developers code high-performance programs in high-level languages, while taking maximum benefit from the hardware. In particular, we seek to alleviate control and memory divergence, which are important performance limiters specific to GPU architectures. For instance, the call fusion optimization factors out a common function call invoked from multiple independent conditional branches to enable the hardware to execute the function in SIMD mode regardless of branch divergence.

8.3.2. Informal collaborations

The ALF project-team has informal collaborations (visits, common publications) with University of Wisconsin at Madison (Pr Wood), University of Toronto (Pr Moshovos), University of Ghent (Dr Eyerman), University of Upsalla (Pr Hagersten), University of Cyprus (Pr Sazeides), the Egyptian-Japanese University of Science and Technology (Pr Ahmed El-Mahdy).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Dr Stijn Eyerman from University of Ghent has been visiting the ALF project-team in April-May 2014.
- Pr Erik Hagerstern from Uppsala University has been visiting the ALF project-team in September-December 2014
- Pr Fernando Magno Quintão Pereira, from the Federal University of Minas Gerais visited the ALF project for 1 week in January 2014.

8.4.2. Visits to International Teams

Sylvain Collange has been invited on a professor chair at Universidade Federal de Minas Gerais, Brasil (September-December 2014). The subject of the collaboration is "Compiler Support for emerging parallel architectures".

ATEAMS Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. 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.

7.1.2. 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.

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

This is a 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.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Program: FP7 STREP

Project acronym: OSSMeter

Project title: Automated Measurement and Analysis of Open Source Software

Duration: 30 months (2012-10-01 – 2015-03-31)

Coordinator: Scott Hansen

Other partners: CWI, SOFTEAM (France), Tecnalia Research and Innovation (Spain), The Open Group (Belgium), University of L'Aquila (Italy), UNINOVA (Portugal), National Centre for Text Mining University of Manchester (UK), University of York (UK), Unparallel Innovation (Portugal).

7.3. International Research Visitors

7.3.1. Visits of International Scientists

7.3.1.1. Internships

- Cleverton Hentz, PhD Candidate at the Department of Informatics and Applied Mathematics (Dimap) at Federal University of Rio Grande do Norte (UFRN).

CAIRN Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Images & Réseaux Competitivity Cluster - Embrace (2014-2016)

Participants: Raphaël Bardoux, Arnaud Carer, Matthieu Gautier, Olivier Sentieys.

Embrace (Embedded Radio Accelerator) is a project which involves CAIRNand two Small Medium Enterprises (SMEs): Digidia and PrimeGPS. Embrace aims at developing a software radio platform to enable the digital demodulation of HF signals. Both SMEs will use this platform as the first step to implement new products. These products will be dedicated to two different applications (Global Navigation Satellite System and Navigation Safety) at the heart of the markets of the SMEs. CAIRNgoal is the technological transfer of the methods proposed by the team that enable the rapid prototyping of digital radios.

8.2. National Initiatives

The CAIRNteam mainly collaborates with the following laboratories: CEA List, CEA Leti, LEAT Nice, Lab-Sticc (Lorient, Brest), LIRMM (Montpellier, Perpignan), LIP6 Paris, IETR Rennes, DTIM-ONERA Toulouse, LAAS Toulouse, IRIT Toulouse, Inria 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

8.2.1. ANR Blanc - PAVOIS (2012–2016)

Participants: Arnaud Tisserand, Emmanuel Casseau, Philippe Quémerais, Jérémie Métairie, Nicolas Veyrat-Charvillon, 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.

8.2.2. 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.agence-nationale-recherche.fr/en/anr-funded-project/?tx_lwmsuivibilan_pi2[CODE]=ANR-11-INFR-0005. Faon involves Orange Labs, CEA-LETI, University of South Brittany (Lab-STICC laboratory) and Univ. Rennes I (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.

8.2.3. Equipex FIT - Future Internet (of Things)

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

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.

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

Participants: Arnaud Tisserand, Philippe Quémerais.

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

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

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

COMPA (model oriented design of embedded and adaptive multiprocessor) is a project which involves CAIRN, IETR (Rennes) and Lab-STICC (Lorient). The aim of the project is to design adaptive multiprocessor embedded systems for executing dataflow programs. The use case is the 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. Specific scheduling and actor's mapping are also investigated for runtime execution. For more details see http://www.compa-project.org.

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

Participants: Olivier Sentieys, Romuald Rocher, Nicolas Simon.

DEFIS (Design of fixed-point embedded systems) is a project which involves CAIRN, LIP6 (University of Paris 6), 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.

8.2.7. Labex CominLabs - BoWI (2014-2018)

Participants: Olivier Sentieys, Antoine Courtay, Olivier Berder, Pascal Scalart, Arnaud Carer, Viet-Hoa Nguyen, Zhongwei Zheng.

The BoWi project (Body Wold Interactions) aims at designing an accurate gesture and body movement estimation using very-small and low-power wearable sensor nodes. It initially stems from a proposal of the CominLabs think thank focused on the society challenge called Digital Environment for the Citizen. It is also related to the social challenge ICT for Personalized Medicine and to the research track Energy Efficiency in ICT. The main objective of the project is to propose pioneer interfaces for an emerging interacting world based on smart environments (house, media, information and entertainment systems...). Basically the project relies on Wireless Body Areas Sensor Networks; the aim is the accurate Gesture and Body Movement estimation with extremely severe constraints in terms of footprint and power consumption according to on-body energy harvesting perspectives. The BoWI geolocation approach will combine radio communication distance measurement and inertial sensors and it will also strongly benefit from cooperative techniques based on multiple observations and distributed computation. Different types of applications, as health care, activity monitoring and environment control, will be considered and evaluated along with a human-machine interface expertise.

The scientific challenge is global and deals with the solution to be interactively invented by all partners: a short-range geolocation method based on distributed and coopering devices processing multisource data issued from radio-communication distance estimation and integrated inertial sensors. It includes several specific contributions:

- Dynamic and cooperative communication coding and protocol for inter-nodes communications. This includes cooperative communications and protocols such as cooperative MIMO, relaying, error coding, network coding and MAC and wake-up radio protocols.
- Node hardware/software architecture design and self-adaptive distributed processing for geolocation with aggressive low-power run-time optimisation.
- Channel models and antennas for short-range communications. This study will be performed for various radio standards from upcoming BAN 802.15.6, 802.15.4a technologies to future UWB solutions.
- Channel models and antennas for WBASN at millimeter waves. This is a promising perspective for antenna miniaturization, however no front-ends are yet available.
- In depth and specific analysis of human-machine interactions to set system constrains and define user requirement according to various application perspectives.

In practice the BoWi partners aim to deliver the design of basic components, a prototype based on available radio front-ends and energy harvesting devices as well as a system simulator including mm-wave models. Results will also concern the specification of future radio-front ends. The BoWI involves CAIRN, IETR (Rennes), and Lab-STICC (Brest, Lorient, Vannes). For more details see http://www.bowi.cominlabs.ueb.eu/fr.

8.2.8. Labex CominLabs - 3DCORE (2014-2018)

Participants: Olivier Sentieys, Daniel Chillet, Cédric Killian, Jiating Luo, Van Dung Pham.

3DCORE (3D Many-Core Architectures based on Optical Network on Chip) is a project which involves CAIRN, FOTON (Rennes, Lannion) and Institut des Nanotechnologies de Lyon. 3D integration in the ultra deep submicron domain means the implementation of billions of transistors or of hundreds of cores on a single chip with the need to ensure a large number of exchanges between cores, and the obligation to limit the power consumption. Focusing on system integration rather than transistor density, allows for both functional and technological diversification in integrated systems. The functional diversification allows for non-digital functionalities to migrate from the board level into the (on-)chip level. This allows for integration of new technologies that enable high performance, low power, high reliability, low cost, and high design productivity. Use of Optical Network-on-Chip (ONoC) promises to deliver significantly increased bandwidth, increased immunity to electromagnetic noise, decreased latency, and decreased power consumption while wavelength routing and Wavelength Division Multiplexing (WDM) contributes to the valuable properties of optical interconnect by permitting low contention or even contention free routing. WDM allows for multiple signals to be transmitted simultaneously, facilitating higher throughput. Individual realization of CMOS compatible optical components, such as, waveguides, modulators, and detectors lets the community foresee that such integration may be possible in the next ten years. The aim of the project is therefore to investigate new optical interconnect solutions to enhance by 2 to 3 magnitude orders energy efficiency and data rate of on-chip interconnect in the context of a many-core architecture targeting both embedded and high-performance computing. Moreover, we envisage taking advantage of 3D technologies for designing a specific photonic layer suitable for a flexible and energy efficient high-speed optical network on chip (ONoC).

8.2.9. Labex CominLabs - RELIASIC (2014-2018)

Participants: Emmanuel Casseau, Arnaud Tisserand, Huu Van Long Nguyen.

RELIASIC (Reliable Asic) is a project which involves CAIRN, Lab-STICC (University of Bretagne Sud) and IETR (Institut d'Electronique et de Télécommunications de Rennes). One of the most critical challenges of the next design technologies will be fault-tolerant computation. The increase in integration density and the requirement of low-energy consumption can only be sustained through low-powered components, with the drawback of a looser robustness against transient errors. In the near future, electronic gates to process information will be inherently unreliable. New techniques will be required to increase the reliability of operators and components. The aim of the project is to address this problem with a bottom-up approach, starting from an existing application as a use case (a GPS receiver) and adding some redundant mechanisms to allow the GPS receiver to be tolerant to transient errors due to low voltage supply.

8.2.10. Labex CominLabs & Lebesgue - H-A-H (2014-2017)

Participants: Arnaud Tisserand, Nicolas Veyrat-Charvillon, Karim Bigou, Gabriel Gallin.

H-A-H for *Hardware and Arithmetic for Hyperelliptic Curves Cryptography* is a project on advanced arithmetic representation and algorithms for hyper-elliptic curve cryptography. It involves IRISA-CAIRN(Lannion) and IRMAR (Rennes).

Arithmetic has an important role to play in providing algorithms robust against physical attacks (e.g., analysis of the power consumption, electromagnetic radiations or computation timings). Currently, there are only a very few hardware implementations of HECC (without any open source availability). This project will provide novel implementations of HECC based cryptographic algorithms on custom hardware platforms. For more details see http://h-a-h.inria.fr/.

8.3. European Initiatives

8.3.1. 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 - Mar. 2015

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.

8.3.2. FP7 ALMA

Participants: Steven Derrien, Romuald Rocher, Olivier Sentieys, 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 - Nov. 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 multi-core systems-on-chip, software development tools and real world applications. The academic partners will contribute their outstanding expertise in reconfigurable computing and compilation tools development.

8.4. International Initiatives

8.4.1. Inria Associate Teams

8.4.1.1. HARDIESSE

Title: Heterogeneous Accelerators for Reconfigurable DynamIc, Energy efficient, Secure SystEms

International Partner (Institution - Laboratory - Researcher):

University of Massachusetts at Ahmerst (USA)

Duration: 2014 - 2016

See also: https://team.inria.fr/cairn/hardiesse/

Rapid evolutions of applications and standards require frequent in-the-field system modifications and thus strengthen the need for adaptive devices. This need for a strong flexibility, combined with technology evolution (and the so-called power wall) has motivated the surge towards the use of multiple processor cores on a single chip (MPSoC). While it is now clear that we have entered the multi-core era, it is however indisputable that, especially for energy-efficient embedded systems, these architectures will have to be heterogeneous, by combining processor cores and specialized accelerators. We foresee a need for systems able to continuously adapt themselves to changing environments where software updates alone will not be enough for tackling energy management and error tolerance challenges. We believe that a dynamic and transparent adaptation of the hardware structure is the key to success. Security will also be an important challenge for embedded devices. Protections against physical attacks will have to be integrated in all secured components. In this Associated Team, we will study new reconfigurable structures for such hardware accelerators with specific focus on: energy efficiency, runtime dynamic reconfiguration, security, and verification.

8.4.2. Inria International Partners

8.4.2.1. Declared Inria International Partners

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

Department of Computer Science, Lund University (Sweden), Prof. Krzysztof Kuchcinski, Hardware accelerators modeling using constraint-based programming.

Tampere University of Technology (Finland), Prof. Jarmo Takala, From dataflow-based video applications to embedded multicore platforms.

University College Cork (Ireland), Prof. Liam Marnane and Prof. Emanuel Popovici, Arithmetic operators for cryptography, side channel attacks for security evaluation, energy-harvesting sensor networks, and sensor networks for health monitoring.

University of Massachusetts at Amherst (USA), Prof. Russel Tessier and Prof. Maciej Ciesielski, Methods and tools for automatic reconfigurable arithmetic circuit generation.

8.4.2.2. Informal International Partners

Imec (Belgium), Optimization of embedded systems using fixed-point arithmetic.

Electrical Engineering Department, Indian Institute of Technology Delhi (India), Cooperative and MIMO wireless communications.

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

Technical University of Madrid - UPM (Spain),

Optimization of embedded systems using fixed-point arithmetic.

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.

Department of Electrical and Computer Engineering, University of Patras (Greece), Wireless Sensor Networks, data merging, priority scheduling, loop transformations for memory optimizations.

Karlsruhe Institute of Technology - KIT (Germany), Loop parallelization and compilation techniques for embedded multicores.

Ruhr - University of Bochum - RUB (Germany), Reconfigurable architectures.

University of Science and Technology of Hanoi (Vietnam), Participation of several CAIRN's members in the Master ICT / Embedded Systems.

8.4.3. Participation In other International Programs

8.4.3.1. 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.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Prof. Liam Marnane (University College Cork, Ireland) for one week in November (funded by CNRS PICS SpiNaCH project).

Fiona Edwards-Murphy, PhD student, (University College Cork, Ireland) for two weeks in September (funded by CNRS PICS SpiNaCH project).

Prof. Sanjay Rajopadhye (Colorado State University, USA) for one week in June (visiting professor position from University Rennes 1).

8.5.1.1. Internships

Singh Rajhans, B.Eng. student, Indian Institute of Technology Roorkee (Roorkee, India), Intrinsic Fault Tolerance of Hopfield Artificiel Neural Network Model for task scheduling in RSoC, from May 2014 to July 2014 [63].

Jiating Luo, Master's student, École centrale de Pékin (Beijing, China), Design of a Wavelength Allocator for Optical Network-on-Chips, from May 2014 to Sep 2014.

8.5.2. Visits to International Teams

Viet Hoa Nguyen, PhD student, visited IIT Delhi for 3 months between October and December 2014.

Christophe Huriaux, PhD student, visited UMASS for 3 months between May and July 2014.

Steven Derrien visited UMASS for 1 week in December 2014.

CAMUS Team

8. Partnerships and Cooperations

8.1. National Initiatives

Philippe Clauss, Alain Ketterlin, Cédric Bastoul and Vincent Loechner are involved in the Inria Project Lab entitled "Large scale multicore virtualization for performance scaling and portability" and regrouping several french researchers in compilers, parallel computing and program optimization [0]. 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.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, except FP7 & H2020

Program: ITEA

Project acronym: MANY

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

Duration: 09/2011 - 12/2014

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

International Partner (Institution - Laboratory - Researcher):

Universidad de Buenos Aires (ARGENTINE)

Duration: 2011 - ___AT.ANNEEMOISFIN???___

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.

[0] https://team.inria.fr/multicore

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

8.4.1.1. Internships

Matías Hernando Pérez Matías

Date: May 2014 - Nov 2014

Institution: Universidad de Buenos Aires (Argentina)

Sabater César Rufino

Date: May 2014 - Oct 2014

Institution: Universidad Nacional de Rosario (Argentina)

Campostrini Luis Esteban

Date: Jul 2014 - Dec 2014

Institution: Universidad Nacional de Rosario (Argentina)

COMPSYS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. In Relation with the LYONCALCUL Initiative

Compsys follows or participates to the activities of LyonCalcul (http://lyoncalcul.univ-lyon1.fr/), a network to federate activities on high-performance computing in Lyon. In this context, and with the support of the Labex MILYON (http://milyon.universite-lyon.fr/), Compsys organized a thematic quarter on compilation from April 2013 to July 2013 (http://labexcompilation.ens-lyon.fr). A new thematic quarter is in preparation for 2016, initiated by Violaine Louvet (Institute Camille Jordan), with the participation of the LIP teams Avalon, Compsys, and Roma. Also, Alain Darte and Alexandre Isoard have regular exchanges with Violaine Louvet and Thierry Dumont on tiling code optimizations.

8.1.2. Streaming Day with CITI Laboratory

Compsys has some common research interests with the Socrate Inria team from the CITI laboratory (Insa-Lyon), in particular streaming languages. In this context, Socrate (Lionel Morel), with the help of Compsys (Alain Darte), organized in April 2014, a thematic day on the "compilation and execution of streaming programs" in Domaine des Hautannes, St Germain au Mont d'Or, with 7 speakers and 32 participants. See the webpage of the event http://streaming.conf.citi-lab.fr.

8.2. National Initiatives

8.2.1. French Compiler Community

Until 2010, the french compiler community had no official national meetings. Laure Gonnord and Fabrice Rastello decided to motivate the different french actors to meet regularly. All groups whose activities are related to compilation were contacted and the first "compilation day" was organized in September 2010 in Lyon. The next sessions, in a form of 3-days workshops, took place in Aussois (winter 2010), Dinard (spring 2011), Saint-Hippolyte (autumn 2011), Rennes (summer 2012), Annecy (spring 2013, organized by Compsys again), Dammarie-les-lys (winter 2013), and Nice (summer 2014). This effort is a success: the community (http://compilfr.ens-lyon.fr) is now well identified and such an event occurs at least once a year. The community is still animated by Laure Gonnord and Fabrice Rastello, and now also by Florian Brandner (ENSTA), and is now recognized as a sub-group of the CNRS GDRs ASR (Architecture, System, Network) and GPL (Software Engineering and Programming). As a subgroup of GPL, the community is (from 2014) now in charge of organizing one day during the Research school "Ecole des jeunes chercheurs en Algorithmique et Programmation".

8.3. European Initiatives

8.3.1. Collaborations with Major European Organizations: HIPEAC network

Compsys members participate to the European Network of Excellence on High Performance and Embedded Architecture and Compilation (HiPEAC, http://www.hipeac.net/), either as members or affiliate members. The International Workshop on Polyhedral Compilation Techniques (IMPACT, see Section 8.4.1.2), co-created by Christophe Alias in 2011, is now an annual event of the HIPEAC conference, as an official workshop. The 5th edition, IMPACT'15, is co-organized and co-chaired by Alain Darte (see http://impact.gforge.inria.fr/impact2015/).

8.4. International Initiatives

8.4.1. Inria International Partners

8.4.1.1. Declared Inria International Partners

- Christophe Alias has a regular collaboration with Sanjay Rajopadhye from the Colorado State University (USA), through the advising of the PhD thesis of Guillaume Iooss. This year, this collaboration led to several publications, see Sections 6.8 and 6.5 .
- Laure Gonnord has 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 6.4 and 6.3 . In Jan.-Feb. 2015, Compsys will host Fernando Pereira as an invited professor.

8.4.1.2. Polyhedral Community

In 2011, as part of the organization of the workshops at CGO'11, Christophe Alias (with C. Bastoul) organized IMPACT'11 (international workshop on polyhedral compilation techniques, http://impact2011.inrialpes.fr/). This workshop in Chamonix was the very first international event on this topic, although it was introduced by Paul Feautrier in the late 80s. Alain Darte gave the introductory keynote talk. After this first very successful edition (more than 60 people), IMPACT continued as a satellite workshop of the HIPEAC conference, in Paris (2012), Berlin (2013), Vienna (2014). Alain Darte is program chair for the next edition, in Amsterdam (2015). The creation of IMPACT, now the annual event of the polyhedral community, helped to identify this community and to make it more visible. This effort was complemented by the organization of the first (and for the moment unique) school on polyhedral code analysis and optimizations (http://labexcompilation.ens-lyon.fr/polyhedral-school/). Alain Darte also manages two new mailing lists for news (polyhedral-news@listes.ens-lyon.fr) and discussions (polyhedral-discuss@listes.ens-lyon.fr) on polyhedral code analysis and optimizations.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Internships

- Romain Labolle, a L3 ENS-Lyon student, worked, from June 2014 to July 2014, on the adaptation of parametric tiling with inter-tile data reuse to GPUs (reuse for global memory, reuse for shared memory, reuse for registers, i.e., register tiling), supervised by Alain Darte and Alexandre Isoard.
- Shikhar Makkar, a student from the National Institute of Technology Kurukshetra in India, worked, from June 2014 to August 2014, on the mapping of piece-wise affine functions on FPGAs, supervised by Christophe Alias. His internship was funded by the LIP.
- Amir Teshome Wonjiga, a M1 ENS-Lyon student from Ethiopia, worked, from May 2014 to August 2014, on an implementation of an operational semantics of the X10 language, supervised by Paul Feautrier and Laure Gonnord. His internship was funded by Compsys and the LIP.

DREAMPAL Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

The CPER has financed the visit of Prof. Dorel Lucanu from Univ. Iasi (Romania) in July and August 2014.

7.2. International Initiatives

7.2.1. Participation In other International Programs

Wissem Chouchene is financed by the Euramus Mondus programme.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

Prof. Dorel Lucanu from Univ. Iasi (Romania) visited us in July and August 2014. We continued 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 communication IPs.

GCG Team

8. Partnerships and Cooperations

8.1. International Initiatives

8.1.1. Inria International Partners

8.1.1.1. Informal International Partners

- P. Sadayappan, OSU, Columbus, Ohio, USA: Collaboration on automatic analysis of I/O complexity (several co-publications); collaboration on code optimization (one join paper + one submitted paper)
- Fernando Pereira, UFMG, Bello Horizonte, Brazil: Collaboration on static analysis (on join paper); collaboration on hybrid analysis (one submitted paper)

8.2. International Research Visitors

8.2.1. Visits of International Scientists

- Prof. Fernando Magno Pereira, 1 months 1/2, UFMG Brazil

8.2.2. Visits to International Teams

8.2.2.1. Research stays abroad

- Fabrice Rastello: 2 months at OSU, Columbus, Ohio with the team of P. Sadayappan.

PAREO Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

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

We are also involved in the GDR-GPL (CNRS Research Network on Software Engineering), as a member of the FORWAL group and member of the Scientific Board of the GDR.

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7 & H2020

Program: PHC Polonium

Project title: Expressing concurrency through control operators

Duration: January 2015 - December 2016

Coordinator: Sergueï Lenglet

Other partner: Institute of Computer Science, University of Wrocław, Poland

Abstract: The goal of this project is to explore the interplay between concurrency, continuations, and control operators at a fundamental level. We do not restrict ourselves to a specific programming language, but we use more general and well established formal models, namely process calculi (such as the π-calculus) for concurrency, and the λ-calculus (a model of sequential functional programming) for continuations and control operators. We want to find new connections between concurrency and control operators, and especially new ways of implementing concurrent and distributed programs with the help of control operators.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

7.3.1.1. Internships

Nauval Atmaja

Subject: Property Based Testing

Date: from Feb 2014 until Jun 2014

Institution: Erasmus Mundus MSc in Dependable Software Systems

POSTALE Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

- **CALIFHA project (DIM Digiteo 2011)**: CALculations of Incompressible Fluid flows on Heterogeneous Architectures. Funding for a PhD student. Collaboration with LIMSI/CNRS. Participants: Marc Baboulin (Principal Investigator), Joel Falcou, Yann Fraigneau (LIMSI), Laura Grigori, Olivier Le Maître (LIMSI), Laurent Martin Witkowski (LIMSI)

7.2. National Initiatives

- **EDF**: Contract with EDF on improving performance and designing algorithms of iterative solvers on parallel machines with accelerators (Marc Baboulin). This contract enables to hire a postdoc researcher in October 2014.
  Participants: Marc Baboulin, Amal Khabou.
- **Lal/In2P3/CERN** The collaboration with CERN and LAL/IN2P3 + LRI focuses on LHCb and Atlas tracker code optimization. Those experiments must analyze results in realtime (10ms for analyzing particle trajectography). Early results show that these tracking algorithms can run in real time on SIMD multicore General Purpose Processor and on Xeon-Phi.
  Participant: Lionel Lacassagne.
- **Inserm** Contract with Paris X / INSERM U669 (Christophe Genolini) in the R++ project. R++ is an open source effort to modernize and increase performance of the R language used by scientists to develop statistical analysis tools. Funding for one research engineer has been received to support this project.
  Participant: Joël Falcou.
- **followup of the ANR Cosinus project PetaQCD - Towards PetaFlops for Lattice Quantum ChromoDynamics** Collaboration with Lal (Orsay), LPT (Orsay), LABRI (Bordeaux). About the design of architecture, software tools and algorithms for Lattice Quantum Chromodynamics.
  Participants: Christine Eisenbeis, Michael Kruse, Konstantin Petrov.

7.3. European Initiatives

7.3.1. ITEA

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.
Participants: Lénaïc Bagnères, Cédric Bastoul, Taj Muhammad Khan.

7.4. International Initiatives

7.4.1. Inria Associate Teams

Participants: Marc Baboulin, Jack Dongarra.

R-LAS is an Inria associate team with University of Tennessee,(https://www.lri.fr/~baboulin/r-las.html), 2014-2017.

This project is proposed in the context of developing a class of fast algorithms based on randomization for numerical linear algebra solvers. The funding was used in 2014 to cover exchange visits for researchers and PhD students from Inria and University of Tennessee.

7.4.1.1. Informal International Partners

- **Lawrence Berkeley National Laboratory** - USA: collaboration of Marc Baboulin with Sherry Li on application of randomization techniques to the solution of large sparse linear systems using direct methods (joint publications and co-organizations of mini-symposia for SIAM conferences).
- **Old Dominion University** - USA: Collaboration with Pr. Masha Sosonkina on locality optimization for numerical linear algebra solvers (joint publication) and preconditioned Krylov subspace methods (PhD thesis of Aygül Jamal, starting in October 2014).
- **Louisiana State University** - USA: collaboration of Joel Falcou with the STELLAR team in the framework of the HPX project (Hartmut Kaiser). It is mainly related to the design and implementation of a C++ asynchronous runtime system. In this framework, the STELLAR team hosted 2 PhD students of the Postale team for extended visits in 2013 and 2014.
- **Texas A&M University** - USA: collaboration of Joel Falcou with the PARASOL team in the framework of the STAPL project (Lawrence Rauchwerger). It is mainly related to the applicability of parallel skeletons inside STAPL on large scale parallel machines.
- **University of Illinois at Urbanna Champaign** (UIUC) - USA, in the context of the Inria Joint Laboratory for Petascale computing. Since 2011, we have initiated collaborations with researchers from UIUC (Wen-mei Hwu, Karl Rupp) in the area of numerical software.
- **University of Manchester**: collaboration with Professors Nick Higham and Françoise Tisseur on random orthogonal matrices and fault-tolerant linear algebra algorithms (Amal Khabou).
- **University of California - Irvine**: collaboration of Christine Eisenbeis with Professor Jean-Luc Gaudiot on Application Characterization for Modern Multicore Architectures

7.4.2. Participation In other International Programs

Stic AmSud: BioCloud-EEAmSud **Participants:** Christine Eisenbeis, Alessandro Ferreira Leite, Claude Tadonki.

BioCloud-EEAmSud is a cooperation project integrated by Brazil, Chile and France following the 2012 STIC-AmSud call. Partners in Brazil are Universidade de Brasilia, Universidade Federal Fluminense, and EMBRAPA-Genetic Resources and Biotechnology (CENARGEN), through the support of the Coordination of Improvement of Senior Staff of the Ministry of Education in Brazil (CAPES). In Chile, the main partner is Universidad de Santiago de Chile, through the support of the National Commission for Scientific and Technological Research of Chile (CONICYT). In France, the institutions involved are Mines ParisTech (CRI) and Inria-Saclay, through the support of the Ministry of Foreign and European Affairs (MAEE). The international project coordinator is Pr. Maria Emília Machado Telles Walter (UnB). Alessandro Ferreira Leite' thesis work is a joint University of Brazilia - université Paris-Sud 11 thesis and is partially supported by BioCloud-EEAmSud. Maria Emilia Machado Telles Walter and Alba Cristian de Melo visited Grand-Large in 2013, as well as Taina Rajol.

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- Masha Sosokina (Professor, Old Dominion University, USA), June 10-13, 2014.
- Tingxing Tim Dong (PhD student, University of Tennessee, USA), August 25-26, 2014.
- Anthony Danalis (University of Tennessee, USA), December 15-16, 2014.
- Tetsuya Sakurai (University of Tsukuba, Japan), December 15-16, 2014.
- Jose Roman (University of Valencia, Spain), December 15-16, 2014.
- Jean-Luc Gaudiot, UCLA, Irvine, March 3rd, September 4th, November 24th, 2014.

TASC Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Atlanstic

Participants: Raphael Chenouard, Laurent Granvilliers, Christophe Jermann, Frédéric Lardeux, Éric Monfroy, Frédéric Saubion.

Title: Atlanstic project about problem modelisation, conversion, and transformation.

Duration: 2014-2015.

Budget: 8000 Euros.

Others partners: LERIA, IRCYNN.

Topic: modelling and model transformation.

8.1.2. EPOC

Participants: Nicolas Beldiceanu, Didier Lime, Gilles Madi Wamba, Jean-Marc Menaud, Olivier H. Roux.

Title: EPOC: Energy Proportional and Opportunistic Computing system.

Duration: 2014-2017.

Budget: founding for a PhD thesis.

Topic: an integrated approach combining time automata and constraint programming for modeling dynamic aspects of vm management in a data center.

8.2. National Initiatives

8.2.1. IBEX

Participants: Ignacio Araya, Clément Carbonnel, Gilles Chabert, Benoit Desrochers, Luc Jaulin, Bertrand Neveu, Jordan Ninin, Gilles Trombettoni.

Title: Development of IBEX.

Others partners: ENSTA Bretagne, ENPC PariTech, Lirmm, LAAS, University Federico Santa Maria, Chile.

Development of IBEX (see Section 6.3).

8.2.2. SUSTAIN

Participants: Charlotte Truchet, Bruno Belin.

Title: SUSTAINS.

Duration: 2010-2014.

Type: FUI.

Budget: 151400 Euros.

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

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

8.2.3. ANR NetWMS2

Participants: Gilles Chabert, Ignacio Salas Donoso, Nicolas Beldiceanu.

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

Duration: 2011-2014.

Type: cosinus research program.

Budget: 189909 Euros.

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

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

8.2.4. ANR INFRA-JVM

Participants: Xavier Lorca, Charles Prud'Homme.

Title: Towards a Java Virtual Machine for pervasive computing.

Duration: 2011-2015.

Type: **new project**.

Budget: 78000 Euros.

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

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

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

The GRACeFUL project (Global systems Rapid Assessment tools through Constraint FUnctional Languages) from the H2020-FETPROACT track has been accepted and will start in January 2015 for a period of three year. The abstract of the project is given below.

The making of policies coping with Global Systems is a process that necessarily involves stakeholders from diverse disciplines, each with their own interests, constraints and objectives. People play a central role in such collective decision making and the quest for solutions to a problem generally intertwines its very specification. Simulators can assist in this process provided they employ adequate high-level modelling to separate the political question from the underlying scientific details. Domain-specific Languages (DSL) embedded in Functional Programming (FP) languages offer a promising way to implement scalable and verifiable simulators. But the use of simulators is essentially a trial-and-error process too tedious for execution in a group session. A paradigm shift is needed towards active problem solving where stakeholders' objectives can be taken along from the very beginning. Constraint Programming (CP) has demonstrated to enable such a shift for e.g. managed physical systems like water and power networks. This project lays the base for a DSL aimed at building scalable Rapid Assessment Tools for collective policy making in global systems. This can be achieved through foundational scientific work at different levels: from the high-level, political modelling,

adapting the social discipline of Group Model Building (as used in business organizations), through visual forms of CP as well as gamification aspects, down to the needs for a host language, combining CP and FP. Special emphasis is put on domain-specific constraints, constraint composition, and composable solvers and heuristics. Results are applied and validated for the problem case of Climate-Resilient Urban Design, but the ambition is a general framework applicable to many other systems. The case study is assessed by an external multi-disciplinary Advisory Board of Stakeholders that guides the specification process and evaluates needs and usability of the tools.

8.3.2. Collaborations in European Programs, except FP7 & H2020

8.3.2.1. PHC Ulysses

Participants: Charlotte Truchet, Florian Richoux, Alejandro Reyes.

Title: Development and estimation analysis of massively parallel local search approaches to the k-medoids problem.
Duration: 2014.
Type: **new project**.
Budget: 2500 Euros.
Others partners: 4C (Cork, Ireland).

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

8.4. International Initiatives

8.4.1. Inria Associate Teams

8.4.1.1. TASCMELB

Title: Synergy between Filtering and Explanations for Scheduling and Placement Constraints
International Partner (Institution - Laboratory - Researcher):
NICTA (AUSTRALIE)
Duration: 2014 - 2016
See also: http://www.normalesup.org/ truchet/TASCMELB.html
In the context of Constraint Programming and SAT the project addresses the synergy between filtering (removing values from variables) and explanations (explaining why values were removed in term of clauses) in order to handle in a more efficient way correlated resource scheduling and placement constraints. It combines the strong point of Constraint Programming, namely removing value that leads to infeasibility, with the strong point of SAT, namely taking advantage from past failure in order to quickly identify infeasible sub-problems.

8.4.1.2. 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.

8.4.2. Inria International Partners

8.4.2.1. Informal International Partners

- SICS, Sweden.
- Uppsala University, Sweden.
- 4C, Ireland.
- Univ. Austral de Chile, Valparaiso, Chile.

8.4.3. Participation In other International Programs

Ulysse (cooperation with 4C, Cork, Ireland).

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Mats Carlsson (SICS, Sweden), *Automata constraints* (5 days).
- Philippe Codognet (Japanese-French Laboratory for Informatics at the University of Tokyo, Japan), *Prediction models of local search speed-up* (15 days).
- Pierre Flener, (Uppsala University, Sweden), *Automata constraints* (5 days).
- Justin Pearson, (Uppsala University, Sweden), *Automata constraints* (5 days).
- Helmut Simonis, (Insight Centre for Data Analytics, University College Cork, Ireland), *Learning constraint models* (3 months).

8.5.2. Visits to International Teams

8.5.2.1. Sabbatical programme

Thierry Petit is currently visiting the Foisie School of business of WPI (Worcester Polytechnic Institute, Massachusetts, USA), collaborating with Andrew C. Trapp on optimization problems, since July, 2014.

8.5.2.2. Research stays abroad

- Nicolas Beldiceanu, 4C Cork Ireland: work on *learning generic models* and work on *learning constraints in the context of EDF* with Helmut Simonis (two weeks).
- Nicolas Beldiceanu, Uppsala University and SICS: work on *automata and constraints* with Pierre Flener and Justin Pearson and Mats Carlsson (one month).
- Éric Monfroy, Univ. Austral de Chile, Valparaiso, Chile: work with Ricardo Soto.
- Florian Richoux visited the Japanese-French Laboratory for Informatics at the University of Tokyo, to work with Philippe Codognet on massively parallel combinatorial optimization algorithms and to start collaborations on Game AI, with Ruck Thawonmas from Ritsumeikan University (from the 1st of April till the 31st of August).

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 2015, and was subject of extensive preparation at the end of 2014.

The ANR HOPE project 8.2.1.1 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 8.2.1.1). Similarly, the CLISTINE FUI project was labeled by the platform as microelectronic branch of the SCS competitiveness cluster.

8.2. National Initiatives

8.2.1. ANR

8.2.1.1. 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.
Although this project was officially started in November 2013, 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. A publication on multiview modeling (including performance, power, and temperature) was presented at FDL'2014, reflecting Ameni Khecharem ongoing PhD work.

8.2.1.2. 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 CLISTINE

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

This project was started in Oct 2013, aprovides PhD funding for Amine Oueslati. 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). We started a thorough classification of parallel program types (konown as "Dwarfs" in teh literature), to provide benchmarks to evaluate the platform design options.

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 with the kick-off meeting held on April, 2013 for administrative reasons. Research will target solutions for probabilistic component-based models, and a Ph.D. thesis should start at latest on September 2015. The goal is to unify in a common framework probabilistic scheduling techniques with compositional assume/guarantee contracts that have different levels of criticality.

8.2.3.2. CLARITY

Participants: Yann Bondue, Julien Deantoni, Robert de Simone, Marie Agnès Peraldi-Frati.

This project is funded by the LEOC Call (*Logiciel Embarqué et Objets Connectés*) of the national support programme *Investissements d'Avenir*. It was started in September 2014 , and a kick-of meeting was held on October 9th. Partners are: Thales (several divisions), Airbus, Areva, Altran, All4Tec, Artal, the Eclipse Fondation, Scilab Enterprises, CESAMES, U. Rennes, and Inria. The purpose of teh project is to develop and promote an open-source version of the ARCADIA Melody system design environment from Thales, renamed CAPPELLA for that purpose.

8.2.3.3. Capacites

Participants: Liliana Cucu-Grosjean, Dumitru Potop-Butucaru, Yves Sorel, Walid Talaboulma.

This project is funded by the LEOC Call (*Logiciel Embarqué et Objets Connectés*) of the national support programme *Investissements d'Avenir*. It has started on November 1st, 2014 with the kick-off meeting held on November, 12th 2014. The project cordinator is Kalray, and teh objective of the project is to stydy relevance of Kalray-style MPPA processor array for real-time computation in the avionic domain (with partners such as Airbus for instance).

8.3. European Initiatives

8.3.1. Collaborations in European Programs, except FP7 & H2020

8.3.1.1. 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 International Labs

8.4.1.1. HADES LIAMA project

This joint project is held in collaboration with ECNU Shanghai, together with the Scale Inria team, and extends in scope the Associated Team DAESD (see below). As part of this project Frédéric Mallet spends a sabbatical year at ECNU Shanghai, partly funded by an Inria delegation programme.
We attended a number of LIAMA meetings, both in France and in Beijing, most often in confcall form.

8.4.2. Inria Associate Teams

8.4.2.1. DAESD

Title: Distributed/Asynchronous and Embedded/synchronous Systems Development

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

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 Summer School was organized this year in Shanghai (July 8-11), with participation of Julien Deantoni and Frédéric Mallet from Aoste.
DAESD is strongly linked with the LIAMA project HADES, that it supports.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Invited Professor

Qingguo XU

Date: July 2014 to June 2015

Institution: Shanghai University (China)

8.5.2. Visits to International Teams

8.5.2.1. Sabbatical programme

Mallet Frédéric

Date: Sep 2014 - Aug 2015

Institution: ECNU (China)

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 [0] 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) modeling 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 § 6.5.4) 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 [0] (*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-machine interfaces formally using the LNT language and in verifying them using CADP (see § 6.5.7).

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*) Motwin 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.

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

Bluesky started in September 2012 for three years. The main contributions of CONVECS to Bluesky (see § 6.1.3 and § 6.5.5) are the definition of GRL, the formal pivot language for describing the asynchronous behavior of logic controller networks, and the automated verification of the behavior using compositional model checking and equivalence checking techniques.

8.1.3. Other National Collaborations

Additionally, we collaborated in 2014 with the following Inria project-teams:

- OASIS (Inria Sophia-Antipolis – Méditerranée): Eric Madelaine and Ludovic Henrio,
- ESTASYS (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 (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),
- Christophe Deleuze, Ioannis Parissis, and Mouna Tka Mnad (LCIS, Valence),
- Pascal Poizat (LIP6, Paris).

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. SENSATION

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

SENSATION [0] (*Self ENergy-Supporting Autonomous computaTION*) is a European project no. 318490 funded by the FP7-ICT-11-8 programme. It gathers 9 participants: Inria (ESTASYS 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 (see § 6.3.1), studying common semantic models for quantitative analysis, and applying formal modeling and analysis to the case studies provided by the industrial partners (see § 6.5.6).

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 [0]. R. Mateescu was the chairman of the FMICS working group until November 1st, 2014. H. Garavel is member of the FMICS board, in charge of dissemination actions.

[0] http://sensation-project.eu/
[0] http://fmics.inria.fr

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 2014 with several European universities and research centers, including:

- Saarland University (Alexander Graf-Brill, Holger Hermanns, and Felix Freiberger),
- RWTH Aachen (Joost-Pieter Katoen and Xiaoxiao Yang),
- 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 (Carlos Canal, Francisco Duran and Ernesto Pimentel), and
- Brandenburg University of Technology Cottbus - Senftenberg (Monika Heiner).

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

8.3.1. Inria International Labs

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.

8.3.2. Other International Collaborations

In 2014, we had scientific relations with several universities abroad, including:

- University of California at Santa Barbara, USA (Tevfik Bultan),
- University of Utah, USA (Chris Myers and Zhen Zhang), and
- Universidad Nacional de Cordoba, Argentina (Pedro d'Argenio).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Alexandre Hamez (ISAE, Toulouse) visited us on March 26-28, 2014. He gave a seminar entitled "*Symbolic Model Checking and Hierarchical Set Decision Diagrams*".
- Chris Myers (University of Utah, USA) visited us from July 7–11, 2014. He gave a talk entitled "*Genetic Design Automation*" on July 8, 2014.
- The annual CONVECS seminar was held in Herbelon (France) on June 23-25, 2014. The following invited scientists attended the seminar:
  - Laurence Pierre (TIMA, Grenoble, France) gave on June 23, 2014 a talk entitled "*Verification of Correctness and Safety Requirements for SoC Models*".
  - Matthias Güdemann (Systerel, Aix-en-Provence) gave on June 24, 2014 a talk entitled "*Industrial Formal Methods*".
  - Lom Messan Hillah (LIP6, Paris) gave on June 25, 2014 a talk entitled "*Formal Methods in Model-Driven Development and Model-Driven Development in Formal Methods: Practice Makes a Better Bridge*".

HYCOMES Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

- Ayman Aljarbouh's PhD is partially funded by an ARED grant of the Brittany Regional Council. His doctoral work takes place in the context of the Modrio and Sys2Soft projects on hybrid systems modeling — see sections 7.3.1 and 7.2 . Ayman Aljarbouh is working on accelerated simulation techniques for hybrid systems. In particular, he is focusing on the regularisation, at runtime, of chattering behaviour and the approximation of Zeno behaviour.
- Benoît Caillaud is participating to the S3PM project of the CominLabs excellence laboratory [0]. This project focuses on the computation of surgical procedural knowledge models from recordings of individual procedures, and their execution [24]. 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.

7.2. 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.

7.3. European Initiatives

7.3.1. Collaborations in European Programs, except FP7 & H2020

Program: ITEA2

Project acronym: Modrio

Project title: Model Driven Physical Systems Operation

Duration: September 2012 – November 2015

Coordinator: EDF (France)

[0] http://www.cominlabs.ueb.eu/themes/project/

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).

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.

7.4. International Initiatives

7.4.1. Inria International Partners

7.4.1.1. Informal International Partners

Extending beyond the context of the Modrio project (see section 7.3.1 , the Hycomes team is collaborating with the team of Dassault Systems, located in Lund (Sweden), in charge of developping Dymola, one of the major software tools in the Modelica community.

MUTANT Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

7.1.1.1. 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.

7.1.2. Other National Initiatives

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

The team is also an active member of the ANR network CHRONOS (investigator Gérard Berry, Collège de France).

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7 & H2020

Mutant has started a cooperation with the team of Christoph Kirsch at the University of Salzburg, Austria, around the application of the application of the Logical Execution Time realtime programming paradigm to computer music systems supporting advanced temporal structure in music and advanced dynamics in interactivity. We have settled a project LETITBE accepted in the program PHC Amadeus, and to be started in january 2015.

7.3. International Initiatives

7.3.1. Inria International Partners

7.3.1.1. Informal International Partners

- Shlomo Dubnov (UCSD)
- Edward Lee (UC Berkeley)
- Miller Puckette (UCSD)
- Masahiko Sakai (U. Nagoya)
- Slawek Staworko (U. Edinburgh)
- David Wessel (UC Berkeley)

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Masahiko Sakai (Professor at the University of Nagoya) visited MuTant for two weeks in April and October 2014, For collaborations on term rewriting techniques applied to the representations of rhythm in music notations.

Slawek Staworko (LINKS, on leave at U. of Edinburgh) visited MuTant for two weeks in June and July 2014, for collaborations on the problem of automatic rhythm transcriptions.

7.4.2. Visits to International Teams

MuTant team members Arshia Cont, Jean-Louis Giavitto and José Echeveste made a formal visit to M.I.T. MediaLab in May 2014 to showcase MuTant work and discuss further collaborations with several New Media teams at MIT.

7.4.2.1. Research stays abroad

José Echeveste stays during six weeks in several Universities of United States which enables collaborations with the following teams and centers:

- Center for Hybrid and Embedded Software Systems (UC Berkeley)
- The Center for New Music and Audio Technologies (UC Berkeley)
- Center for Computer Research in Music and Acoustics (Stanford)
- Roger Dannenberg's team (Carnegie Mellon University)
- Computer Music Center (Columbia University)

This trip allows to share research experience with many people with different areas of expertise and to broadly disseminate the Mutant team work in the main computer music centers and other important computer research centers of United States.

José Echeveste (MuTant PhD students) undertook a Research Stay in UC Berkeley's EECS department, Center for Hybrid and Embedded Software Systems (CHESS) for two months between April and May 2014. His visit was highlighted by several master classes and workshops on MuTant research in diverse institutions such as UC Berkeley, Columbia University and MIT.

PARKAS Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. 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 CAFEIN, 2013-2015. Marc Pouzet.

7.1.2. 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), Alain Darte (COMPSYS, Lyon), Fabrice Rastello (CORSE, Grenoble).

7.1.3. Others

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

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. COPCAMS

Type: ARTEMIS JU

Defi: NC

Instrument: ASP

Objectif: NC

Duration: April 2013 - March 2016

Coordinator: Christian Fabre

Partner: CEA LETI, Grenoble, France

Inria contact: Albert Cohen

Abstract: Cognitive cameras on manycore platforms

7.2.1.2. EMC2

Type: ARTEMIS JU

Defi: NC

Instrument: AIPP

Objectif: NC

Duration: April 2014 - March 2917

Coordinator: Werner Weber

Partner: Infineon, Munich ,Germany

Inria contact: Albert Cohen

Abstract: Embedded multicrical systems on multicores

7.2.1.3. ITEA2

Type: ITEA2

Defi: NC

Instrument: NC

Objectif: NC

Duration: September 2012 - November 2015

Coordinator: Daniel Bouskela (EDF)

Partner: Dassault-Systèmes, EDF, Modelon, DLR (Germany)

Inria contact: Benoit Caillaud, Marc Pouzet

Abstract: Model Driven Physical Systems Operation

7.3. International Initiatives

7.3.1. Inria Associate Teams

7.3.1.1. POLYFLOW

Title: Polyhedral Compilation for Data-Flow Programming Languages

International Partner (Institution - Laboratory - Researcher):

IISc Bangalore (INDE)

Duration: 2013 - 2015/12

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.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Prof. Cesare Tinelli, was invited by ENS in the PARKAS team.

Date: June 2014 (one month)

Institution: Iowa State University, USA.

7.4.1.1. Internships

Siddharth Prusty Siddharth

Date: May 2014 - Jul 2014

Institution: IITK (India)

Vijay Keswani Vijay

Date: May 2014 - Jul 2014

Institution: IITK (India)

Quentin Bunel

Date: May 2014 - Jul 2014

Institution: UPMC (France)

Abhishek Jain

Date: May 2014 - Jul 2014 and Dec 2014 - Jan 2015

Institution: IITD (India)

Yabin Hu

Date: Jun 2014 - Jul 2014

Institution: China Nat. Univ. of Defense and Technology (China)

SPADES Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR Projects

8.1.1.1. PiCoq (ANR project)

Participant: 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)

Participant: 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. European Initiatives

8.2.1. Collaborations in European Programs, except FP7 & H2020

Program: COST

Project acronym: IC1405

Project title: Reversible Computation

Duration: 2015-2019

Coordinator: I. Ulidowski (U. Leicester, UK)

Abstract: This recently launched COST Action aims to establisjh a research network of excellence on reversible commputation. Reversible computation is an emerging paradigm that extends the standard forward-only mode of computation with the ability to execute in reverse, so that computation can run backwards as naturally as it can go forwards. It aims to deliver novel computing devices and software. the potential benefits include the design of new reversible logic gates and circuits – leading to low-power computing –, and new conceptual frameworks, language abstractions and software tools for reliable and recovery-oriented distributed systems.

8.3. International Initiatives

8.3.1. Inria Associate Teams

8.3.1.1. RIPPES

Title: RIgorous Programming of Predictable Embedded Systems

International Partner (Institution - Laboratory - Researcher):

University of California Berkeley (USA)

University of Auckland (New Zealand)

Duration: 2013 - 2015

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

The RIPPES associated teams gathers the SPADES team from Inria Grenoble Rhône-Alpes, the Ptolemy group from UC Berkeley (EECS Department), and the Embedded Systems Research group from U. 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.

8.3.2. Inria International Partners

8.3.2.1. Informal International Partners

University of Bologna, Department of Computer Science (Italy)

Topics: reversibility in concurrent languages

TU Braunschweig, (Germany)

Topics: typical worst-case schedulability analysis

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- April 2014: Eugene Yip (PhD student, U. Auckland) visited Inria Grenoble to work on the semantics of the FOREC PRET programming language (RIPPES associated team).

- April 2014: David Broman (Ass. Prof. KTH Stockholm and UC Berkeley) visited Inria Grenoble to attend the RePP'14 workshop and to work on PRET programming (RIPPES associated team).
- September 2014: Ismail Assayad (Ass. Prof. U. Casablanca) visited Inria Grenoble to work on multi-criteria optimization and scheduling for embedded system.
- September 2014: Lilia Sfaxi (Ass. Prof. ENSI Tunis) and Imen Boudabous (PhD student, ENSI Tunis) visited Inria Grenoble to work on scheduling and energy optimization of data-flow applications on multi-core chips.
- November and December 2014: Partha Roop (Senior Lecturer, U. Auckland) and Hugh Wang (PhD student, U. Auckland) visited Inria Grenoble to work on the FOREC PRET programming language (RIPPES associated team).

8.4.2. Visits to International Teams

- Alain Girault visited UC Berkeley (USA) in February 2014 to work on the parametric dataflow model of computation and on PRET programming (RIPPES associated team).

TEA Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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.

——

Program: ANR

Project acronym: **Feever**

Project title: Faust Environment Everyware

Duration: 2014-2016

Coordinator:

Other partners:

URL: http://www.feever.fr

Abstract:

The aim of project FEEVER is to ready the Faust music synthesis language for the Web. In this context, we collaborate with Mines ParisTech to define a type system suitable to model music signals timed at multiple rates and to formally support playing music synthesised from different physical locations.

8.1.2. 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 ITEA2 OPEES and Artemisia CESAR 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 TEA 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..

8.1.3. PAI 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 TEA is to define a specification method and to provide a generator of multi-task applications.

8.2. International Initiatives

8.2.1. International Project Grants

8.2.1.1. USAF Office for Scientific Research – 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 (Institution - Laboratory - Researcher):

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

Abstract: 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.

8.2.2. Inria International Partners

8.2.2.1. Declared Inria International Partners

8.2.2.1.1. The University of Hong Kong

Title: Virtual Prototyping of embedded software architectures

International Partner (Institution - Laboratory - Researcher):

The University of Hong Kong (Hong ,Kong)

Duration: 2012 - now

We collaborate with John Koo at the University of Hong Kong (HKU) and the LIAMA since two years through visiting grants of the Chinese Academy of Science and of the University of Rennes on the topics of heterogeneous time modelling and virtual prototyping. We submitted an ANR project proposal on this topic.

An engineer of SIAT, Riu Li, has developed a pilot project to evaluate Polychrony in the context of virtual prototyping and real-time simulation of automotive systems (the controller of a V6 turbo-charged engine model in LMS [0]). Our collaboration started in 2011 at the occasion of a joint Summer School on Embedded Systems organised by SIAT and LIAMA at SIAT. John Koo was invited scientist at Inria-Rennes in Summer 2012 and Jean-Pierre Talpin invited at SIAT by the Chinese Academy of Science from December 2012 to August 2013.

The partners submitted a PHC proposal and intend to resubmit a joint project proposal for the ANR-HK international program. A longer term goal of our collaboration is to setup, within the IET, a joint laboratory with Inria, in order to both disseminate formal methods for embedded system design on a specific Master program, and jointly contribute to an open-source system design platform with European and Asian industrial partners which are sponsoring the IET.

8.2.2.1.2. Virginia Tech Research Laboratories

Title: Models of computation for embedded software design

International Partner (Institution - Laboratory - Researcher):

Virginia Tech Research Laboratories (USA)

Duration: 2003 - now

Team TEA collaborates with Sandeep Shukla, Virginia Tech, since 2002. First, in the frame of the NSF-Inria program with Rajesh Gupta, UCSD, until 2004; Inria’s associated project BALBOA, until 2007; with the sabbatical of Sandeep Shukla at IRISA in 2008-2009 (funded by Inria-Rennes, the University of Rennes 1, Inria’s scientific board); and, from 2011 to 2013, in the context of the associate-project POLYCORE, together with the ESG group at TU Kaiserslautern.

Following up Sandeep’s sabbatical, the Fermat Laboratory was awarded a series of research grant by the US Air Force Research Laboratory (AFRL) to develop a modelling environment based on Polychrony. In this context, Virginia Tech hired a former PhD. of team ESPRESSO, Julien Ouy, to contribute and coordinate this project’s work. Since 2013, the scope of our collaboration has extended with the three years grant awarded to team TEA by the USAF Office for Scientific Research (AFOSR).

To date, our fruitful and sustained collaboration has yield the creation of the ACM-IEEE MEMOCODE conference series [0] in 2003, of the ACM-SIGDA FMGALS workshop series, and of a full-day tutorial at ACM-IEEE DATE’09 on formal methods in system design. We have jointly edited

[0] LMS by Siemens http://www.plm.automation.siemens.com/en_us/products/lms

[0] ACM-IEEE MEMOCODE conference series. http://memocode-conference.com

two books with Springer [00], two special issues of the IEEE Transactions on Computers and one of the IEEE Transactions on Industrial Informatics, and published more than 30 joint papers in international scientific journals and conferences.

8.2.2.2. Informal International Partners

8.2.2.2.1. Technische Universitaet Kaiserslautern (DE)

We collaborate with Klaus Schneider, leader of the ESG group at Uni. Kaiserslautern, since 2011 in the frame of the POLYCORE associate project. Our aim is to develop a joint, open-source, toolchain based on the Averest (ESG) and POP (TEA) environments. Our collaboration has been quite fruitful with several recent journal publications [00]. Numerous visits and exchanges of personnel between team TEA and the ESG have allowed us to develop ONYX, a cross-compiler between the Averest and POP environments.

Onyx mixes imperative Quartz modules and declarative Signal networks to specify multi-clocked systems. We intend to further its development by the submission of a joint ANR or European project. Our objective is to develop an environment capable of synthesising distributed, loosely synchronised executives from imperative Quartz modules whose schedules are specified by multi-clocked data-flow specifications. A new version of this front-end, developed by Sun Ke, will be integrated in the POP environment.

8.3. International Research Visitors

8.3.1. Visits to International Teams

8.3.1.1. Research stays abroad

Jean-Pierre Talpin was awarded a visiting researcher grant by the US Air Force Research Laboratories for collaborative research with the Virginia Tech Research Laboratories. In this context, he visited the Arlington and Falls Church VT campuses in Spring, Summer and Fall 2014 for a duration of two and a half months.

[0] *Formal methods and models for system design*, R. Gupta, S. Shukla, J.-P. Talpin, Eds. ISBN 1-4020-8051-4. Springer, 2004.

[0] *Synthesis of embedded systems*. S. Shukla, J.-P. Talpin, Eds. ISBN 978-1-4419-6399-4. Springer, 2010

[0] *Embedding polychrony into synchrony*. J. Brandt, M. Gemünde, K. Schneider, S. Shukla, and J.-P. Talpin. In Transactions on Software Engineering (TSE). IEEE, 2012.

[0] *Representation of synchronous, asynchronous, and polychronous components by clocked guarded Actions*. J. Brandt, M. Gemünde, K. Schneider, S. Shukla, and J.-P. Talpin. In Design Automation for Embedded Systems (DAES), Special Issue on Languages, Models and Model Based Design for Embedded Systems. Springer, 2012.

ANTIQUE Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. AnaStaSec

Title: Static Analysis for Security Properties

Type: ANR générique 2014

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: January 2015 - December 2018

Coordinator: Inria Paris-Rocquencourt (France)

Others partners: Airbus France (France), AMOSSYS (France), CEA LIST (France), Inria Rennes-Bretagne Atlantique (France), TrustInSoft (France)

Inria contact: Jérôme Feret

See also: http://www.di.ens.fr/ feret/anastasec/

Abstract: An emerging structure in our information processing-based society is the notion of trusted complex systems interacting via heterogeneous networks with an open, mostly untrusted world. This view characterises a wide variety of systems ranging from the information system of a company to the connected components of a private house, all of which have to be connected with the outside.

It is in particular the case for some aircraft-embedded computer systems, which communicate with the ground through untrusted communication media. Besides, the increasing demand for new capabilities, such as enhanced on-board connectivity, e.g. using mobile devices, together with the need for cost reduction, leads to more integrated and interconnected systems. For instance, modern aircrafts embed a large number of computer systems, from safety-critical cockpit avionics to passenger entertainment. Some systems meet both safety and security requirements. Despite thorough segregation of subsystems and networks, some shared communication resources raise the concern of possible intrusions.

Some techniques have been developed and still need to be investigated to ensure security and confidentiality properties of such systems. Moreover, most of them are model-based techniques operating only at architectural level and provide no guarantee on the actual implementations. However, most security incidents are due to attackers exploiting subtle implementation-level software vulnerabilities. Systems should therefore be analysed at software level as well (i.e. source or executable code), in order to provide formal assurance that security properties indeed hold for real systems.

Because of the size of such systems, and considering that they are evolving entities, the only economically viable alternative is to perform automatic analyses. Such analyses of security and confidentiality properties have never been achieved on large-scale systems where security properties interact with other software properties, and even the mapping between high-level models of the systems and the large software base implementing them has never been done and represents a great challenge. The goal of this project is to develop the new concepts and technologies necessary to meet such a challenge.

The project ANASTASECproject will allow for the formal verification of security properties of software-intensive embedded systems, using automatic static analysis techniques at different levels of representation: models, source and binary codes. Among expected outcomes of the project will be a set of prototype tools, able to deal with realistic large systems and the elaboration of industrial security evaluation processes, based on static analysis.

8.1.1.2. 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 VERASCOadvocates 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.

8.1.1.3. 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)

Inria contact: Antoine Miné

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.

8.2. European Initiatives

8.2.1. FP7 & H2020 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.

8.2.1.2. MBAT

Title: Combined Model-based Analysis & Testing of Embedded Systems

Type: Artemis Call 10

Instrument: FP7 project

Duration: November 2011 - October 2014

Coordinator: Daimler (Germany)

Others partners: 38 partners in Austria, Denmark, Estonia, France, Germany, Italy, Sweden, and United Kingdom

See also: https://artemis-ia.eu/project/29-mbat.html

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

8.3. International Initiatives

8.3.1. Participation In other International Programs

8.3.1.1. EXEK

Title: EXEcutable Knowledge

Type: DARPA

Instrument: DARPA Program

Program: Big Mechanism

Duration: July 2014 - December 2017

Coordinator: Harvard Medical School (Boston, USA)

Partner: Inria Paris-Rocquencourt, École normale supérieure de Lyon Université Paris-Diderot,

Inria contact: Jérôme Feret

Abstract: Our overarching objective is Executable Knowledge: to make modeling and knowledge representation twin sides of biological reasoning. This requires the definition of a formal language with a clear operational semantics for representing proteins and their interaction capabilities in terms of agents and rules informed by, but not exposing, biochemical and biophysical detail. Yet, to achieve Executable Knowledge we need to go further:

- Bridge the gap between rich data and their formal representation as executable model elements. Specifically, we seek an intermediate, but already formal, knowledge representation (meta-language) to express granular data germane to interaction mechanisms; a protocol defining which and how data are to be expressed in that language; and a translation procedure from it into the executable format.
- Implement mathematically sound, fast, and scalable tools for analyzing and executing arbitrary collections of rules.
- Develop a theory of causality and attendant tools to extract and analyze the unfolding of causal lineages to observations in model simulations.

We drive these technical goals with the biological objective of assembling rule-based models germane to Wnt signaling in order to understand the role of combinatorial complexity in robustness and control.

8.3.2. Inria International Labs

Xavier Rival attended the LIAMA Open Day in July 2014, gave a talk on “Modular Construction of Shape-Numeric Analyzers” and participated to the associated Summer School, giving a one day introduction to Verification by Abstract Interpretation.

8.3.3. Inria International Partners

8.3.3.1. Informal International Partners

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

Research on sensitivity is done in partnership with the group of Sukyoung Ryu (Assistant Professor at KAIST, Daejeon, Korea).

Research on numeric abstract domain is done in partnership with the groups of Ji Wang and Liqian Chen (National University of Defense Technology, Changsha, China) and of Deepak Kapur (University of New Mexico, USA).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Kwangkeun Yi (Professor at Seoul National University, Seoul, Korea) visited the group during two weeks in June-July 2014. Sukyoung Ryu (Assistant Professor at KAIST, Daejeon, Korea) visited the group during four weeks in July-August 2014.

8.4.2. Internships

Benjamin Audry accomplished a under the supervision of Jérôme Feret (while he was a student at “Collège du Parc”, Sucy en Brie, France).

Pretesh Agrawal accomplished a pre-doctoral internship undern the supervision of Jérôme Feret and Norman Ferns (while he was a fourth year undergraduate student at IIT Kanpur, India).

Émile Ferreux and Nessim Morsli accomplished under the supervision of Jérôme Feret (while they were L1 student of the FDV Bachelor program, Frontiers in Life Science, at University Paris-Descartes, France).

Huisong Li accomplished a pre-doctoral internship under the supervision of Xavier Rival (while she was a student at the Institute of Software, at the Chinese Academy of Sciences (Beijing, China).

Thibault Suzanne accomplished a Master internship under the supervision of Antoine Miné.

Abdelraouf Ouadjaout, a PhD student at CERIST Research Center (Alger), performed a one-month internship in the group under the supervision of Antoine Miné. The internship was funded by the Ministry of Higher Education and Scientific Research of Algeria.

CELTIQUE Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. 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 December 2010 to November 2014.

6.1.2. 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.

6.1.3. The ANR Binsec project

Participants: Frédéric Besson, Sandrine Blazy, Pierre Wilke, Colas Le Guernic.

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.

6.1.4. The ANR MALTHY project

Participant: David Cachera.

The MALTHY project, funded by ANR in the program INS 2013, aims at advancing the state-of-the-art in real-time and hybrid model checking by applying advanced methods and tools from linear algebra and algebraic geometry. MALTHY is coordinated by VERIMAG, involving CEA-LIST, Inria Rennes (Estasys and Celtique), Inria Saclay (MAXPLUS) and VISEO/Object Direct.

6.1.5. The ANR AJACS project

Participants: Martin Bodin, Thomas Jensen, Alan Schmitt.

The goal of the AJACS project is to provide strong security and privacy guarantees on the client side for web application scripts. To this end, we propose to define a mechanized semantics of the full JavaScript language, the most widely used language for the Web. We then propose to develop and prove correct analyses for JavaScript programs, in particular information flow analyses that guarantee no secret information is leaked to malicious parties. The definition of sub-languages of JavaScript, with certified compilation techniques targeting them, will allow us to derive more precise analyses. Finally, we propose to design and certify security and privacy enforcement mechanisms for web applications, including the APIs used to program real-world applications.

The project partners include the following Inria teams: Celtique, Indes, Prosecco, and Toccata; it also involves researchers from Imperial College as external collaborators. The project runs from December 2014 to June 2018.

6.1.6. The ANR DISCOVER project

Participants: Sandrine Blazy, Delphine Demange, Thomas Jensen, David Pichardie.

The DISCOVER project project aims at leveraging recent foundational work on formal verification and proof assistants to design, implement and verify compilation techniques used for high-level concurrent and managed programming languages. The ultimate goal of DISCOVER is to devise new formalisms and proof techniques able to scale to the mechanized correctness proof of a compiler involving a rich class of optimizations, leading to efficient and scalable applications, written in higher-level languages than those currently handled by cutting-edge verified compilers.

In the light of recent work in optimizations techniques used in production compilers of high-level languages, control-flow-graph based intermediate representations seems too rigid. Indeed, the analyses and optimizations in these compilers work on more abstract representations, where programs are represented with data and control dependencies. The most representative representation is the sea-of-nodes form, used in the Java Hotspot Server Compiler, and which is the rationale behind the highly relaxed definition of the Java memory model. DISCOVER proposes to tackle the problem of verified compilation for shared-memory concurrency with a resolute language-based approach, and to investigate the formalization of adequate program intermediate representations and associated correctness proof techniques.

The project runs from October 2014 to September 2018.

6.1.7. Labex COMIN Labs Seccloud project

Participants: Frédéric Besson, Thomas Jensen, Alan Schmitt, Thomas Genet, 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.

6.2. International Initiatives

6.2.1. Inria Associate Teams

6.2.1.1. JCERT

Title: Verified Compilation of Concurrent Managed Languages

International Partner (Institution - Laboratory - Researcher):

Purdue University (ÉTATS-UNIS)

Duration: 2014 -

See also: http://www.irisa.fr/celtique/ea/jcert/

Safety-critical applications demand rigorous, unambiguous guarantees on program correctness. While a combination of testing and manual inspection is typically used for this purpose, bugs latent in other components of the software stack, especially the compiler and the runtime system, can invalidate these hard-won guarantees. To address such concerns, additional laborious techniques such as manual code reviews of generated assembly code are required by certification agencies. Significant restrictions are imposed on compiler optimizations that can be performed, and the scope of runtime and operating system services that can be utilized. To alleviate this burden, the JCert project is implementing a verified compiler and runtime for managed concurrent languages like Java or C#.

6.2.2. Inria International Partners

6.2.2.1. Informal International Partners

Yann Salmon spent one month in Luke Ong's group at Oxford University (UK) between january and february. The objective of this stay was, on the one side, to promote Yann's work on strategy-dependant analysis of functional programs and, on the other side, to learn from Luke Ong's group on the analysis principles for higher-order functions.

6.2.2.1.1. JSCert

The JSCert project is an informal collaboration between Inria (Celtique and Toccata teams) and Imperial College. Alan Schmitt (Celtique) and Arthur Charguéraud (Toccata) are external collaborators for the "Certified Verification of Client-Side Web Programs" EPSRC project, led by Imperial College. Sergio Maffeis and Philippa Gardner are external collaborators for the "AJACS" ANR project, led by Inria.

6.3. International Research Visitors

6.3.1. Visits to International Teams

6.3.1.1. Sabbatical programme

Jensen Thomas

Date: Sep 2014 - Aug 2015

Institution: University of Copenhagen, Denmark

Pichardie David

Date: Sep 2011 - Aug 2012

Institution: Purdue University (PAYS???)

6.3.1.2. Explorer programme

Salmon Yann

Date: Jan 2014 - Feb 2014

Institution: University of Oxford (UK)

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.

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*.

The ANR mid-term review of the project took place in October 2014 and the members of the project received very positive feedbacks from the reviewers. A more detailed report is expected from the reviewers in early 2015.

7.1.3. ANR Tarmac

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

7.2. International Research Visitors

7.2.1. Visits to International Teams

7.2.1.1. Research stays abroad

Olivier Hermant was an invited researcher at the Natal University (UFRN, Brazil) in December 2014.

ESTASYS Exploratory Action

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. ESTASE

Participants: Axel Legay, Sean Sedwards.

ESTASE is a create project whose main objective was to initiate the creation of the plasma toolset as well as to propose new model checking algorithms for rare events.

7.1.2. Privacy

Participants: Axel Legay, Fabrizio Biondi, Jean Quilbeuf.

Privacy is a regional project whose objective is to quantify privacy of data. This includes, e.g., quantifying the anonymity of a voting protocol.

7.1.3. Variability

Participants: Axel Legay, Jin Hyun Kim, Louis-Marie Traonouez.

Variability is a regional project whose objective is to lift scheduling techniques to connected-objects. The main application of the project is Systems of Systems.

7.2. National Initiatives

7.2.1. ANR Malthy

Participants: Axel Legay, Rudolf Fahrenberg, Louis-Marie Traonouez.

The objective of this project is to study new models and techniques to reason on quantitative systems. We mainly focus on the composition of timed components in a dynamic setting.

7.2.2. BGLE SyS2Soft

Participants: Axel Legay, Thomas Given-Wilson, Cyrille Jegourel.

This national project studies various languages and techniques for quantitative systems.

7.3. European Initiatives

7.3.1. Danse

Program: FP7

Project acronym: DANSE

Project title: Designing for Adaptability and evolutioN in System of systems Engineering

Duration: mois année début - mois année fin

Coordinator: Offis

Abstract: Design and verification of Systems of Systems. We contributed by proposing the first verification engine for Heterogeneous SoS. For doing so, we have combined Plasma with Desyre that is a simulator for SoS described via the standardised FMI/FMU approach.

7.3.2. Meals

Program: Marie Curie

Project acronym: Meals

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

Duration: Octobre 2012 – Octobre 2016

Coordinator: Germany (Saarbrucken) and Argentina ()

Abstract: Colaborative action on the topic of quantitative systems

7.3.3. Sensation

Program: Fet ProActif

Project acronym: Sensation

Project title: Self Energy-Supporting Autonomous Computation

Duration: Octobre 2012 – Octobre 2015

Coordinator: Aalborg University

Abstract: Development of new results for energy-centric systems. We contributed by proposing new algorithms for rare-event simulation.

7.3.4. DALI

Program: FP7

Project acronym: DALI

Project title: Devices for assisted living

Duration: Octobre 2011 - Octobre 2014

Coordinator: Trento University

Abstract: Development of a machine to guide a lady in a commercial center. We contributed by designing the cognitive algorithm. The machine is one example of a component of a large SoS that has its own objective but whose global behavior depends on those of other components. This is also a good illustration that our tool can be miniaturized to work in a small robot.

7.3.5. EMC2

Program: ARTEMIS

Project acronym: EMC2

Project title: Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments

Duration: mars 2014 – mars 2017

Coordinator: Infineon

Abstract: Large initiative on embadded systems and SoS. We will contribute with our expertise from DANSE and Sensation projects.

7.4. International Initiatives

Our team has strong collaboration with University of Namur, Carnegie Mellon University, University of Aalborg, Verimag Grenoble, and University of Waterloo. So far, those activities have not yet been funded.

7.5. International Research Visitors

7.5.1. Visits of International Scientists

7.5.1.1. Internships

- Jan Kretinsky, PostDoc at IST Austria
- Karin Quaas, PostDoc at Leipzig University
- Kim Larsen, Professor at Aalborg University
- Zoltan Esik, Professor at University of Szeged

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.

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 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, Maxime Dénès, 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

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 & H2020 Projects

8.2.1.1. DEEPSEA

Type: FP7

Defi: NC

Instrument: ERC Starting Grant

Objectif: NC

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 Partners

8.3.1.1. Informal International Partners

- Princeton University: interactions between the CompCert verified C compiler and the Verified Software Toolchain developed at Princeton.
- Cambridge University and Microsoft Research Cambridge: formal modeling and testing of weak memory models.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Sigurd Schneider, Ph.D. student at Saarlandes University in Saarbrucken, visited Gallium from Mar 2014 to May 2014. As part of his Ph.D., Sigurd Schneider develops an intermediate representation that unifies static single assignment form (SSA) and functional intermediate representations. During his internship, he considered the addition of GC support to this intermediate representation. He also developed a program logic to verify the correctness of a class of optimizations, including constant subexpression elimination (CSE) and global value numbering.

8.4.1.2. Research stays abroad

Since November 2014, Damien Doligez is on a sabbatical at Jane Street (New York, USA), a financial company (member of the Caml Consortium) that invests considerable R&D in the OCaml language and system.

MARELLE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

In 2014, we participated to two successful applications for funding from the French national agency for research (ANR).

- BRUTUS "Chiffrements authentifiés et résistants aux attaques par canaux auxiliaires", started on October 1st, 2014, for 60 months, with a grant of 41 kEuros for Marelle. Other partners are Université de Rennes 1, CNRS, secrétariat Général de la défense et de la sécurité nationale, and Université des Sciences et Technologies de Lille 1. The corresponding researcher for this contract is Benjamin Grégoire.
- FastRelax, "Fast and Reliable Approximations", started on October 1st, 2014, for 60 months, with a grant of 75 kEuros for Marelle. Other partners are Inria Grenoble (ARIC project-team), LAAS-CNRS (Toulouse), Inria Saclay (Toccata and Specfun project-teams), and LIP6-CNRS (Paris). The corresponding researcher for this contract is Laurence Rideau.

8.2. International Initiatives

8.2.1. Inria International Partners

8.2.1.1. Informal International Partners

Our main partner for work on Ssreflect is Georges Gonthier, senior researcher at Microsoft Research, Cambridge.

Our team has important discussions with the team of Thierry Coquand at *Chalmers University and University of Göteborg*. This was illustrated in the past by the European project FORMATH, in the context of which we collaborated around the formalization of various aspects of Algebra (linear algebra and algebraic topology). This effort was continued in the context of the international effort around *homotopy type theory*, where Cyril Cohen is deeply involved (in particular in the implementation of a model for cubical sets). In the future, we may hope to play a continuing role in *homotopy theory* and establish more contacts with other sites involved in this topic.

We participate in the international development of the Coq community and maintain frequent contacts with the most active users around the world. In practice, this implies many contacts with several universities in the United States of America: Princeton University, University of Pennsylvania, the Massachusetts Institute of Technology, Harvard University, and Yale University.

We have intensive collaborations with IMDEA, Madrid. In particular, the software systems EasyCrypt and ZooCrypt are developed in collaboration with this institution, and several of our publications are co-authored between Inria and IMDEA.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

8.3.1.1. Sabbatical programme

Amy Felty, professor at University of Ottawa, was a member of our team until September 30th, on sabbatical leave from her university, and with no extra financial support from Inria.

Dough Howe, professor at Carleton University, was a member of our team until August 31st, on sabbatical leave from his university, and with no extra financial support from Inria.

MEXICO Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. 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 has ended on August 31, 2014.

8.2. IRT

8.2.1. 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. MIC is scheduled to be completed late in 2016.

8.3. National Initiatives

8.3.1. 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.

8.4. European Initiatives

8.4.1. FP7 & H2020 Projects

8.4.1.1. Hycon2

Type: FP7 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

Partners: 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.

8.5. International Initiatives

8.5.1. Inria International Partners

8.5.1.1. 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/), see below.
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 (Maciej Koutny, Alex Yakovlev, Victor Khomenko and Andrey Mokhov), with visits in both directions.

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

8.5.2.1. EGIDE: TAMTV

Since October 2013, Benedikt Bollig has been the French coordinator of the EGIDE-Procope project TAMTV (2013/2014), which is a collaboration with LIAFA (Paris) and the University of Ilmenau (Germany).

8.5.2.2. LIA INFORMEL

The Indo-French Formal Methods Lab is an International Associated Laboratory (LIA) fostering the scientific collaboration between India and France in the domain of formal methods and applications to the verification of complex systems. Our research focuses on theoretical foundations of games, automata, and logics, three important tools in formal methods. We study applications to the verification of safety-critical systems, with an emphasis on quantitative aspects (time, cost, energy, etc.), concurrency, control, and security protocols. The Laboratory was founded in 2012 by a consortium of researchers from the French Centre for Scientific Research (CNRS), Ecole Normale Supérieure de Cachan (ENS Cachan), Université Bordeaux 1, the Institute of Mathematical Sciences Chennai (IMSc), the Chennai Mathematical Institute (CMI), and the Indian Institute of Science Bangalore (IISc). It is directed by Paul Gastin (ENS Cachan, MExICo team) and Madhavan Mukund (CMI). The LIA has been scientifically extremely active and productive since its creation. The LIA has supported numerous scientific exchanges and joint research papers, see http://projects.lsv.ens-cachan.fr/informel/

8.6. International Research Visitors

8.6.1. Visits of International Scientists

- Maciej Koutny from Newcastle University came as an invited Profeessor (for ENS Cachan) from February 10 to 14 and from March 3 to 7, 2014.
- From May 12 to June 3rd, K. Narayan Kumar from CMI Chennai, India, visited to work with C. Aiswarya and Paul Gastin on controllers for distributed systems.
- From June 1 to 10, 2014, S. Akshay from IIT Bombay visited MExICo to work with Paul Gastin, on split-width techniques for timed systems.
- Stanislav Böhm from the Technical University of Ostrava visited the group from 7 october to 7 december 2014.

8.6.2. Internships hosted by MExICo

Athanasiou Konstantinos - Athanasios

Date: Apr 2014 - Aug 2014

Institution: National University of Athens, Greece

Jana Schubert

Date: 30 Sept 2013 - 28 February 2014

Institution: Universität Dresden, Germany

Akshay Kumar

Date: May 10 to July 22, 2014

Institution: IIT Khanpur

8.6.3. Visits to International Teams

8.6.3.1. Shorter Visits

- Paul Gastin visited S. Akshay at IIT Bombay twice, first January 11-17 to work on probabilistic timed systems , and then from December 7 to 19 to work on timed pushdown systems and to deliver an invited talk at FSTTCS in Delhi.
- Stefan Haar visited the PAIS lab at Higher School of Economics in Moscow from Sept. 15 to 23.

PARSIFAL Project-Team

7. Partnerships and Cooperations

7.1. European Initiatives

7.1.1. FP7 & H2020 Projects

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.

7.2. International Initiatives

Members of the team have applied for the following three international projects. All three are still pending, the final results are not currently know.

1. A generic ANR proposal for collaboration between several French sites and the University of Bologna.
2. A proposal to ANR and JCJC (Japan).
3. A proposal to the Ministry of Education, Singapore for collaboration with the Nanyang Technological University.

7.3. International Research Visitors

- Chuck Liang (Professor from Hofstra University, NY, USA) visited for three weeks 26 May – 20 June 2014 and for another week starting 15 December.
- Gopalan Nadathur (Professor from the University of Minnesota) visited 2 - 11 July.
- Mary Southern (PhD candidate at the University of Minnesota, USA), May – Aug 2014
  Internship supervised by K. Chaudhuri.
- Yuting Wang (PhD candidate at the University of Minnesota, USA), May – Aug 2014

PI.R2 Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

Alexis Saurin (coordinator) and Yann Régis-Gianas are members of the four-year RAPIDO ANR project accepted in 2014 and starting in January 2015. RAPIDO aims at investigating the use of proof-theoretical methods to reason and program on infinite data objects. The goal of the project is to develop logical systems capturing infinite proofs (proof systems with least and greatest fixed points as well as infinitary proof systems), to design and to study programming languages for manipulating infinite data such as streams both from a syntactical and semantical point of view. Moreover, the ambition of the project is to apply the fundamental results obtained from the proof-theoretical investigations (i) to the development of software tools dedicated to the reasoning about programs computing on infinite data, *e.g.* stream programs (more generally coinductive programs), and (ii) to the study of properties of automata on infinite words and trees from a proof-theoretical perspective with an eye towards model-checking problems. Other permanent members of the project are Christine Tasson from PPS, David Baedle from LSV, ENS-Cachan, and Pierre Clairambault, Damien Pous and Colin Riba from LIP, ENS-Lyon.

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. This project is with members of the LAGA (Laboratory of Mathematics, Univ. Paris 13).

Pierre-Louis Curien (coordinator), Yves Guiraud and Philippe Malbos are members of the four-years Cathre ANR project, started in January 2014. This project investigates 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 in 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 (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 in January 2012 and is a joint project with LRI, PPS and Inria Grenoble.

Yann Régis-Gianas collaborates with Mitsubishi Rennes on the topic of differential semantics. This collaboration led to the CIFRE grant for the PhD of Thibaut Girka.

Matthieu Sozeau is a member of the CoqHoTT project led by Nicolas Tabareau (Ascola team, École des Mines de Nantes), funded by an ERC Starting Grant.

6.2. European Initiatives

6.2.1. Collaborations with Major European Organisations

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 International Partners

The project-team has collaborations with Wroclaw University (Poland), University of Aarhus (Denmark), University of Oregon, University of Tokyo, University of Sovi Sad, University of Nottingham, Institute of Advanced Study, MIT and University of Cambridge.

6.3.2. 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).

6.4. International Research Visitors

6.4.1. Visits of International Scientists

Beta Ziliani (MPI Saarbrücken) visited πr^2 for one week in November 2014 to collaborate with Yann Régis-Gianas and Matthieu Sozeau.

Peter Aczel (Manchester Univ.), Steve Awodey (Carnegie Mellon University), Thierry Coquand (Univ. Göteborg), and Vladimir Voevodsky (Institute for Advanced Study) were Inria funded invited professors for the thematic IHP trimester Semantics of Proofs and Certified Mathemtatics.

6.4.1.1. Internships

Akira Yoshimizu is an international Inria intern, working on abstract machines for quantum programmming languages inspired from game semantics and linear logic.

6.4.2. Visits to International Teams

6.4.2.1. Research stays abroad

Pierre-Louis Curien visited Chili (Univ. of Talca) in March 2014 (collaborative work with Maria Ronco in operad theory).

SUMO Project-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, 2011-2015, 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, web site
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, web site.
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) and Antoine Rollet (Labri) on the enforcement of timed properties.

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

8.2. International Initiatives

8.2.1. Inria International Labs

Eric Badouel is member of the team Aloco (Architecture logicielle à composants) of LIRIMA, the Inria International Lab in Africa. This collaboration is on the development of artifact-centric business process models.

8.2.2. 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)

8.2.3. Inria International Partners

8.2.3.1. Informal International Partners

We have long lasting relations with indian labs : The Chennai Mathematical Institute in Chennai (M. Mukund, N. Kumar), the Institute for Mathematical Sciences in Chennai (R. Ramanujam, K. Lodaya). We are extending these relations in India. S. Akshay holds a permanent position in IIT Bombay after his postdoc at IRISA. Our relation with our Indian partners has been formalized as associated teams (currently EA DISTOL 2012-2015).

We have started a collaboration with J. Mullins from Université Polytechnique de Montréal. The main theme of this collaboration is security properties in concurrency models. We have submitted a joint paper of variants of interference properties (information leakage) for partial order models.

We collaborate with Laurie Ricker (Mount Allison University, Canada) on the control of distributed systems and the enforcement of opacity.

8.2.4. Participation In other International Programs

AVeRTS is an Indo-French project on the algorithmic verification of real-time systems. The project is funded by CNRS on the french side, and by DST on the Indian side, under the CEFIPRA - Indo-French Program in ICST 2014-2016. From SUMO, Nathalie Bertrand and Blaise Genest are involved and contribute on stochastic timed games.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

This year, S. Akshay, from IIT Bombay visited us for a one month stay, from end of May to July. This visit was funded by Rennes 1 University. During this visit, he has worked with B. Genest and L. Hélouët on verification of extensions of Petri nets calle time Petri nets with restricted urgency, that can be used to model communication systems with threshold and latency in messages. The work performed this summer is currently under submission.

Christel Baier, professor at Dresden University, was also invited for a 2-week stay paid by Rennes 1 University. She has worked during her visit with N. Bertrand on long-run quantiles in Markov decision processes.

Doron Peled visited our team for a total duration of a month in Spring 2014. He worked with B. Genest on knowledge computation in distributed systems, a work currently under review.

Valentin Goranko, professor at Stockholm University, was invited for a 2-week stay paid by Rennes 1 University. He has worked during his visit with C. Morvan on first order properties of Rational Graphs.

Laurie Ricker (Mount Allison University) visited us during for 2 months [Mai-June 2014] on the control of distributed systems and the enforcement of opacity.

Robert Nsaibirni (University of Yaoundé) visited SUMO from July to August 2014 on the use of the Guarded Attribute Grammar formalism for the description of the workspaces of actors of a disease surveillance system.

8.3.1.1. Internships

Rishika Garg

Date: May 2014 - Jul 2014

Institution: IIT Kampur (India)

Engel Lefaucheux

Date: March 2014 - July 2014

Institution: ENS Cachan (France)

Ayush Maheshwari

Date: May 2014 - July 2014

Institution: IIT Kanpur (India)

Maroua Maalej

Date: Apr 2014 - July 2014

Institution: ENSI Tunis (Tunisia)

Sanaa Mairouch

Date: May 2014 - Aug 2014

Institution: ISTIC (France)

Aminatou Mohamadou

Date: Jun 2014 - July 2014

Institution: ISTIC (France)

Dhananjay Raju

Date: March 2014 - July 2014

Institution: CMI (India)

8.3.1.2. Research stays abroad

N. Bertrand spent two visits of one month each at Mons University (Belgium), pursuing a collaboration with Thomas Brihaye, and funded by the FNRS. The resulting work on stochastic timed automata with decisions was presented at the QEST conference [29].

TEMPO Team

7. Partnerships and Cooperations

7.1. International Initiatives

7.1.1. Inria International Labs

The TEMPO project belongs to the LIAMA laboratory in China. The project is hosted by East China Normal University Software Engineering Institute.

7.1.2. Inria International Partners

7.1.2.1. Declared Inria International Partners

The projects is run in collaboration with East China Normal University Software Engineering Institute and Netherlands CWI.

7.1.3. Participation In other International Programs

The project is run within the context of China LIAMA laboratory.

TOCCATA Project-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-year 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 [101], [65], [100],[19]. This is sorely needed to ease the verification of numerical applications, especially those involving advanced mathematics.

Partners: team SpecFun from LIX (Palaiseau), University Paris 13

8.1.2. ELFIC

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

ELFIC is a working group of the Digicosme Labex. S. Boldo is the principal investigator.

Project ELFIC focuses on proving the correctness of the FELiScE (Finite Elements for Life Sciences and Engineering) C++ library which implements the finite element method for approximating solutions to partial differential equations. Finite elements are at the core of numerous simulation programs used in industry. The formal verification of this library will greatly increase confidence in all the programs that rely on it. Verification methods developed in this project will be a breakthrough for the finite element method, but more generally for the reliability of critical software relying on intricate numerical algorithms.

Partners: Inria team Pomdapi; Ecole Polytechnique, LIX; CEA LIST; Université Paris 13, LIPN; UTC, LMAC (Compiègne).

8.2. National Initiatives

8.2.1. ANR Ajacs

Participant: Arthur Charguéraud [contact].

The AJACS research project is funded by the programme “Société de l’information et de la communication” of the ANR, for a period of 42 months, starting on October 1st, 2014.

The goal of the AJACS project is to provide strong security and privacy guarantees on the client side for web application scripts implemented in JavaScript, the most widely used language for the Web. The proposal is to prove correct analyses for JavaScript programs, in particular information flow analyses that guarantee no secret information is leaked to malicious parties. The definition of sub-languages of JavaScript, with certified compilation techniques targeting them, will allow deriving more precise analyses. Another aspect of the proposal is the design and certification of security and privacy enforcement mechanisms for web applications, including the APIs used to program real-world applications. On the Toccata side, the focus will be on the formalization of secure subsets of JavaScript, and on the mechanization of proofs of translations from high-level languages into JavaScript.

Partners: team Celtique (Inria Rennes - Bretagne Atlantique), team Prosecco (Inria Paris - Rocquencourt), team Indes (Inria Sophia Antipolis - Méditerranée), and Imperial College (London).

8.2.2. ANR FastRelax

Participants: Sylvie Boldo [contact], Guillaume Melquiond.

This is a research project funded by the programme “Ingénierie Numérique & Sécurité” of the ANR. It is funded for a period of 48 months and it has started on October 1st, 2014. http://fastrelax.gforge.inria.fr/

Our aim is to develop computer-aided proofs of numerical values, with certified and reasonably tight error bounds, without sacrificing efficiency. Applications to zero-finding, numerical quadrature or global optimization can all benefit from using our results as building blocks. We expect our work to initiate a "fast and reliable" trend in the symbolic-numeric community. This will be achieved by developing interactions between our fields, designing and implementing prototype libraries and applying our results to concrete problems originating in optimal control theory.

Partners: team ARIC (Inria Grenoble Rhône-Alpes), team MARELLE (Inria Sophia Antipolis - Méditerranée), team SPECFUN (Inria Saclay - Île-de-France), Université Paris 6, and LAAS (Toulouse).

8.2.3. ANR Soprano

Participants: Sylvain Conchon [contact], Évelyne Contejean, Guillaume Melquiond.

The Soprano research project is funded by the programme “Sciences et technologies logicielles” of the ANR, for a period of 42 months, starting on October 1st, 2014.

The SOPRANO project aims at preparing the next generation of verification-oriented solvers by gathering experts from academia and industry. We will design a new framework for the cooperation of solvers, focused on model generation and borrowing principles from SMT (current standard) and CP (well-known in optimization). Our main scientific and technical objectives are the following. The first objective is to design a new collaboration framework for solvers, centered around synthesis rather than satisfiability and allowing cooperation beyond that of Nelson-Oppen while still providing minimal interfaces with theoretical guarantees. The second objective is to design new decision procedures for industry-relevant and hard-to-solve theories. The third objective is to implement these results in a new open-source platform. The fourth objective is to ensure industrial-adequacy of the techniques and tools developed through periodical evaluations from the industrial partners.

Partners: team DIVERSE (Inria Rennes - Bretagne Atlantique), Adacore, CEA List, Université Paris-Sud, and OCamlPro.

8.2.4. ANR CAFEIN

Participant: Sylvain Conchon [contact].

The CAFEIN research project is funded by the programme “Ingénierie Numérique & Sécurité” of the ANR, for a period of 3 years, starting on February 1st, 2013. https://cavale.enseeiht.fr/CAFEIN/.

This project addresses the formal verification of functional properties at specification level, for safety critical reactive systems. In particular, we focus on command and control systems interacting with a physical environment, specified using the synchronous language Lustre.

A first goal of the project is to improve the level of automation of formal verification, by adapting and combining existing verification techniques such as SMT-based temporal induction, and abstract interpretation for invariant discovery. A second goal is to study how knowledge of the mathematical theory of hybrid command and control systems can help the analysis at the controller’s specification level. Third, the project addresses the issue of implementing real valued specifications in Lustre using floating-point arithmetic.

Partners: ONERA, CEA List, ENSTA, teams Maxplus (Inria Saclay - Île-de-France), team Parkas (Inria Paris - Rocquencourt), Perpignan University, Prover Technology, Rockwell Collins.

8.2.5. ANR BWare

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

The BWare research project is funded by the programme “Ingénierie Numérique & Sécurité” of the ANR, a period of 4 years, starting on September 1st, 2012. http://bware.lri.fr.

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 guarantee 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 [109]. 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); teams Gallium and Deducteam (Inria Paris - Rocquencourt) ; Mitsubishi Electric R&D Centre Europe, ClearSy (the company which develops and maintains *Atelier B*), and the start-up OCamlPro.

8.2.6. ANR Verasco

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

The Versaco research project is funded by the programme "Ingénierie Numérique & Sécurité" of the ANR, for a period of 4 years, starting on January 1st, 2012. Project website: 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).

8.3. European Initiatives

8.3.1. FP7 & H2020 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 Paris - Rocquencourt) is the principal investigator of this ERC-funded project. The other main 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/.

8.4. International Initiatives

8.4.1. Inria International Partners

8.4.1.1. Declared Inria International Partners

S. Conchon, A. Mebsout and F. Zaïdi (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.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- P. Roux (ISAE, Onera) visited for 7 months in order to collaborate with S. Boldo and G. Melquiond on the topic of formal verification of numerical algorithms.
- Bas Spitters visited for 3 months from April to June funded by a Digiteo grant. He worked with C. Paulin on the extension of the ALEA library to continuous structures and the use of "lower reals" (monotonic sequences of rationals). He also worked on adapting the Corn and Math-classes libraries to the new Coq release. During that time he published a final version of a paper presented at the Workshop on Quantum Physics and Logic in 2012 [119].
- Andrew Tolmach is a visiting researcher from Portland State University, on a one-year Digiteo Chair. His research project will initiate a new research effort to develop principles, techniques, and tools for large-scale proof engineering. It is focused on the Coq proof assistant and is designed to take advantage of the deep pool of expertise available in the Paris area (at Paris-Sud, LIX, Inria, etc.) concerning both the use and development of Coq. Initial results are expected to include: a precise description of requirements for large proof management; sample prototype tools addressing one or more of these requirements; and a technical survey of relevant proof representation options.

VERIDIS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Participants: Jingshu Chen, Pablo Federico Dobal, Pascal Fontaine, Stephan Merz.

The PhD thesis of Pablo Federico Dobal benefits from joint funding by Région Lorraine since September 2014, complementing funding through the ANR-DFG project SMArT (section 8.2).

The post-doctoral research stay of Jingshu Chen was supported by joint funding by Région Lorraine and the Airbus Foundation.

8.2. National Initiatives

8.2.1. ANR-DFG Project SMArT

Participants: Haniel Barbosa, David Déharbe, Pablo Federico Dobal, Pascal Fontaine, Maximilian Jaroschek, Marek Košta, Stephan Merz, Thomas Sturm.

The SMArT (Satisfiability Modulo Arithmetic Theories) project is funded by *ANR-DFG Programmes blancs 2013*, a program of the Agence Nationale de la Recherche and the (German) Deutsche Forschungsgemeinschaft DFG. It started in April 2014. The partners are both the French and German parts of VeriDis and the Systerel company. The objective of the SMArT project is to provide advanced techniques for arithmetic reasoning beyond linear arithmetic for formal system verification, and particularly for SMT. Arithmetic reasoning is one strong direction of research at MPI, and the state-of-the-art tool Redlog (section 5.4) is mainly developed by Thomas Sturm. The SMT solver veriT (section 5.1), developed in Nancy, will serve as an experimentation platform for theories, techniques and methods designed within this project.

In September 2014, Pablo Federico Dobal has been hired as a PhD student in joint supervision with Saarland University, co-funded by the SMArT project and the Région Lorraine. More information on the project can be found on http://smart.gforge.inria.fr/.

8.2.2. ANR Project IMPEX

Participants: Manamiary Andriamiarina, Dominique Méry.

The ANR Project IMPEX is an INS ANR project that started in December 2013 for 4 years. It is coordinated by Dominique Méry, the other partners are IRIT/ENSEIHT, Systerel, Supelec and Telecom Sud Paris.

All software systems execute within an environment or context. Reasoning about the correct behavior of such systems is a ternary relation linking the requirements, system and context models. Formal methods are concerned with providing tool (automated) support for the synthesis and analysis of such models. These methods have quite successfully focused on binary relationships, for example: validation of a formal model against an informal one, verification of one formal model against another formal model, generation of code from a design, and generation of tests from requirements. The contexts of the systems in these cases are treated as second-class citizens: in general, the modeling is implicit and usually distributed between the requirements model and the system model. This project proposal is concerned with the explicit modeling of contexts as first-class citizens.

Several approaches aim at formalizing mathematical theories that are applicable in the formal developments of systems. These theories are helpful for building complex formalizations, expressing and reusing proof of properties. Usually, these theories are defined within contexts, that are imported and and/or instantiated. They usually represent the implicit semantics of the systems and are expressed by types, logics, algebras, etc. However, an implicit handling of contexts loses important information, and therefore is not expressive enough for ensuring that even a verified system is "correct". As a very simple example, take two formally developed systems that are composed to exchange currency data represented by a float. This system is no longer consistent if one system refers to Euros and the other to dollars. The objective of the IMPEX project is to build explicit formal models of contextual semantics and to extend proof-based techniques for handling such a stronger semantics [23].

8.2.3. Inria Development Action VeriT

Participants: Pablo Federico Dobal, Pascal Fontaine.

Inria funded 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). Pablo Federico Dobal was 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 also contributed to the maintenance of the deltaSMT tool, which has been used by several other teams of SMT developers for debugging SMT solvers.

8.3. European Initiatives

8.3.1. 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)

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

Inria contact: Catuscia 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 within work package 2. In 2014, the project funded visits by Stephan Merz to Córdoba and by Carlos Areces, Luciana Benotti, Raúl Fervari, and Guillaume Hoffmann to Nancy.

8.3.2. Cooperation with NUI Maynooth, Ireland

Participant: Dominique Méry.

We cooperate with Rosemary Monahan of NUI Maynooth on exchanges between techniques of software refinement and software verification. Our cooperation was financially supported in 2013 by a one-year project funded by PHC Ulysses. 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 and provide 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 for integrating the *a posteriori* paradigm Spec# and the *a priori* paradigm Event-B. This integration induces a methodology that bridges the gap between software modeling and program verification in the software development life cycle. During 2014, we have designed the Rodin plugin EB2RC that implements transformations of Event-B models into algorithms.

8.4. International Initiatives

8.4.1. Participation In International Programs

8.4.1.1. STIC AmSud MISMT

Participants: Carlos Areces, Haniel Barbosa, Luciana Benotti, Richard Bonichon, David Déharbe, Pablo Federico Dobal, Raúl Fervari, Pascal Fontaine, Guillaume Hoffmann, Stephan Merz, Claudia Tavares.

VeriDis has a close working relationship with two South American teams at Universidade Federal do Rio Grande de Norte (UFRN), Brazil (more specifically with Prof. David Déharbe), and at Universidad Nacional de Córdoba, Argentina (more specifically with Prof. Carlos Areces). The STIC AmSud MISMT project, including both teams and VeriDis, started in 2014. It complements the MEALS project (section 8.3) and extends it to cooperation with UFRN.

The project is centered around Satisfiability Modulo Theories, with a focus on applications to Modal Logic. Notably, the project sustains the development of the veriT solver (section 5.1), of which David Déharbe and Pascal Fontaine are the main developers. First results on using SMT for modal logic have been accepted for publication.

In February, Stephan Merz spent three weeks in Córdoba. David Déharbe stayed in Nancy until July, on a sabbatical from UFRN. A workshop with many participants from the project took place in Nancy in early July. Richard Bonichon and Claudia Tavares visited Nancy in September. At the end of the year, Haniel Barbosa (VeriDis PhD student in joint supervision with Natal) spent three months in Natal and visited Córdoba for two weeks.

More information on the STIC AmSud MISMT project is available on http://mismt.gforge.inria.fr/.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

David Déharbe from UFRN (Natal, Brazil) spent a sabbatical year with the VeriDis team in Nancy from August, 2013 to July, 2014.

8.5.1.1. Internships

Ignacio Martin Queralt

Subject: Symbolic transition checking for TLA$^+$

Date: April to September, 2014

Institution: Universidad Nacional de Córdoba (Argentina)

Clément Herouard

Subject: SMT techniques for modal logics and extensions

Date: May to July, 2014

Institution: Ecole Normale Supérieure de Rennes (France)

CARTE Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Région Lorraine- Université de Lorraine

Simon Perdrix is the principal investigator of the project *measurement-based quantum computing* funded by Région Lorraine and Université de Lorraine.

7.2. National Initiatives

7.2.1. ANR

- The team is a funding partner in ANR Elica (2014-2019), "Elargir les idées logistiques pour l'analyse de complexité". The Carte team is reknown for its expertise in implicit computational complexity.
- The team is a funding partner in ANR Binsec (2013-2017), whose aim is to fill part of the gap between formal methods over executable code, 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.

7.3. European Initiatives

7.3.1. FP7 & H2020 Projects

7.3.1.1. 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: 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.

7.4. International Initiatives

7.4.1. Informal International Partners

- Submission of an Inria associate team proposal THOR (complexity Theory at Higher ORder) in collaboration with Syracuse University, Wesleyan University (Royer, Danner, Ramyaa Ramyaa) and Egypt-Japan University (Walid Gomaa).

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- Cristóbal Rojas (Univ. Andres Bello, Chili) was Inria "Chercheur Invité" for 3 months from July to September 2014. The collaboration led to the paper [20] accepted at STACS 2015.
- Visit of Marco Gaboardi, full researcher at Dundee University, for one week in March 2014.

7.5.2. Short Visits to International Teams

- Romain Péchoux, two one-week visits to Dundee University in March and August 2014.
- Simon Perdrix, visit to the quantum group, Oxford University Computing Laboratory, 1 week in October 2014.
- Simon Perdrix, visit to the Tsinghua University, Beijing, 1 week in December 2014.

CASSIS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- The 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 micro-systems, in particular for a distributed micro airduct. Several teams of the FEMTO-ST institute work together on micro-systems specification, simulation and validation.

8.2. National Initiatives

8.2.1. ANR

- ANR PROSE *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 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 SEQUOIA *Security properties, process equivalences and automated verification*, duration: 4 years, starting in October 2014. Most protocol analysis tools are restricted to analyzing reachability properties while many security properties need to be expressed in terms of some process equivalence. The increasing use of observational equivalence as a modeling tool shows the need for new tools and techniques that are able to analyze such equivalence properties. The aims of this project are *(i)* to investigate which process equivalences-among the plethora of existing ones-are appropriate for a given security property, system assumptions and attacker capabilities; *(ii)* to advance the state-of-the-art of automated verification for process equivalences, allowing for instance support for more cryptographic primitives, relevant for case studies; *(iii)* to study protocols that use low-entropy secrets expressed using process equivalences; *(iv)* to apply these results to case studies from electronic voting.

8.2.2. Fondation MAIF

Project *Protection de l'information personnelle sur les réseaux sociaux*, duration: 3 years, started in October 2014. The goal of the project is to lay the foundation for a risk verification environment on privacy in social networks. Given social relations, this environment will rely on the study of metrics to characterize the security level for a user. Next, by combining symbolic and statistical techniques, it is a question to synthesize a model of risk behavior as a rule base. Finally, a verifier à la model-checking will be developed to assess the security level of user. Partners are Cassis (leader), Orpailleur and Fondation Maif.

8.2.3. Competitivity Clusters

- Project "Investissement d'Avenir - Développement de l'Economie 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 focusses on developping tools for service security verification and testing tasks.
- ProSecure (2011-2016) [0]— 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 (2012-2014) [0] — *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 defining game-based privacy for e-voting protocols.
- Collaboration with Myrto Arapinis (University of Edinburgh) on simplification results for the formal analysis of e-voting protocols.

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

- Collaboration with Matteo Maffei (CISPA, Germany) on type systems for e-voting systems.
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction.
- 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-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), March, December 2014
- David Bernhard (Bristol University), March 2014
- Fabienne Eigner (University of Saarbruecken), February, May 2014
- Joshua Guttman (MITRE), January 2014
- Olivier Pereira (University of Louvain-la-Neuve), March 2014
- Nicolas Pouillard (DemTech, University of Copenhagen), February 2014

8.5.1.1. Internships

Tushant Jha

Subject: Synthesis of Secure Services Composition

Supervisor: Michaël Rusinowitch

Date: from May 2014 until July 2014

Institution: IIIT Hyderabad

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)

Itsaka Rakotonirina

Subject: Automated verification of security protocols with loops

Supervisor: Steve Kremer

Date: from June 2014 until July 2014

Institution: ENS Cachan

Ludovic Robin

Subject: Analysis of security protocols using weak secrets

Supervisor: Steve Kremer

Date: from April 2014 until September 2014

Institution: U. Bordeaux

COMETE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. 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 & H2020 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-MSR joint lab

7.3.1.1. Privacy-Friendly Services and Apps

Title: Privacy-Friendly Services and Applications

Inria principal investigator: Catuscia Palamidessi

International Partners:

Cedric Fournet, Microsoft Research Lab, Cambridge, UK

Andy Gordon, Microsoft Research Lab, Cambridge, UK

Duration: 2014 - 2016

URL: http://www.msr-inria.fr/projects/privacy-friendly-services-and-apps/

Abstract: This is a project sponsored by Microsoft Research Lab, on methods to preserve privacy in web services and location-based services.

7.3.2. Inria Associate Teams

7.3.2.1. 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.

7.3.3. Inria International Partners

7.3.3.1. Informal International Partners

Moreno Falaschi, Professor, University of Siena, Italy

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil

Annabelle Mciver, Associate Professor, Macquarie University, Australia

Charles Carroll Morgan, Professor, University of New South Wales, Australia

Carlos Olarte, Adjunct professor at Universidade Federal do Rio Grande do Norte, Brazil

Camilo Rueda, Professor, Universidad Javeriana Cali, Colombia

7.3.4. Participation In other International Programs

7.3.4.1. 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.

7.3.4.2. 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.

7.3.4.3. MUSICAL

Program: CNPq Science Without Borders.

Project title: Music and Spatial Interaction with Constraints, Algebra and Logic: Foundations and Applications.

Duration: Oct 2014- Oct 2016

URL: http://cic.puj.edu.co/~caolarte/musical/Musical/Welcome.html

Coordinator: Elaine Pimentel, Universidade Federal do Rio Grande do Norte (Brazil),

Other PI's and partner institutions: Camilo Rueda, PUJ Cali (Colombia). Carlos Olarte, Universidade Federal do Rio Grande do Norte (Brazil). Frank Valencia, CNRS-LIX and Inria Saclay (France). Gerard Assayag, IRCAM (France).

Abstract: This multi-disciplinary project aims to develop and integrate tools from logic and concurrency theory for the design and analysis of reactive systems and to their application to musical processes and multimedia systems.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Mauricio Cano, Masters Student, Universidad Javeriana Cali, Colombia, Nov 2014

Moreno Falaschi, Professor, University of Siena, Italy, from July 2014 until Aug 2014

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil, Dec 2014

Maurizio Gabbrielli, Professor, University of Bologna, Italy, from July 2014 until Aug 2014

Daniel Gebler, PhD student, Free University of Amsterdam, The Netherlands, Jun 2014

Justin Hsu, PhD student, University of Pennsylvania, USA, Nov 2014

Annabelle McIver, Associate Professor, Macquarie University, Australia, Dec 2014

Hernan Claudio Melgratti, Associate Professor, University of Buenos Aires, Argentina, Apr 2014

Carroll Morgan, Professor, University of New South Wales and NICTA, Australia, Dec 2014

Carlos Olarte, Adjunct professor at Universidade Federal do Rio Grande do Norte, Brazil, from June 2014 until Jul 2014

Camilo Rueda, Professor, Universidad Javeriana Cali, Colombia, from Nov 2014 to Nov 2014

Geoffrey Smith, Professor, Florida International University, USA, Dec 2014

7.4.1.1. Internships

7.4.1.1.1. Raphaelle Crubillé

Duration: From Mar 2014 until Jul 2014

Subject: Formal modelling of RFID distance bounding protocols

Institution: ENS Lyon

7.4.2. Visits to International Teams

Konstantinos Chatzikokolakis and Catuscia Palamidessi visited the team of Annabelle McIver and Carroll Morgan at Macquarie University, Australia, July 2014.

Frank Valencia visited the team of Camilo Rueda (AVISPA) at Pontifical Universidad Javeriana Cali, from July 2014 until July 2014

DICE Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

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

7.2. National Initiatives

7.2.1. ANR

DICE is involved in two 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.

7.3. European Initiatives

7.3.1. FP7 & H2020 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.

7.4. International Initiatives

7.4.1. Inria International Labs

DICE is involved in the Inria IPL citylab project headed by Valerie Issarny.

7.4.2. Participation In other International Programs

DICE has a joint project on BigData and intermediation "Promises of intermediation platforms for services frugal in resources" that is carried out within the cooperation framework JORISS between ENS Lyon and ECNU Shanghai.

DICE is starting a cooperation with CERN for the design of a new Javascript 2D/3D architecture for LHC event display experiments.

7.5. International Research Visitors

7.5.1. Visits of International Scientists

7.5.1.1. Internships

In 2014, the team DICE supervised three internships of master students, including two international students.

PRIVATICS Project-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. FUI

7.2.1.1. XDATA

Title: XDATA.

Type: FUI.

Duration: April 2013 - April 2015.

Coordinator: Data Publica

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

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

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

7.2.2. ANR

7.2.2.1. 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.

7.2.2.2. 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.

7.2.2.3. 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.

7.2.3. Other

7.2.3.1. 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.

7.2.3.2. CAPPRIS

Title: CAPPRIS

Type: Inria Project Lab

Duration: January 2011 - 2014.

Coordinator: PRIVATICS

Others partners: Inria (CIDRE, Comete, Secsi,Smis), Eurecom, LAAS and CRIDS

Abstract: Cappris (Collaborative Action on the Protection of Privacy Rights in the Information Society) is an Inria Project Lab initiated in 2013. The general goal of Cappris is to foster the collaboration between research groups involved in privacy in France and the interaction between the computer science, law and social sciences communities in this area.

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 Associate Teams

7.4.1.1. CLOUDY

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

International Partner (Institution - Laboratory - Researcher):

University of California Berkeley (ÉTATS-UNIS)

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 of International Scientists

7.5.1.1. Explorer programme

Cunche Mathieu

Date: Oct 2014 - Nov 2014

Institution: NICTA (Australia)

PROSECCO Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

7.1.1.1. 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.

7.1.1.2. AJACS

Title: AJACS: Analyses of JavaScript Applications: Certification and Security

Other partners: Inria-Rennes/Celtique, Inria-Saclay/Toccata, Inria-Sophia Antipolis/INDES, Imperial College London

Duration: October 2014 - March 2019.

Coordinator: Alan Schmitt, Inria (France)

Abstract: The goal of the AJACS project is to provide strong security and privacy guarantees for web application scripts. To this end, we propose to define a mechanized semantics of the full JavaScript language, the most widely used language for the Web, to develop and prove correct analyses for JavaScript programs, and to design and certify security and privacy enforcement mechanisms.

7.1.2. FUI

7.1.2.1. 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

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. CRYSP

Type: FP7

Defi: NC

Instrument: ERC Starting Grant

Objectif: NC

Duration: November 2010 - October 2015

Coordinator: Karthikeyan Bhargavan

Partner: Inria (France)

Inria contact: Valérie Boutheon

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.

7.3. International Initiatives

7.3.1. Inria International Partners

7.3.1.1. Informal International Partners

- Microsoft Research (Cambridge, Redmond): Joint research and development on F*, miTLS, and JavaScript with Cedric Fournet, Markulf Kohlweiss, and Nikhil Swamy
- University of Pennsylvania, Portland State University, Harvard University: Joint research on Micro-Policies: Formally Verified Low-Level Tagging Schemes for Safety and Security
- Imperial College (London): Joint research on web application security with Sergio Maffeis
- University of Venice Ca'Foscari: Joint research on security APIs

7.4. International Research Visitors

7.4.1. Visits of International Scientists

- Nikhil Swamy, Limin Jia, Benjamin Pierce, Cedric Fournet visited our group and gave seminars.
- Matteo Maffei, Dominique Unruh, Gilles Barthe, François Dupressoir, came to teach at the Joint EasyCrypt-F*-CryptoVerif School.

7.4.1.1. Internships

Cairns Kelsey

Date: Mar 2014 - May 2014

Institution: Washington State University (USA)

Paraskevopoulou Zoi

Date: Apr 2014 - Sep 2014

Institution: National Technical University of Athens (Greece)

Giannarakis Nikolaos

Date: Apr 2014 - Sep 2014

Institution: National Technical University of Athens (Greece)

Azevedo De Amorim, Arthur

Date: Mar 2014 - Aug 2014

Institution: University of Pennsylvania (USA)

Jindal Shubham

Date: May 2014 - Jul 2014

Institution: Indian Institute of Technology Delhi (India)

Thomson Susan

Date: Jun 2014 - Aug 2014

Institution: University of Bristol (UK)