RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2015

Section Partnerships and Cooperations

Edition: 2016-03-21

ARIC Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

- ARC6 PhD Programme. The PhD grant of Valentina Popescu is funded since Sep. 2014 by Région Rhône-Alpes through the "ARC6" programme.
- PALSE Project. Benoît Libert was awarded a 500keur (from July 2014 to November 2016) grant for his PALSE (Programme d'Avenir Lyon Saint-Etienne) project *Towards practical enhanced asymmetric encryption schemes*.

9.2. National Initiatives

9.2.1. ANR HPAC Project

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

9.2.2. 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.

9.2.3. 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.

9.2.4. ANR MetaLibm Project

Participants: Claude-Pierre Jeannerod, Jean-Michel Muller.

MetaLibm is a four-year project (started in October 2013) focused on the design and implementation of code generators for mathematical functions and filters. The web page of the project is http://www.metalibm.org/ANRMetaLibm/. It is headed by Florent de Dinechin (INSA Lyon and Socrate team) and, besides Socrate and AriC, also involves teams from LIRMM (Perpignan), LIP6 (Paris), CERN (Geneva), and Kalray (Grenoble). The main goals of the project are to automate the development of mathematical libraries (libm), to extend it beyond standard functions, and to make it unified with similar approaches developed in or useful for signal processing (filter design). Within AriC, we are especially interested in studying the properties of fixed-point arithmetic and floating-point arithmetic that can help develop such a framework.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

LATTAC ERC GRANT. Damien Stehlé was awarded an ERC Starting Grant for his project *Euclidean lattices: algorithms and cryptography* (LattAC) in 2013 (1.4Meur for 5 years from January 2014). The LattAC project aims at studying all computational aspects of lattices, from algorithms for manipulating them to applications. The main objective is to enable the rise of lattice-based cryptography.

OPENDREAMKIT is a H2020 Infrastructure project providing substantial funding to the open source computational mathematics ecosystem. It will run for four years, starting from September 2015. Clément Pernet is a participant.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

9.4.1.1. Visiting Scientists

- Jung Hee Cheon from July to August;
- Arnold Neumaier from August to December;
- Khoa Ta Toa Nguyen until October;
- Peter Tang, from June to July;
- Yong Sue Song from July to August.

9.4.1.2. Internships

Fabrice Mouhartem

Date: February 2015–July 2015

Institution: ENS de Lyon

Supervisor: Benoît Libert

Alice Pellet-Mary

Date: February 2015–July 2015

Institution: ENS de Lyon

Supervisor: Damien Stehlé

Andrada Popa

Date: July 2015–September 2015

Institution: Technical University of Cluj-Napoca (Roumanie)

Supervisor: Nicolas Brisebarre

Pablo Rotondo

Date: March 2015–June 2015

Institution: Universidad de la Republica Uruguay (Uruguay)

Supervisor: Bruno Salvy

Weiqiang Wen

Date: February 2015–July 2015

Institution: SCNU, China

Supervisor: Damien Stehlé

CARAMEL Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

In the context of the research grant "CPER Cyberentreprises", involving the French ministry of research, Région Lorraine, Inria, CNRS, and the European fund FEDER, we solicited and obtained funding for a new computer equipment dedicated to the computation of large polynomial systems. The corresponding machine has been delivered in November 2015, and will be put into service in the first weeks of 2016.

9.2. 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.

9.2.1. 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. According to the schedule, the project ended on Dec. 31st, 2015. Two project meetings were held in 2015: in Nancy on January 13-14, 2015, and in Palaiseau on October 1-2, 2015. The last project meeting was attached to an international workshop which brought together international experts on the Discrete Logarithm Problem to discuss the massive advances on this topic during the last years. A mid-term project review of the CATREL project was conducted by ANR in March 2015. The review outcome was very positive.

9.2.2. PEPS JCJC INSII RiCoRé (Résolution de systèmes polynomiaux pour les codes correcteurs et la robotique)

Participant: Pierre-Jean Spaenlehauer.

The RiCoRé proposal has been accepted in the PEPS JCJC INSII program in 2015. This project is coordinated by Romain Lebreton (Maître de Conférence, Univ. Montpellier). The other participants are Salih Abdelaziz (Maître de Conférence, Univ. Montpellier) and Eleonora Guerrini (Maître de Conférence, Univ. Montpellier). The aim of this project is to study the interactions of symbolic algorithms for polynomial system solving with some problems arising in coding theory and robotics.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

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

  During his stay here, he worked on implementing the elliptic curve factorization method (ECM) on the Kalray MPPA-256 manycore processor. A paper is currently in progress.
- Nadia Heninger, Assistant Professor at the University of Pennsylvania, visited us from June 22 to June 26.

CASCADE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives with Industrials

7.1.1. PRINCE

Title: Proven Resilience against Information leakage in Cryptographic Engineering

Program: ANR ARPEGE

Duration: December 2010 – May 2015

Coordinator: Tranef

Partners:

- ENS
- UVSQ
- Oberthur Technologies
- Ingenico
- Gemalto
- Tranef

Local coordinator: Michel Abdalla

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.

7.1.2. SIMPATIC

Title: SIM and PAiring Theory for Information and Communications security

Program: ANR INS

Duration: February 2013 – July 2016

Coordinator: Orange Labs

Partners:

- Orange Labs
- ENS
- INVIA
- Oberthur Technologies
- STMicroelectronics
- Université Bordeaux 1
- Université de Caen Basse-Normandie
- Université de Paris VIII

Local coordinator: David Pointcheval

We aim at providing the most possible efficient and secure hardware/software implementation of a bilinear pairing in a SIM card.

7.1.3. CryptoComp

Program: FUI

Duration: October 2014 – September 2017

Coordinator: CryptoExperts

Partners:

CEA

CNRS

Kalray

Inria

Dictao

Université de Limoges

VIACESS

Bertin technologies

GEMALTO

Local coordinator: Vadim Lyubashevsky (until July 2015) and David Pointcheval (from August 2015)

We aim at studying delegation of computations to the cloud, in a secure way.

7.2. National Collaborations within Academics

7.2.1. ROMAnTIC

Title: Randomness in Mathematical Cryptography

Program: ANR JCJC

Duration: October 2012 – September 2016

PI: Damien Vergnaud

Partners:

ANSSI

Univ. Paris 7

Univ. Limoges

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).

7.2.2. CLE

Title: Cryptography from Learning with Errors

Program: ANR JCJC

Duration: October 2013 – December 2015

PI: Vadim Lyubashevsky

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.

7.2.3. EnBiD

Title: Encryption for Big Data

Program: ANR JCJC

Duration: October 2014 – September 2018

PI: Hoeteck Wee

Partners:

Univ. Paris 2

Univ. Limoges

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.

7.3. European Initiatives

7.3.1. CryptoAction

Title: Cryptography for Secure Digital Interaction

Program: H2020 ICT COST

Duration: April 2014 – April 2018

Local coordinator: Vadim Lyubashevsky (until July 2015) and Michel Abdalla (from August 2015)

The aim of this COST CryptoAction is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments.

7.3.2. CryptoCloud

Title: Cryptography for the Cloud

Program: FP7 ERC Advanced Grant

Duration: June 2014 – May 2019

PI: David Pointcheval

The goal of the CryptoCloud project is to develop new interactive tools to provide privacy to the Cloud.

7.3.3. SAFEcrypto

Title: Secure Architectures of Future Emerging Cryptography

Program: H2020

Duration: January 2015 - January 2019

Coordinator: The Queen's University of Belfast

Partners:

Inria/ENS (France)

Emc Information Systems International (Ireland)

Hw Communications (United Kingdom)

The Queen's University of Belfast (United Kingdom)

Ruhr-Universitaet Bochum (Germany)

Thales Uk (United Kingdom)

Universita della Svizzera italiana (Switzerland)

Local coordinator: Vadim Lyubashevsky (until July 2015) and Michel Abdalla (from August 2015)

SAFEcrypto will provide a new generation of practical, robust and physically secure post quantum cryptographic solutions that ensure long-term security for future ICT systems, services and applications. Novel public-key cryptographic schemes (digital signatures, authentication, public-key encryption, identity-based encryption) will be developed using lattice problems as the source of computational hardness. The project will involve algorithmic and design optimisations, and implementations of the lattice-based cryptographic schemes addressing the cost, energy consumption, performance and physical robustness needs of resource-constrained applications, such as mobile, battery-operated devices, and of real-time applications such as network security, satellite communications and cloud. Currently a significant threat to cryptographic applications is that the devices on which they are implemented on leak information, which can be used to mount attacks to recover secret information. In SAFEcrypto the first analysis and development of physical-attack resistant methodologies for lattice-based cryptographic implementations will be undertaken. Effective models for the management, storage and distribution of the keys utilised in the proposed schemes (key sizes may be in the order of kilobytes or megabytes) will also be provided. This project will deliver proof-of-concept demonstrators of the novel lattice-based public-key cryptographic schemes for three practical real-word case studies with real-time performance and low power consumption requirements. In comparison to current state-of-the-art implementations of conventional public-key cryptosystems (RSA and Elliptic Curve Cryptography (ECC)), SAFEcrypto's objective is to achieve a range of lattice-based architectures that provide comparable area costs, a 10-fold speed-up in throughput for real-time application scenarios, and a 5-fold reduction in energy consumption for low-power and embedded and mobile applications.

7.3.4. ECRYPT-NET

Title: Advanced Cryptographic Technologies for the Internet of Things and the Cloud

Program: H2020 ITN

Duration: March 2015 – February 2019

Coordinator: KU Leuven (Belgium)

Partners:

KU Leuven (Belgium)

École Normale Supérieure (France)

Ruhr-Universität Bochum (Germany)

Royal Holloway, University of London (UK)

University of Bristol (UK)

CryptoExperts (France)

NXP Semiconductors (Belgium)

Technische Universiteit Eindhoven (the Netherlands)

Local coordinator: Michel Abdalla

ECRYPT-NET is a research network of six universities and two companies, as well as 7 associated companies, that intends to develop advanced cryptographic techniques for the Internet of Things and the Cloud and to create efficient and secure implementations of those techniques on a broad range of platforms.

7.3.5. aSCEND

Title: Secure Computation on Encrypted Data

Program: H2020 ERC Starting Grant

Duration: June 2015 – May 2020

PI: Hoeteck Wee

The goals of the aSCEND project are (i) to design pairing and lattice-based functional encryption that are more efficient and ultimately viable in practice; and (ii) to obtain a richer understanding of expressive functional encryption schemes and to push the boundaries from encrypting data to encrypting software.

7.4. 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.

7.5. International Research Visitors

- Dennis Hofheinz (KIT, Germany)
- Melissa Chase (MSR Redmond)
- Mariana Raykova (Yale University)
- Phil Rogaway (UC Davis)
- Alexandra Boldyreva (Georgia Tech)

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). 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 was the European director of LIAMA until October 2015.

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)

Guangwu Xu (Univ. Wisconsin, USA)

5.4.2. Visits to International Teams

5.4.2.1. Research stays abroad

Yang Yu visited CWI for 3 months in Fall 2015.

GALAAD2 Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. 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.

7.1.2. 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.

7.2. International Initiatives

7.2.1. 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 2014-August 2015. 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.

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.

We coordinate a research project which is funded by the regional program Math-AmSud for two years: 2015-2016. This project is composed by research teams from Argentina, Universidad de Buenos Aires (Nicolás Botbol, Alicia Dickenstein), Brazil, Universidade Federal de Rio de Janeiro, de Pernambuco e de Sergipe (Sayed Hamid Hassanzadeh, Aron Simis) and France, Institut de Mathématiques de Jussieu (Marc Chardin) and Galaad.

Title: Geometry of SYzygies of RAtional Maps with applications to geometric modeling (SYRAM)

Abstract: The study of rational maps is of theoretical interest in algebraic geometry and commutative algebra, and of practical importance in geometric modeling. This research proposal focus on rational maps in low dimension, typically parameterizations of curves and surfaces embedded in the projective space of dimension 3, but also dominant rational maps in dimension two and three. The two main objectives amount to unravel geometric properties of these rational maps from the syzygies of their projective coordinates. The first one aims at extending and generalizing the determination of the closed image of a rational map, as well as its geometric features, whereas the second one will focus on the study of dominant rational maps, in particular on the characterization of those that are generically one-to-one.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

7.3.1.1. Internships

Ibrahim Adamou (Université Dan Dicko DanKoulodo de Maradi, Niger), *Voronoï diagram of half-lines*, December 2015 - January 2016.

Nathan Clement (University of Texas at Austin, USA), *Offset of parametric curves*, Jun 2015-Aug 2015

Alexis Papagiannopoulos (NTUA, Athens, Greece), *Isogeometric analysis and parameterization of computational domains*, May 2015- September 2015.

Meng Wu (Hefei Univ. of Technology, China), *Splines over domain with arbitrary topology and isogeometric applications*, October 2015 - November 2015.

7.3.2. Visits to International Teams

7.3.2.1. Sabbatical programme

Hubert Evelyne

Date: Sep 2015 - Feb 2016

Institution: Fields Institute, Toronto, Canada.

GEOMETRICA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR Présage

Participants: Marc Glisse, 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?

9.1.2. ANR TOPDATA

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

- Acronym : TopData.

- Type : ANR blanc.

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

- Coordinator : Frédéric Chazal (GEOMETRICA).

- Duration : 4 years starting October 2013.

- Others Partners: Département de Mathématiques (Université Paris Sud), Institut de Mathématiques (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

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. ERC GUDHI

Title: Algorithmic Foundations of Geometry Understanding in Higher Dimensions.

Program: FP7.

Type: ERC.

Duration: February 2014 - January 2019.

Coordinator: Inria.

PI: Jean-Daniel Boissonnat.

'The central goal of this proposal is to settle the algorithmic foundations of geometry understanding in dimensions higher than 3. We coin the term geometry understanding to encompass a collection of tasks including the computer representation and the approximation of geometric structures, and the inference of geometric or topological properties of sampled shapes. The need to understand geometric structures is ubiquitous in science and has become an essential part of scientific computing and data analysis. Geometry understanding is by no means limited to three dimensions. Many applications in physics, biology, and engineering require a keen understanding of the geometry of a variety of higher dimensional spaces to capture concise information from the underlying often highly nonlinear structure of data. Our approach is complementary to manifold learning techniques and aims at developing an effective theory for geometric and topological data analysis. To reach these objectives, the guiding principle will be to foster a symbiotic relationship between theory and practice, and to address fundamental research issues along three parallel advancing fronts. We will simultaneously develop mathematical approaches providing theoretical guarantees, effective algorithms that are amenable to theoretical analysis and rigorous experimental validation, and perennial software development. We will undertake the development of a high-quality open source software platform to implement the most important geometric data structures and algorithms at the heart of geometry understanding in higher dimensions. The platform will be a unique vehicle towards researchers from other fields and will serve as a basis for groundbreaking advances in scientific computing and data analysis.'

9.3. International Initiatives

9.3.1. CATS

Title: Computations And Topological Statistics.

International Partner (Institution - Laboratory - Researcher):

Carnegie Mellon University (United States) - Department of Statistics - Larry Wasserman

Start year: 2015.

See also: http://geometrica.saclay.inria.fr/collaborations/CATS/CATS.html

Topological Data Analysis (TDA) is an emergent field attracting interest from various communities, that has recently known academic and industrial successes. Its aim is to identify and infer geometric and topological features of data to develop new methods and tools for data exploration and data analysis. TDA results mostly rely on deterministic assumptions which are not satisfactory from a statistical viewpoint and which lead to a heuristic use of TDA tools in practice. Bringing together the strong expertise of two groups in Statistics (L. Wasserman's group at CMU) and Computational Topology and Geometry (Inria Geometrica), the main objective of CATS is to set-up the mathematical foundations of Statistical TDA, to design new TDA methods and to develop efficient and easy-to-use software tools for TDA.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Ramsay Dyer (University of Groningen), May

Arijit Ghosh (MPII, Saarbrucken), June-July

Clément Maria (Queen's College, Brisbane), June

Omer Brobowski (Duke University), May

Jessica Cisewski (Carnegie Mellon), October

Jisu Kim (Carnegie Mellon), May-July

Yanir Kleiman (Tel Aviv University), October

Bertrand Michel (Paris 6), 2015

Jan Felix Senge (Bremen), October

Primoz Skraba (Jozef Stefan Institute), May

Kelly Spendlove (Rutgers), May-July

Jian Sun (Tsinghua), February

Justin Solomon (Stanford), February

9.4.1.1. Internships

Sivaprasad Sudhir (IIT Bombay), June-July

Stéphane Lundy (Supélec), July-August

Siargey Kachanovich (ENS Rennes), March-August

Anatole Moreau (EPITA), May-August

Tullia Padellini (Roma University), May-September

Yuping Ren (Erasmus), January-July

9.4.2. Visits to International Teams

9.4.2.1. Research stays abroad

+ Steve Oudot spent 1 month in July-August in the group of Benjamin Burton at the Pure Maths Department of University of Queensland, Australia.

GRACE Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. 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.

Two M2 interns, Loïs Saublet and Kofi Manful, have been hired, located in Aviz team, and D. Augot co-supervised them with Petra and Tobias Isenberg.

9.1.2. 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). After hiring J. Nielsen the first year, we have hired V. Ducet for the second year, both 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 [33], 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.

9.2. National Initiatives

9.2.1. ANR

- CATREL (accepted June 2012, ending December 2015): "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.
- MANTA (accepted July 2015, starting January 2016): "Curves, surfaces, codes and cryptography". This project deals with applications of coding theory error correcting codes to in cryptography, multi-party computation, and complexity theory, using advanced topics in algebraic geometry and number theory. See http://anr-manta.inria.fr/

9.2.2. DGA

- DIFMAT-3: this one-year project aims to find matrices with good diffusion properties over small finite fields. 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 [34].
- 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 Rennes), and D. Augot.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: TECHNISCHE UNIVERSITEIT EINDHOVEN

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

Nxp Semiconductors Belgium Nv (Belgium)

Ruhr-Universitaet Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Coding Theory and Cryptology group, Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

Online security depends on a very few underlying cryptographic algorithms. Public-key algorithms are particularly crucial since they provide digital signatures and establish secure communication. Essentially all applications today are based on RSA or on the discrete-logarithm problem in finite fields or on elliptic curves. Cryptographers optimize parameter choices and implementation details for these systems and build protocols on top of these systems; cryptanalysts fine-tune attacks and establish exact security levels for these systems.

It might seem that having three systems offers enough variation, but these systems are all broken as soon as large quantum computers are built. The EU and governments around the world are investing heavily in building quantum computers; society needs to be prepared for the consequences, including cryptanalytic attacks accelerated by these computers. Long-term confidential documents such as patient health-care records and state secrets have to guarantee security for many years, but

information encrypted today using RSA or elliptic curves and stored until quantum computers are available will then be as easy to decipher.

PQCRYPTO will allow users to switch to post-quantum cryptography: cryptographic systems that are not merely secure for today but that will also remain secure long-term against attacks by quantum computers. PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, with reference implementations.

9.3.2. Major European Organizations with which the Team have followed Collaborations

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.

9.4. International Initiatives

9.4.1. Inria International Partners

9.4.1.1. Informal International Partners

- P. Beelen, J. Nielsen, DTU Lyngby
- M. Bossert, Ulm Universität
- S. Galbraith, Department of Mathematics, University of Auckland.

9.5. International Research Visitors

9.5.1. Internships

- C. Berghoff is a visiting Phd student, from Bonn Universität.

LFANT Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR Peace – Parameter spaces for Efficient Arithmetic and Curve security Evaluation

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

7.1.2. ANR Simpatic – SIM and PAiring Theory for Information and Communications security

Participants: Guilhem Castagnos, Damien Robert, Sorina Ionica, Cyril Bouvier.

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.

G. Castagnos is a participant in the Task 4 whose role is to design new cryptographic primitives adapted to the specific applications of the Simpatic Project.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. ANTICS

Title: Algorithmic Number Theory in Computer Science

Programm: FP7

Duration: January 2012 - December 2016

Coordinator: Inria

Inria contact: Andreas Enge

'During the past twenty years, we have witnessed profound technological changes, summarised under the terms of digital revolution or entering the information age. It is evident that these technological changes will have a deep societal impact, and questions of privacy and security are primordial to ensure the survival of a free and open society. Cryptology is a main building block of any security solution, and at the heart of projects such as electronic identity and health cards, access control, digital content distribution or electronic voting, to mention only a few important applications. During the past decades, public-key cryptology has established itself as a research topic in computer science; tools of theoretical computer science are employed to "prove" the security of cryptographic primitives such as encryption or digital signatures and of more complex protocols. It is often forgotten, however, that all practically relevant public-key cryptosystems are rooted in pure mathematics, in particular, number theory and arithmetic geometry. In fact, the socalled security "proofs" are all conditional to the algorithmic untractability of certain number theoretic problems, such as factorisation of large integers or discrete logarithms in algebraic curves. Unfortunately, there is a large cultural gap between computer scientists using a black-box security reduction to a supposedly hard problem in algorithmic number theory and number theorists, who are often interested in solving small and easy instances of the same problem. The theoretical grounds on which current algorithmic number theory operates are actually rather shaky, and cryptologists are generally unaware of this fact. The central goal of ANTICS is to rebuild algorithmic number theory on the firm grounds of theoretical computer science.'

7.2.1.2. Open Dream Kit

Title: Algorithmic Number Theory in Computer Science

Programm: FP7

Duration: September 2015 - August 2019

Inria contact: Karim Belabas

OpenDreamKit is a Horizon 2020 European Research Infrastructure project (#676541, call e-infrastructures for virtual research environments) that will run for four years, starting from September 2015. It will provide substantial funding to the open source computational mathematics ecosystem, and in particular popular tools such as LinBox, MPIR, SageMath, GAP, Pari/GP, LMFDB, Singular, MathHub, and the IPython/Jupyter interactive computing environment.

From this ecosystem, OpenDreamKit will deliver a flexible toolkit enabling research groups to set up Virtual Research Environments, customised to meet the varied needs of research projects in pure mathematics and applications, and supporting the full research life-cycle from exploration, through proof and publication, to archival and sharing of data and code.

The project involves about 50 people spread over 15 sites in Europe, with a total budget of about 7.6 million euros. The largest portion of that will be devoted to employing an average of 11 researchers and developers working full time on the project. Additionally, the participants will contribute the equivalent of six other people working full time.

Countries involved include France (Universités Paris-Sud, Versailles, Bordeaux, Grenoble and the industrial partner Logilab), Germany (Kaiserslautern, Bremen), United Kingdom (Oxford, Southampton, Sheffield, St Andrews, Warwick), Norway (Simula), Poland (University Silesia), Switzerland (University Zürich).

7.3. International Initiatives

7.3.1. 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 (EMA) in Libreville with the International Center for Pure and Applied Mathematics (ICPAM/CIMPA), March 2015, attended by most of the members of Macisa;
- The visit of Abdoul Aziz Ciss (Dakar) and Emmanuel Fouotsa (Bamenda) to Bordeaux, September 2015, for the Elliptic Curve Cryptography and Summer School conference;
- The visit of Tony Ezome to Bordeaux, October 2015;
- The visit of Damien Robert to Yaoundé, Cameroun, to give courses on cryptography for a special seminar on security event.

7.3.2. Inria International Partners

7.3.2.1. 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).

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Researchers visiting the team to give a talk to the team seminar include David Kohel (Université d'Aix-Marseille), Tony Ezome (Université des Sciences et Techniques de Masuku, Franceville), Abdoul Aziz Ciss (Ecole Polytechnique de Thiès, Sénégal), Emmanuel Fouotsa (École Normale Supérieure de l'Université de Bamenda), Renate Scheidler (University Calgary), Eduardo Friedman (Universidad de Chile), Benjamin Smith (Inria & LIX, École Polytechnique), Bernadette Perrin-Riou (Paris-Sud).

The visit of Ciss, Ezome and Fouotsa were also part of the collaboration through the Macisa team.

POLSYS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **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).

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. A3

Type: PEOPLE

Instrument: Career Integration Grant

Duration: May 2013 - April 2017

Coordinator: Jean-Charles Faugère

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

Inria contact: Elias Tsigaridas

Abstract: The project Algebraic Algorithms and Applications (A3) is an interdisciplinary and multidisciplinary project, with strong international synergy. It consists of four work packages The first (Algebraic Algorithms) focuses on fundamental problems of computational (real) algebraic geometry: effective zero bounds, that is estimations for the minimum distance of the roots of a polynomial system from zero, algorithms for solving polynomials and polynomial systems, derivation of non-asymptotic bounds for basic algorithms of real algebraic geometry and application of polynomial system solving techniques in optimization. We propose a novel approach that exploits

structure and symmetry, combinatorial properties of high dimensional polytopes and tools from mathematical physics. Despite the great potential of the modern tools from algebraic algorithms, their use requires a combined effort to transfer this technology to specific problems. In the second package (Stochastic Games) we aim to derive optimal algorithms for computing the values of stochastic games, using techniques from real algebraic geometry, and to introduce a whole new arsenal of algebraic tools to computational game theory. The third work package (Non-linear Computational Geometry), we focus on exact computations with implicitly defined plane and space curves. These are challenging problems that commonly arise in geometric modeling and computer aided design, but they also have applications in polynomial optimization. The final work package (Efficient Implementations) describes our plans for complete, robust and efficient implementations of algebraic algorithms.

8.2.2. Collaborations in European Programs, except FP7 & H2020

Program: ICT COST Action IC1403

Project acronym : CRYPTACUS)

Project title: Cryptanalysis of ubiquitous computing systems

Duration: 12/2014 – 12/2018

Coordinator: Prof Gildas AVOINE

Abstract: Recent technological advances in hardware and software have irrevocably affected the classical picture of computing systems. Today, these no longer consist only of connected servers, but involve a wide range of pervasive and embedded devices, leading to the concept of "ubiquitous computing systems".

The objective of the Action is to improve and adapt the existent cryptanalysis methodologies and tools to the ubiquitous computing framework. Cryptanalysis, which is the assessment of theoretical and practical cryptographic mechanisms designed to ensure security and privacy, will be implemented along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems.

Researchers have only recently started to focus on the security of ubiquitous computing systems. Despite the critical flaws found, the required highly-specialized skills and the isolation of the involved disciplines are a true barrier for identifying additional issues. The Action will establish a network of complementary skills, so that expertise in cryptography, information security, privacy, and embedded systems can be put to work together.

The outcome will directly help industry stakeholders and regulatory bodies to increase security and privacy in ubiquitous computing systems, in order to eventually make citizens better protected in their everyday life.

Program: COST Action IC1306

Project acronym : CryptoAction

Project title: Cryptography for Secure Digital Interaction

Duration: 04/2014 – 04/2018

Coordinator: Dr. Claudio ORLANDI

Abstract: As increasing amounts of sensitive data are exchanged and processed every day on the Internet, the need for security is paramount. Cryptography is the fundamental tool for securing digital interactions, and allows much more than secure communication: recent breakthroughs in cryptography enable the protection - at least from a theoretical point of view - of any interactive data processing task. This includes electronic voting, outsourcing of storage and computation, e-payments, electronic auctions, etc. However, as cryptography advances and becomes more complex, single research groups become specialized and lose contact with "the big picture". Fragmentation in this field can be dangerous, as a chain is only as strong as its weakest link. To ensure that the ideas

produced in Europe's many excellent research groups will have a practical impact, coordination among national efforts and different skills is needed. 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. The Action will foster a network of European research centers thus promoting movement of ideas and people between partners.

8.3. International Initiatives

8.3.1. Inria International Labs

8.3.1.1. Inria@SiliconValley

See https://project.inria.fr/siliconvalley/fr/

Associate Team involved in the International Lab:

GOAL

Title: Geometry and Optimization with ALgebraic methods.

International Partner (Institution - Laboratory - Researcher):

University of California Berkeley (United States) - Dept. of Mathematics - Bernd Sturmfels

Start year: 2015

See also: http://www-polsys.lip6.fr/GOAL/index.html

Polynomial optimization problems form a subclass of general global optimization problems, which have received a lot of attention from the research community recently; various solution techniques have been designed. One reason for the spectacular success of these methods is the potential impact in many fields: data mining, big data, energy savings, etc. More generally, many areas in mathematics, as well as applications in engineering, biology, statistics, robotics etc. require a deeper understanding of the algebraic structure of their underlying objects.

A new trend in the polynomial optimization community is the combination of algebraic and numerical methods. Understanding and characterizing the algebraic properties of the objects occurring in numerical algorithms can play an important role in improving the efficiency of exact methods. Moreover, this knowledge can be used to estimate the quality (for example the number of significant digits) of numerical algorithms. In many situations each coordinate of the optimum is an algebraic number. The degree of the minimal polynomials of these algebraic numbers is the Algebraic Degree of the problem. From a methodological point of view, this notion of Algebraic Degree emerges as an important complexity parameter for both numerical and the exact algorithms. However, algebraic systems occurring in applications often have special algebraic structures that deeply influence the geometry of the solution set. Therefore, the (true) algebraic degree could be much less than what is predicted by general worst case bounds (using Bézout bounds, mixed volume, etc.), and would be very worthwhile to understand it more precisely.

The goal of this proposal is to develop algorithms and mathematical tools to solve geometric and optimization problems through algebraic techniques. As a long-term goal, we plan to develop new software to solve these problems more efficiently. These objectives encompass the challenge of identifying instances of these problems that can be solved in polynomial time with respect to the number of solutions and modeling these problems with polynomial equations.

The kickoff workshop was held at UC Berkeley in May 2015, see https://math.berkeley.edu/~bernd/GOALworkshop.html.

Both Carlos Améndola Cerón and Kaies Kubjas visited the team one month through the associated team.

8.3.1.2. Sino-European Laboratory of Informatics, Automation and Applied Mathematics (LIAMA)

See http://liama.ia.ac.cn/.

Associate Team involved in the International Lab:

ECCA

Title: Exact/Certifed Computation with Algebraic Systems

International Partner (Institution - Laboratory - Researcher):

KLMM – Chinese Academy of Sciences, Lihong Zhi.

Start year: 2012

See also: http://liama.ia.ac.cn/research/liama-projects/current/265-ecca-project-description-and-achievements.html

Exact/Certifed Computation with Algebraic Systems (ECCA) is a project run within the LIAMA Consortium as a cooperation project between CNRS/Inria/LIP6, KLMM, SKLOIS and LMIB. The main scientific objective of this project is to study and compute the solutions of nonlinear algebraic systems and their structures and properties with target applications to computational geometry, algebraic cryptanalysis, global optimization, and algebraic biology.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Carlos Améndola Cerón

Date: Sept. 2015

Institution: Technische Universität Berlin, Germany

Kaie Kubjas

Date: Oct. 2015

Institution: Aalto Science Institute, Finland

Cordian Riener

Date: May 2015

Institution: Aalto Science Institute, Finland

Igor Shparlinski

Date: Sept. 2015

Institution: The University of New South Wales, Australia

Rekha Thomas

Date: Feb. 2015

Institution: University of Washington, USA.

8.4.1.1. Internships

Matías Bender

Date: Sep 2014 - Feb 2015

Institution: Universidad de Buenos Aires (Argentina)

Supervisor: Jean-Charles Faugère

Jérôme Govinden

Date: Feb. 2015 - Sept. 2015

Institution: UPMC

Supervisors: Jean-Charles Faugère, Ludovic Perret

SECRET Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR BLOC** (10/11 → 03/16)
  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 → 02/16)
  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 → 12/15)
  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.

- **DGA-MI (**$09/15 \rightarrow 09/16$**)**
  Analysis of binary streams: reconstructing LDPC codes.
  28.6 kEuros.
  The objective of this contract was to examine the code reconstruction problem (from noisy observation) for LDPC codes.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: TECHNISCHE UNIVERSITEIT EINDHOVEN

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

Nxp Semiconductors Belgium Nv (Belgium)

Ruhr-Universitaet Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

Online banking, e-commerce, telemedicine, mobile communication, and cloud computing depend fundamentally on the security of the underlying cryptographic algorithms. Public-key algorithms are particularly crucial since they provide digital signatures and establish secure communication without requiring in-person meetings. Essentially all applications today are based on RSA or on the discrete-logarithm problem in finite fields or on elliptic curves. Cryptographers optimize parameter choices and implementation details for these systems and build protocols on top of these systems; cryptanalysts fine-tune attacks and establish exact security levels for these systems. Alternative systems are far less visible in research and unheard of in practice. It might seem that having three systems offers enough variation, but these systems are all broken as soon as large quantum computers are built. The EU and governments around the world are investing heavily in building quantum computers; society needs to be prepared for the consequences, including cryptanalytic attacks accelerated by these computers. Long-term confidential documents such as patient healthcare records and state secrets have to guarantee security for many years, but information encrypted today using RSA or elliptic curves and stored until quantum computers are available will then be as easy to decipher as Enigma-encrypted messages are today. PQCRYPTO will allow users to switch to post-quantum cryptography: cryptographic systems that are not merely secure for today but that will also remain secure long-term against attacks by quantum computers. PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet of Things. PQCRYPTO will provide efficient implementations of high-security post-quantum cryptography for a broad spectrum of real-world applications.

8.2.2. 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.

Anne Canteaut is co-leader of the working group on cryptographic primitives.

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)

Start year: 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

- Georgi Ivanov, Bulgarian Academy of Science, Sofia, Bulgaria, visiting PhD student (COST CryptoAction), Jan.-Feb. 2015
- Sumanta Sarkar, ISI Kolkata, India, visiting scientist, Feb.-March 2015
- Dimitrios Simos, SBA Research, Vienna, Austria, visiting scientist, July 2015
- Nastja Cepak, University of Primoska, Koper, Slovenia, visiting PhD student, from Sept. 2015.
- Enes Pasalic, University of Primoska, Koper, Slovenia, visiting scientist, Oct. 2015.

8.4.1.1. Internships

- Rodolfo Canto Torres, Univ. Bordeaux (M2), March-Aug. 2015
- Yann Rotella, MPRI and Telecom ParisTech (M2), March-Sept. 2015
- Aurélie Phesso, Univ. Bordeaux (M1), June-Aug. 2015
- Victoire Dupont de Dinechin, HEC (L3), June 2015

SPECFUN Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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.
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/.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, except FP7 & H2020

- Program: COST
- Project acronym: EUTYPES (CA15123)
- Project title: The European research network on types for programming and verification
- Duration: October 2015 - October 2019
- Coordinator: Herman Geuvers (Radboud University, Nijmegen, the Netherlands)
- Other partners: Czech Republic, Estonia, Macedonia, Germany, Greece, the Netherlands, Norway, Poland, Serbia, Slovenia, United Kingdom.
- Abstract: Types are pervasive in programming and information technology. A type defines a formal interface between software components, allowing the automatic verification of their connections, and greatly enhancing the robustness and reliability of computations and communications. In rich dependent type theories, the full functional specification of a program can be expressed as a type. Type systems have rapidly evolved over the past years, becoming more sophisticated, capturing new aspects of the behaviour of programs and the dynamics of their execution. This COST Action will give a strong impetus to research on type theory and its many applications in computer science, by promoting: (1) the synergy between theoretical computer scientists, logicians and mathematicians to develop new foundations for type theory, for example as based on the recent development of “homotopy type theory”, (2) the joint development of type theoretic tools as proof assistants and integrated programming environments, (3) the study of dependent types for programming and its deployment in software development, (4) the study of dependent types for verification and its deployment in software analysis and verification. The action will also tie together these different areas and promote cross-fertilisation. Europe has a strong type theory community, ranging from foundational research to applications in programming languages, verification and theorem proving, which is in urgent need of better networking. A COST Action that crosses the borders will support the collaboration between groups and complementary expertise, and mobilise a critical mass of existing type theory research.

VEGAS Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. 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 random continuous geometric objects.

The project, with a total budget of 400kE, started on Dec. 31st, 2011 and will end in march 2016. It is coordinated by Xavier Goaoc who moved from the Vegas team to Marne-la-Vallée university in 2013.

Project website: http://webloria.loria.fr/~moroz/ANR-Presage.

7.1.2. 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 numerical methods. Thus we plan to extend the class of manipulators that can be analyzed, and the class of algebraic curves and surfaces that can be visualized with certification.

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

In 2015, the project funded the postdoc position of Rémi Imbach.

Project website: https://project.inria.fr/singcast/.

7.2. International Research Visitors

7.2.1. Visits to International Teams

Monique Teillaud was invited at the Workshop on Computational Geometric and Algebraic Topology, *Mathematisches Forschungsinstitut Oberwolfach*, where she presented CGAL, the Computational Geometry Algorithms Library. https://www.mfo.de/occasion/1542/www_view

ALF Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. 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, ProbaYes, IRIT, Onera, Verimag, Inria, Irisa, Tima and Armines.

9.1.2. Inria Project Lab: Multicore 2013-2016

Participants: Erven Rohou, 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.

9.1.3. 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 http://parasuite.inria.fr/, to the research community.

9.1.4. ANR Continuum 2015–2019

Participant: Erven Rohou.

The CONTINUUM project aims to address the energy-efficiency challenge in future computing systems by investigating a design continuum for compute nodes, which seamlessly goes from software to technology levels via hardware architecture. Power saving opportunities exist at each of these levels, but the real measurable gains will come from the synergistic focus on all these levels as considered in this project. Then, a cross-disciplinary collaboration is promoted between computer science and microelectronics, to achieve two main breakthroughs: i) combination of state-of-the-art heterogeneous adaptive embedded multicore architectures with emerging communication and memory technologies and, ii) power-aware dynamic compilation techniques that suitably match such a platform.

Continuum started on Oct 1st 2015. Partners are LIRMM and Cortus SAS.

9.1.5. ANR CHIST-ERA SECODE 2016-2018

Participants: Damien Hardy, Erven Rohou.

SECODE (Secure Codes to thwart Cyber-physical Attacks) was accepted, and will start on January 1st 2016.

In this project, we specify and design error correction codes suitable for an efficient protection of sensitive information in the context of Internet of Things (IoT) and connected objects. Such codes mitigate passive attacks, like memory disclosure, and active attacks, like stack smashing. The innovation of this project is to leverage these codes for protecting against both cyber and physical attacks. The main advantage is a full coverage of attacks of the connected embedded systems, which is considered as a smart connected device and also a physical device. The outcome of the project is first a method to generate and execute cyber-resilient software, and second to protect data and its manipulation from physical threats like side-channel attacks. Theses results are demonstrated by using a smart sensor application with hardened embedded firmware and tamper-proof hardware platform.

Partners are Télécom Paris Tech, Université Paris 8, University of Sabancı(Turkey), and Université Catholique de Louvain (Belgium).

9.1.6. 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.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. ANTAREX

Participant: Erven Rohou.

Title: Auto-Tuning and Adaptivity appRoach for Energy efficient exascale HPC Systems

Programm: H2020

Duration: September 2015 - September 2018

Coordinator: Politecnico di Milano, Italy (POLIMI)

Partners:

- Consorzio Interuniversitario Cineca (Italy)
- Dompe Farmaceutici Spa (Italy)
- Eidgenoessische Technische Hochschule Zuerich (Switzerland)
- Vysoka Skola Banska - Technicka Univerzita Ostrava (Czech Republic)
- Politecnico di Milano (Italy)
- Sygic As (Slovakia)
- Universidade Do Porto (Portugal)

Inria contact: Erven Rohou

Energy-efficient heterogeneous supercomputing architectures need to be coupled with a radically new software stack capable of exploiting the benefits offered by the heterogeneity at all the different levels (supercomputer, job, node) to meet the scalability and energy efficiency required by Exascale supercomputers. ANTAREX will solve these challenging problems by proposing a disruptive holistic approach spanning all the decision layers composing the supercomputer software stack and exploiting effectively the full system capabilities (including heterogeneity and energy management). The main goal of the ANTAREX project is to provide a breakthrough approach to express application self-adaptivity at design-time and to runtime manage and autotune applications for green and heterogenous High Performance Computing (HPC) systems up to the Exascale level.

9.2.1.2. Eurolab-4-HPC

Participant: André Seznec.

Title: EuroLab-4-HPC: Foundations of a European Research Center of Excellence in High Performance Computing Systems

Programm: H2020

Duration: September 2015 - September 2017

Coordinator: CHALMERS TEKNISKA HOEGSKOLA AB

Partners:

Barcelona Supercomputing Center - Centro Nacional de Supercomputacion (Spain)

Chalmers Tekniska Hoegskola (Sweden)

Ecole Polytechnique Federale de Lausanne (Switzerland)

Foundation for Research and Technology Hellas (Greece)

Universitaet Stuttgart (Germany)

Rheinisch-Westfaelische Technische Hochschule Aachen (Germany)

Technion - Israel Institute of Technology (Israel)

Universitaet Augsburg (Germany)

The University of Edinburgh (United Kingdom)

Universiteit Gent (Belgium)

The University of Manchester (United Kingdom)

Inria contact: Albert Cohen (Inria Paris)

Europe has built momentum in becoming a leader in large parts of the HPC ecosystem. It has brought together technical and business stakeholders from application developers via system software to exascale systems. Despite such gains, excellence in high performance computing systems is often fragmented and opportunities for synergy missed. To compete internationally, Europe must bring together the best research groups to tackle the longterm challenges for HPC. These typically cut across layers, e.g., performance, energy efficiency and dependability, so excellence in research must target all the layers in the system stack. The EuroLab-4-HPC project's bold overall goal is to build connected and sustainable leadership in high-performance computing systems by bringing together the different and leading performance oriented communities in Europe, working across all layers of the system stack and, at the same time, fueling new industries in HPC.

9.2.1.3. DAL

Participants: Pierre Michaud, Bharath Narasimha Swamy, Sylvain Collange, Erven Rohou, André Seznec, Arthur Perais, Surya Khizakanchery Natarajan, Sajith Kalathingal, Tao Sun, Andrea Mondelli, Aswinkumar Sridharan.

Title: DAL: Defying Amdahl's Law

Program: FP7

Type: ERC

Duration: April 2011 - March 2016

Coordinator: Inria

Inria contact: André Seznec

Multicore processors have now become mainstream for both general-purpose and embedded computing. Instead of working on improving the architecture of the next generation multicore, with the DAL project, we deliberately anticipate the next few generations of multicores. While multicores featuring 1000's of cores might become feasible around 2020, there are strong indications that sequential programming style will continue to be dominant. Even future mainstream parallel applications will exhibit large sequential sections. Amdahl's law indicates that high performance on these sequential sections is needed to enable overall high performance on the whole application. On many (most) applications, the effective performance of future computer systems using a 1000-core processor chip will significantly depend on their performance on both sequential code sections and single thread. We envision that, around 2020, the processor chips will feature a few complex cores and many (may be 1000's) 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.

9.2.1.4. ARGO

Participants: Isabelle Puaut, Damien Hardy.

Title: Argo: WCET-Aware Parallelization of Model-Based Applications for Heterogeneous Parallel Systems

Program: H2020

Type: RIA

Duration: Jan 2016 - Dec 2018

Coordinator: Karlsruher Institut fuer Technologie (KIT)

Université Rennes I contact: Steven Derrien

Partners:

Karlsruher Institut fuer Technologie (KIT)

SCILAB enterprises SAS

Recore Systems BV

Université de Rennes 1

Technologiko Ekpaideftiko Idryma (TEI) Dytikis Elladas

Absint GmbH

Deutsches Zentrum fuer Luft - und Raumfahrt EV

Fraunhofer

Increasing performance and reducing costs, while maintaining safety levels and programmability are the key demands for embedded and cyber-physical systems in European domains, e.g. aerospace, automation, and automotive. For many applications, the necessary performance with low energy consumption can only be provided by customized computing platforms based on heterogeneous many-core architectures. However, their parallel programming with time-critical embedded applications suffers from a complex toolchain and programming process. Argo (WCET-Aware PaRallelization of Model-Based Applications for HeteroGeneOus Parallel Systems) will address this challenge with a holistic approach for programming heterogeneous multi- and many-core architectures using automatic parallelization of model-based real-time applications. Argo will enhance WCET-aware automatic parallelization by a crosslayer programming approach combining automatic tool-based and user-guided parallelization to reduce the need for expertise in programming parallel heterogeneous architectures. The Argo approach will be assessed and demonstrated by prototyping comprehensive time-critical applications from both aerospace and industrial automation domains on customized heterogeneous many-core platforms.

9.2.2. Collaborations in European Programs, except FP7 & H2020

9.2.2.1. COST Action TACLe - Timing Analysis on Code-Level (http://www.tacle.eu) 10-2012/09-2016

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.

9.2.3. Collaborations with Major European Organizations

9.2.3.1. 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.

9.3. International Initiatives

9.3.1. Inria Associate Teams not involved in an Inria International Labs

9.3.1.1. PROSPIEL

Title: Profiling and specialization for locality

International Partner (Institution - Laboratory - Researcher):

Universidade Federal de Minas Gerais (Brazil) - Dpt of Computer Science - Fernando Magno Quintao Pereira

Start year: 2015

See also: https://team.inria.fr/alf/prospiel/

The PROSPIEL project aims at optimizing parallel applications for high performance on new throughput-oriented architectures: GPUs and many-core processors. Traditionally, code optimization is driven by a program analysis performed either statically at compile-time, or dynamically at run-time. Static program analysis is fully reliable but often over-conservative. Dynamic analysis provides more accurate data, but faces strong execution time constraints and does not provide any guarantee. By combining profiling-guided specialization of parallel programs with runtime checks for correctness, PROSPIEL seeks to capture the advantages of both static analysis and dynamic analysis. The project relies on the polytope model, a mathematical representation for parallel loops, as a theoretical foundation. It focuses on analyzing and optimizing performance aspects that become increasingly critical on modern parallel computer architectures: locality and regularity.

9.3.2. Inria International Partners

9.3.2.1. Informal International Partners

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).

9.3.3. Participation In other International Programs

9.3.3.1. UFMG Chair (Brazil)

Program: Cátedras Francesas UFMG

Title: A language runtime with fault-resiliency for approximate computing

Inria principal investigator: Sylvain Collange

International Partner (Institution - Laboratory - Researcher):

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

Duration: Sep 2015 - Oct 2015

In this project we propose to implement fault tolerance at the runtime level within a virtual machine for a managed language. Our approach consists in developing a just-in-time compiler analysis that identifies and extracts side-effect free computations, such as pure functions, within the code. For each of these computations, an approximate implementation will be generated in addition to the regular native code. When the computation is invoked during execution, the runtime will first execute the approximate implementation. In case the quality or accuracy of the result is not sufficient at the time it is needed, the runtime will transparently re-execute the computation in exact mode.

9.4. International Research Visitors

9.4.1. Visits to International Teams

9.4.1.1. Explorer programme

Perais Arthur

Date: Jan 2015 - Apr 2015

Institution: Carnegie Mellon University (United States)

9.4.1.2. Research stays abroad

Sylvain Collange has been invited on a professor chair at Universidade Federal de Minas Gerais, Brazil (September-October 2015).

ATEAMS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. Master Software Engineering

ATEAMS is a 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.

8.1.2. 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.

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

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

8.1.4. Domain-Specific Languages: A Big Future for Small Programs

Software and programming have a brilliant past that has brought us the automation of many expected and unexpected human and societal activities ranging from banking and consumer electronics to mobile networking, search engines and social networks. The present of software is overwhelming: many software systems have sizes in the range of 10–100 million lines of source code and contain tens of thousands of errors that are yet to be discovered. We claim that software will only have a big future if software itself becomes smaller. Smaller software leads to higher software productivity (we have to write less) and higher software quality (quality guarantees become part of the language and not of the program).

This project is funded by NWO (the Dutch national science foundation).

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

- FP7 STREP “OSSMETER — Automated Measurement and Analysis of Open Source Software” (ended in 2015)

8.2.2. Collaborations with Major European Organizations

Centrum Wiskunde & Informatica (CWI): Software Analysis & Transformation (Netherlands)
CWI SWAT is the research team associated directly with ATEAMS.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

ATEAMS collaborates with the following research teams:

- Eindhoven Technical University - SET (Eindhoven, The Netherlands)
- Universiteit van Amsterdam - Systems and Network Engineering (Amsterdam, The Netherlands)
- Royal Holloway University of London - Dept. of Computer Science
- The University of Hong Kong (China) - Computer Science
- Delft Technical University (The Netherlands)
- University of Texas at Austin (USA)
- TU Darmstadt (Germany)

8.3.1.2. Research stays abroad

- Michael Steindorfer stayed for 3 months at Oracle Labs in Austria to study efficient data-structures and data-structure optimisations on the JVM.

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, 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, Pierre Guilloux.

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.

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. Faon involves Orange Labs, CEA-LETI, University of South Brittany (Lab-STICC laboratory) and Univ. Rennes I (Foton laboratory and CAIRNteam). CAIRNdeveloped a high-rate architecture at the receiver side. Specific receiver algorithms (synchronization and equalization) and FPGA implementation are the key issues that were addressed. This project ended in 2015.

8.2.3. ANR Ingénérie Numérique et Sécurité - ARDyT (2011-2016)

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.

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

Participants: Emmanuel Casseau, Steven Derrien, 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 was 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. This project ended in 2015.

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

Participants: Olivier Sentieys, 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 were 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 reduces 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 guarantees and validates the numerical behavior of the resulting implementation. The proposed infrastructure was validated on two real applications provided by the industrial partners. For more details see http://defis.lip6.fr. This project ended in 2015.

8.2.6. Labex CominLabs - BoWI (2012-2016)

Participants: Olivier Sentieys, Arnaud Carer.

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, IRISA Granit (Lannion), IETR (Rennes), and Lab-STICC (Brest, Lorient, Vannes). For more details see http://www.bowi.cominlabs.ueb.eu/fr.

8.2.7. 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. The 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 photonics layer suitable for a flexible and energy efficient high-speed optical network on chip (ONoC).

8.2.8. Labex CominLabs - RELIASIC (2014-2018)

Participants: Emmanuel Casseau, Arnaud Tisserand.

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.

8.2.9. 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, Daniel Chillet, Philippe Quémerais, Christophe Huriaux.

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 defined and developed an energy-efficient yet programmable heterogeneous manycore platform with self-adaptive capabilities. The manycore is 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 raised 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. This project ended in 2015.

8.3.2. FP7 ALMA

Participants: Steven Derrien, 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 aimed 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 was a fundamental step forward in the necessary introduction of novel computing paradigms and methodologies. This project ended in 2015.

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 (United States) - Department of Electrical and Computer Engineering - Prof. Russel Tessier and Prof. Maciej Ciesielski

Start year: 2014

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

Rapid evolutions of applications and standards require frequent in-the-field system modifications and thus strengthens 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

8.4.2.1.1. LRS

Title: Loop unRolling Stones: compiling in the polyhedral model

International Partner (Institution - Laboratory - Researcher):

Colorado State University (United States) - Department of Computer Science - Prof. Sanjay Rajopadhye

8.4.2.1.2. DAVIAP

Title: From DAtaflow-based VIdeo Appications to embedded multicore Platforms

International Partner (Institution - Laboratory - Researcher):

Tampere University of Technology (Finland) - Department of Pervasive Computing - Prof. Jarmo Takala

8.4.2.1.3. HARAMCOP

Title: Hardware accelerators modeling using constraint-based programming

International Partner (Institution - Laboratory - Researcher):

Lund University (Sweden) - Department of Computer Science - Prof. Krzysztof Kuchcinski

8.4.2.1.4. SPINACH

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

International Partner (Institution - Laboratory - Researcher):

University College Cork (Ireland) - Department of Electrical and Electronic Engineering - 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.

8.4.2.2. Informal International Partners

Imec (Belgium), Optimization of embedded systems using fixed-point arithmetic, fault-tolerant computing architectures.

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.

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.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Prof. Liam Marnane, Dept. of Electrical and Electronic Engineering, University College, Cork, Ireland, for two weeks in October. This visit was founded by ENSSAT.

Prof. Emanuel Popovici, Dept. of Electrical and Electronic Engineering, University College, Cork, Ireland, for two weeks in July. This visit was founded by ENSSAT.

Dr. Michele Magno, Integrated Systems Laboratory, ETH Zurich, Switzerland, for two weeks in June. This visit was founded by ENSSAT.

Prof. Guy Lemieux, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada, for two weeks in December. This visit was founded by HARDIESSE Inria Associate Team.

Prof. Russel Tessier, University of Massachusetts, Amherst, US, for one week in December. This visit was founded by HARDIESSE Inria Associate Team.

Porf. Renato J. Cintra, TDepartment of Statistics, Universidade Federal de Pernambuco, Recife, Brazil, for six months from January 2015.

8.5.1.1. Internships

Minh Thanh Cong, Master ICT, University of Science and Technology of Hanoi, Vietnam, from Apr 2015 until Sep 2015.

Soumitr Dubey, B.Tech./M.Sc. in Electronics and Communication, Indian Institute of Technology (IIT) Hyderabad, India, from May 2015 until Jul 2015.

Chi Dinh Ma, Master ICT, University of Science and Technology of Hanoi, Vietnam, from Apr 2015 until Sep 2015.

Prannoy Pilligundla, B.Eng. Electronics & Instrumentation Engineering, Birla Institute of Technology & Science, Pilani, India, from May 2015 until Jul 2015.

Madhav Singh, B.Tech. in Electrical Engineering, Indian Institute of Technology (IIT) Patna, India, from May 2015 until Jul 2015.

8.5.2. Visits to International Teams

Simon Rockiki visited University of Massachusetts, Amherst, US, for 6 months from January to July 2015. This visit was founded by HARDIESSE Inria Associate Team.

CAMUS Team

9. Partnerships and Cooperations

9.1. 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.

9.2. International Initiatives

9.2.1. Inria International Partners

9.2.1.1. 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
- Ohio State University, Colombus, USA
- Louisiana State University, Baton Rouge, USA
- Indian Institute of Science (IIIS) Bangalore, India
- University of Delaware, DE, USA

9.3. International Research Visitors

9.3.1. Visits of International Scientists

Professor P. Sadayappan from Ohio State University, USA, has been visiting the CAMUS team from November the 4th to November the 7th. He took part of Aravind Sukumaran-Rajam's PhD jury as a reviewer and made several presentations of his research work.

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

COMPSYS Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. 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 in 2013 a thematic quarter on compilation (http://labexcompilation.ens-lyon.fr). A new thematic quarter on high performance computing (HPC) is in preparation for 2016, initiated by Violaine Louvet (Institute Camille Jordan), with the participation of the LIP teams Aric, Avalon, Compsys, and Roma. It will include, in particular, an inter-disciplinary spring school, following the polyhedral school organized in 2013, connecting mathematics (HPC numerical analysis) and computer science (polyhedral optimizations for HPC).

Alain Darte, Alexandre Isoard, and Tomofumi Yuki have also regular exchanges with Violaine Louvet and Thierry Dumont on tiling code optimizations, advising (in an informal way) some of their students during their internships, for implementations on multicore machines and GPUs.

9.1.2. Collaboration with the Verimag lab

Laure Gonnord, who did her PhD in abstract interpretation at Verimag, re-activated her connection with this group, in particular with N. Halbwachs and D. Monniaux. This led to several joint results, exposed in Sections 7.3 and 7.4 . The theme of termination through affine ranking functions was first brought to the attention of Compsys when studying loop transformations for HLS, in the context of the S2S4HLS project with STMicroelectronics. The techniques of Compsys [15] were then extended by Laure Gonnord with D. Monniaux. Conversely, the idea of using Handelman and Schweighofer's theorems to deal with polynomial constraints, as exploited in Section 7.11), was first suggested by D. Monniaux through discussions with Paul Feautrier and some visits at ENS-Lyon.

9.1.3. "PEPS local" with the MMI

Alain Darte and Laure Gonnord participated to the creation of EMI (Education, Musique et Informatique), an educative inter-disciplinary project ("PEPS de site", coordinated by Natacha Portier, from the MC2 team at LIP, and Yann Orlarey from the Grame laboratory) concerning an experience of musical programming with Faust (a functional audio stream language, with its compiler), in the context of the MMI (Maison des mathématiques et de l'informatique), a place for dissemination.

9.2. National Initiatives

9.2.1. French Compiler Community

In 2010, Laure Gonnord and Fabrice Rastello created the french community of compilation, which had no organized venue in the past. All groups with activities related to compilation were contacted and the first "compilation day" was organized in Lyon.This effort has been quickly a success: the community (http://compilfr.ens-lyon.fr/) is now well identified and 3-days workshops now occur at least once a year (the 10th event has been organized in Sep. 2015). The community is animated by Laure Gonnord and Fabrice Rastello since 2010, and now also by Florian Brandner (ex-Compsys too). Alain Darte, Alexandre Isoard, and Tomofumi Yuki participated to the 10th edition, with talks on "Static Analysis of OpenStream Programs", "Liveness Analysis in the Polyhedral Model", and "PolyApps: Case Study of Polyhedral Compilers using Real Applications" respectively.

Recognized as a sub-group of the CNRS GDR GPL (Software Engineering and Programming), the community is also in charge, since 2014, of organizing one day of the research school "Ecole des jeunes chercheurs en Algorithmique et Programmation" (EJCP). Tomofumi Yuki, in this context, gave a one-day lecture at the 2015 edition.

9.2.2. Collaboration with Parkas group, in Paris

Alain Darte and Paul Feautrier have regular meetings with Albert Cohen, from the Parkas team at ENS Paris. The current discussions are mostly related to the analysis and compilation of the OpenStream language developed by Parkas, a research topic that started though the ManycoreLabs project (see Section 8.1). The results of Sections 7.10 and 7.11 are related to this collaboration.

9.2.3. Collaboration with Cairn group, in Rennes

Tomofumi Yuki continues to work with the Cairn group through regular meetings and occasional visits. The topic of the collaboration is in applying compiler techniques for hardware design using high-level synthesis. Section 7.14 presents the results through this collaboration.

9.2.4. Collaboration with Camus group, in Strasbourg

Paul Feautrier and Tomofumi Yuki have an ongoing cooperation with Alain Ketterlin and Eric Violard (Camus group, Strasbourg) on several subjects connected to the analysis and transformations of X10 programs (see Section 7.8).

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

Compsys participated to a H2020 proposal (project Verde) on the convergence of compiler tools for hardware accelerators on one side (HLS tools) and programmable accelerators (multicores, GPUs) on the other side. But the project was not selected.

9.3.2. Collaborations with Major European Organizations

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 9.4.2.2), 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, was co-chaired by Alain Darte (see http://impact.gforge.inria.fr/impact2015/), while the 6h edition, IMPACT'16, was co-chaired by Tomofumi Yuki (see http://impact.gforge.inria.fr/impact2016/).

9.4. International Initiatives

9.4.1. Inria Associate Teams not Involved in an Inria International Labs

Laure Gonnord and Maroua Maleej are involved in the PROSPIEL Associate Team (Inria/Brazil, https://team.inria.fr/alf/prospiel/), led by Sylvain Collange (Inria Alf), in a collaboration with Fernando Pereira's group in UFMG (Brazil). The PROSPIEL project aims at optimizing parallel applications for high performance on new throughput-oriented architectures: GPUs and many-core processors. Specifically, Laure Gonnord and Maroua Maalej are in charge of designing static analyses for GPUs. Maroua Maleej visited the group of Fernando Pereira in Aug. 2015.

9.4.2. Inria International Partners

9.4.2.1. Declared Inria International Partners

- Christophe Alias is co-adviser, with Sanjay Rajopadhye from Colorado State University (USA), of the PhD thesis of Guillaume Iooss. The results described in Section 7.6 are part of this collaboration.
- Tomofumi Yuki, who did his PhD with Sanjay Rajopadhye, then a post-doc in the Cairn team in Rennes, continues his collaboration with these two groups, as the results described in Section 7.14 illustrate. He participates regularly, over the net, to the reading group "Melange" of S. Rajodapdhye's group, with CSU students.
- Laure Gonnord and Maroua Maleej have a regular collaboration with Fernando Magno Quintao Pereira from the University of Mineas Gerais (Brazil). The results described in Section 7.2 are part of this collaboration. In Jan.-Feb. 2015, Compsys hosted Fernando Pereira, as a visiting professor.

9.4.2.2. 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 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 was program co-chair and co-organizer for the past edition, in Amsterdam (2015), while Tomofumi Yuki is program co-chair and co-organizer of the next one, in Prague (2016).

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/). A second polyhedral school, more open, because involving themes and researchers from numerical analysis (users of HPC), will be organized in 2016.

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. Tomofumi Yuki is involved in the development of PolyBench (http://sourceforge.net/projects/polybench), a suite of kernels used for illustrating polyhedral optimizations. He is also developing PolyApps, a set of larger applications to evaluate the gap between kernels and "real" applications, see more details in Section 7.15 .

9.5. International Research Visitors

9.5.1. Visits of International Scientists

9.5.1.1. Invited Professors

- Fernando M. Pereira was invited in Jan. 2015 to work with Maroua Maleej and Laure Gonnord on static analyses for pointers.

9.5.1.2. Internships

- Tristan Dubois, M1 student from Lyon 1 University, worked for 6 weeks in January-February 2015, on pointer arithmetic in LLVM, supervised by Laure Gonnord.
- Marc Vincenti, M1 student from Lyon 1 University, worked for 6 weeks in January-February 2015, on comparison of termination benchmarks, in the context of the Artefact Evaluation of the PLDI'15 publication [7], whose results are described in Section 7.4 .
- Adilla Susungi, a M2 student from Strasbourg University, worked, from March 2015 to July 2015, on the compilation of streaming applications on multi-GPUs, supervised by Christophe Alias. Her internship was funded by Inria.

9.5.2. Visits to International Teams

Paul Feautrier has been invited by the University of Passau (Bavaria) in the team of Prof. Christian Lengauer, where he has given a seminar “Toward a Polynomial Model” (September 2015) and held scientific discussions with Armin Groesslinger and other members of the team.

CORSE Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. HEAVEN Persyval Project

- Title: HEterogenous Architectures: Versatile Exploitation and programiNg
- HEAVEN leaders: François Broquedis, Olivier Muller[TIMA lab]
- Corse participants: François Broquedis, Frédéric Desprez, Georgios Christodoulis
- Computer architectures are getting more and more complex, exposing massive parallelism, hierarchically-organized memories and heterogeneous processing units. Such architectures are extremely difficult to program as they most of the time make application programmers choose between portability and performance.

  While standard programming environments like OpenMP are currently evolving to support the execution of applications on different kinds of processing units, such approaches suffer from two main issues. First, to exploit heterogeneous processing units from the application level, programmers need to explicitly deal with hardware-specific low-level mechanisms, such as the memory transfers between the host memory and private memories of a co-processor for example. Second, as the evolution of programming environments towards heterogeneous programming mainly focuses on CPU/GPU platforms, some hardware accelerators are still difficult to exploit from a general-purpose parallel application.

  FPGA is one of them. Unlike CPUs and GPUs, this hardware accelerator can be configured to fit the application needs. It contains arrays of programmable logic blocks that can be wired together to build a circuit specialized for the targeted application. For example, FPGAs can be configured to accelerate portions of code that are known to perform badly on CPUs or GPUs. The energy efficiency of FPGAs is also one of the main assets of this kind of accelerators compared to GPUs, which encourages the scientific community to consider FPGAs as one of the building blocks of large scale low-power heterogeneous multicore platforms.

  However, only a fraction of the community considers programming FPGAs for now, as configurations must be designed using low-level description languages such as VHDL that application programmers are not experienced with.

  The main objective of this project is to improve the accessibility of heterogeneous architectures containing FPGA accelerators to parallel application programmers. The proposed project focuses on three main aspects:

  – Portability: we don't want application programmers to redesign their applications completely to benefit from FPGA devices. This means extending standard parallel programming environments like OpenMP to support FPGA. Improving application portability also means leveraging most of the hardware-specific low-level mechanisms at the runtime system level ;

  – Performance: we want our solution to be flexible enough to get the most out of any heterogeneous platforms containing FPGA devices depending on specific performance needs, like computation throughput or energy consumption for example ;

  – Experiments: Experimenting with FPGA accelerators on real-life scientific applications is also a key element of our project proposal. In particular, the solutions developed in this project will allow comparisons between architectures on real-life applications from different domains like signal processing and computational finance.

Efficient programming and exploitation of heterogeneous architectures implies the development of methods and tools for system design, embedded or not. The HEAVEN project proposal fits in the PCS research action of the PERSYVAL-lab. The PhD of Georgios Christodoulis is funded by this project.

8.1.2. HPES Persyval Project

- Title: High Performance Embedded Systems
- HPES leader: Henri-Pierre Charles [CEA List, CRI PILSI]
- HPES participants: Suzane Lesecq [CEA Leti], Laurent Fesquet [TIMA Lab], Stéphane Mancini [TIMA Lab], Eric Ruten [Inria/CtrlA], Nicolas Marchand [Gipsa Lab], Bogdan Robu [Gipsa Lab]
- Corse participants: Naweiluo Zhou [PhD Persyval], Fabrice Rastello, Jean-François Méhaut
- The computing area has been recently deeply modified by the emergence of the so-called multicore processor. Within the same chip, several computing units are implemented. This architectural concept allows meeting the performance requirements under stringent energy consumption constraints. Multicores are used for laptops, Graphical Processor Units (GPU), High Performance Computing (HPC) platforms, but also for embedded systems su ch as mobile phones. Moreover, low-power high performance multicores developed for embedded systems will be soon used in data centers for HPC. This raises new scientific challenges to architecture, systems and application designers that have face massively parallel computing platforms.

  The number of cores on a chip is increasing quickly. At the same time, the memory bandwidth is increasing too slowly to ensure the performance such multicore platforms should attain. This phenomenon is known as “Memory Wall” and at the moment no efficient solution to exceed this limitation exists. With the increase in the number of cores, cache coherency is becoming as well a tremendous challenge.

  Power consumption is also a huge challenge as it imposes strong constraints on the computing platform, whatever the application domain. The first machine ranked in the Green500 has an energy performance ratio of 2 Gflops per watt. This ratio has to be improved by 30 when exascale computing is considered. The multi-core processor might help to improve this ratio; however, the software stack should as well evolve to boost this improvement.

8.2. National Initiatives

8.2.1. IPL Multicore

- Title: Large scale multicore virtualization for performance scaling and portability
- Multicore leader: Gilles Muller
- CORSE participants: Fabrice Rastello
- Multicore processors are becoming the norm in most computing systems. However supporting them in an efficient way is still a scientific challenge. This large-scale initiative introduces a novel approach based on virtualization and dynamicity, in order to mask hardware heterogeneity, and to let performance scale with the number and nature of cores. It 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. We hope delivering a solution for compute-intensive applications running on general-purpose standard computers. Research directions are: (1) Memory management and scheduling; (2) Garbage collection; (3) Improving data locality; (4) Dynamic parallelization; (5) Fast execution of Sequential Sections; (6) Dynamic Code Generation; (7) Dynamic Binary Rewriting for Performance Portability; (8) Virtualization of floating-point computation; (9) Convergence between VMKit and StarPU

8.2.2. IPL C2S@Exa

- Title: Computer and Computational Sciences at Exascale
- C2S@Exa leader: Stéphane Lanteri
- Corse participants: François Broquedis, Frédéric Desprez, Jean-François Méhaut
- The C2S@Exa Inria large-scale initiative is concerned with the development of numerical modeling methodologies that fully exploit the processing capabilities of modern massively parallel architectures in the context of a number of selected applications related to important scientific and technological challenges for the quality and the security of life in our society. At the current state of the art in technologies and methodologies, a multidisciplinary approach is required to overcome the challenges raised by the development of highly scalable numerical simulation software that can exploit computing platforms offering several hundreds of thousands of cores. Hence, the main objective of the C2S@Exa Inria large-scale initiative is the establishment of a continuum of expertise in the computer science and numerical mathematics domains, by gathering researchers from Inria project-teams whose research and development activities are tightly linked to high performance computing issues in these domains. More precisely, this collaborative effort involves computer scientists that are experts of programming models, environments and tools for harnessing massively parallel systems, algorithmists that propose algorithms and contribute to generic libraries and core solvers in order to take benefit from all the parallelism levels with the main goal of optimal scaling on very large numbers of computing entities and, numerical mathematicians that are studying numerical schemes and scalable solvers for systems of partial differential equations in view of the simulation of very large-scale problems.

8.2.3. PIA ELCI

- Title: Environnement logiciel pour le calcul intensif
- ELCI leader: Corinne Marchand (BULL SAS)
- Corse participants: François Broquedis, Philippe Virouleau
- Duration: from Sept. 2014 to Sept. 2017
- The ELCI project main goal is to develop a highly-scalable new software stack to tackle high-end supercomputers, from numerical solvers to programming environments and runtime systems. In particular, the CORSE team is studying the scalability of OpenMP runtime systems on large scale shared memory machines through the PhD of Philippe Virouleau, co-advised by researchers from the CORSE and AVALON Inria teams. This work intends to propose new approaches based on a compiler/runtime cooperation to improve the execution of scientific task-based programs on NUMA platforms. The PhD of Philippe Virouleau is funded by this project.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

8.3.1.1. Mont-Blanc

Title: Mont-Blanc (European scalable and power efficient HPC platform based on low-power embedded technology)

Program FP7

Duration: 01/10/2011 - 30/06/2015

Coordinator: Barcelona Supercomputing Center (BSC)

Mont-Blanc consortium: BSC, Arm, Bull, CNRS, CEA Leti, Juelich, LRZ, Genci, Cineca, Univ. Cantabria

Mont-Blanc website: http://www.montblanc-project.eu/

Corse contact: Jean-François Méhaut

Corse participants: Brice Videau, Kevin Pouget

There is a continued need for higher compute performance: scientific grand challenges, engineering, geophysics, bioinformatics, etc. However, energy is increasingly becoming one of the most expensive resources and the dominant cost item for running a large supercomputing facility. In fact the total energy cost of a few years of operation can almost equal the cost of the hardware infrastructure. Energy efficiency is already a primary concern for the design of any computer system and it is unanimously recognized that Exascale systems will be strongly constrained by power. The analysis of the performance of HPC systems since 1993 shows exponential improvements at the rate of one order of magnitude every 3 years: One petaflops was achieved in 2008, one exaflops is expected in 2020. Based on a 20 MW power budget, this requires an efficiency of 50 GFLOPS/Watt. However, the current leader in energy efficiency achieves only 1.7 GFLOPS / Watt. Thus, a 30x improvement is required. In this project, we believe that HPC systems developed from today's energy-efficient solutions used in embedded and mobile devices are the most likely to succeed. As of today, the CPUs of these devices are mostly designed by ARM. However, ARM processors have not been designed for HPC, and ARM chips have never been used in HPC systems before, leading to a number of significant challenges. The Mont-Blanc project has three objectives:

- To develop a fully functional energy-efficient HPC prototype using low-power commercially available embedded technology
- To design a next-generation HPC system together with a range of embedded technologies in order to overcome the limitations identified in the prototype system
- To develop a portfolio of exascale applications to be run on this new generation of HPC systems. This will produce a new type of computer architecture capable of setting future global HPC standards that will provide Exascale performance using 15 to 30 times less energy

8.3.1.2. Mont-Blanc2

Title: Mont-Blanc (European scalable and power efficient HPC platform based on low-power embedded technology)

Program FP7

Duration: 01/10/2013 - 30/09/2016

Coordinator: Barcelona Supercomputing Center (BSC)

Mont-Blanc consortium: BSC, Bull, Arm, Juelich, LRZ, USTUTT, Cineca, CNRS, Inria, CEA Leti, Univ. Bristol, Allinea

Corse contact: Jean-François Méhaut

Corse participants: Brice Videau, Kevin Pouget

The Mont-Blanc project aims to develop a European Exascale approach leveraging on commodity power-efficient embedded technologies. The project has developed a HPC system software stack on ARM, and is deployed the first integrated ARM-based HPC prototype by 2014, and is also working on a set of 11 scientific applications to be ported and tuned to the prototype system.

The rapid progress of Mont-Blanc towards defining a scalable power efficient Exascale platform has revealed a number of challenges and opportunities to broaden the scope of investigations and developments. Particularly, the growing interest of the HPC community in accessing the Mont-Blanc platform calls for increased efforts to setup a production-ready environment. The Mont-Blanc 2 proposal has 4 objectives:

1. To complement the effort on the Mont-Blanc system software stack, with emphasis on programmer tools (debugger, performance analysis), system resiliency (from applications to architecture support), and ARM 64-bit support
2. To produce a first definition of the Mont-Blanc Exascale architecture, exploring different alternatives for the compute node (from low-power mobile sockets to special-purpose high-end ARM chips), and its implications on the rest of the system

3. To track the evolution of ARM-based systems, deploying small cluster systems to test new processors that were not available for the original Mont-Blanc prototype (both mobile processors and ARM server chips)
4. To provide continued support for the Mont-Blanc consortium, namely operations of the original Mont-Blanc prototype, the new developer kit clusters and hands-on support for our application developers

Mont-Blanc 2 contributes to the development of extreme scale energy-efficient platforms, with potential for Exascale computing, addressing the challenges of massive parallelism, heterogeneous computing, and resiliency. Mont-Blanc 2 has great potential to create new market opportunities for successful EU technology, by placing embedded architectures in servers and HPC.

8.3.1.3. HPC4E

Title: HPC for Energy

Programm: H2020

Duration: 01/12/2015 - 30/11/2017

Coordinator: Barcelona Supercomputing Center (BSC)

European partners: Inria, Univ. Lancaster, Ciemat, Total, Repsol, Iberdrola

Brazilian partners: Coppe, LNCC, ITA, Petrobras, UFRGS, UFPE

Inria contact: Stephane Lanteri

Corse contact: Jean-François Méhaut

Corse participants: François Broquedis, Frédéric Desprez, Brice Videau

The main objective is to develop beyond-the-state-of-the-art high performance simulation tools that can help the energy industry to respond future energy demands and also to carbon-related environmental issues using the state-of-the-art HPC systems. HPC4E also aims at improving the usage of energy using HPC tools by acting at many levels of the energy chain for different energy sources. The project includes relevant energy industral partners from Brazil and EU, which will benefit from the project's results. They guarantee that TRL of the project technologies will be very high.

8.3.1.4. EoCoE

Title: Energy oriented Centre of Excellence for computer applications

Programm: H2020

Duration: 01/10/2015 - 30/11/2018

Coordinator: Commissariat à L'Energie Atomique et aux Energies Alternatives (CEA)

European partners: CEA, Juelich, MPG, Enea, Cerfacs, UNITN, Fraunhofer, Univ. Bath, CNR, Univ. Brussels, BSC

Inria contact: Michel Kern

Corse contact: Jean-François Méhaut

Corse participants: François Broquedis, Frédéric Desprez, Brice Videau

This projects establishes an Energy Oriented Centre of Excellence for computing applications, (EoCoE). EoCoE (pronounce "Echo") will use the prodigious potential offered by the ever-growing computing infrastructure to foster and accelerate the European transition to a reliable and low carbon energy supply. To achieve this goal, we believe that the present revolution in hardware technology calls for a similar paradigm change in the way application codes are designed. EoCoE will assist the energy transition via targeted support to four renewable energy pillars: Meteo, Materials, Water and Fusion, each with a heavy reliance on numerical modelling. These four pillars will be anchored within a strong transversal multidisciplinary basis providing high-end expertise in applied

mathematics and HPC. EoCoE is structured around a central Franco-German hub coordinating a pan-European network, gathering a total of 8 countries and 23 teams. Its partners are strongly engaged in both the HPC and energy fields; a prerequisite for the long-term sustainability of EoCoE and also ensuring that it is deeply integrated in the overall European strategy for HPC. The primary goal of EoCoE is to create a new, long lasting and sustainable community around computational energy science. At the same time, EoCoE is committed to deliver high-impact results within the first three years. It will resolve current bottlenecks in application codes, leading to new modelling capabilities and scientific advances among the four user communities; it will develop cutting-edge mathematical and numerical methods, and tools to foster the usage of Exascale computing. Dedicated services for laboratories and industries will be established to leverage this expertise and to foster an ecosystem around HPC for energy. EoCoE will give birth to new collaborations and working methods and will encourage widely spread best practices.

8.4. International Initiatives

8.4.1. Inria International Labs

- JLESC (Joint Laboratory on Exascale Computing)
  The CORSE team is involved in the JLESC with collaborations with UIUC (Sanjay Kalé) and BSC (Mont-Blanc projects). Kevin Pouget, Brice Videau and Jean-François Méhaut attended to the two JLESC workshops (Barcelona and Bonn) in 2015.
  - **Energy Efficiency and Load Balancing**
  - The power consumption of High Performance Computing (HPC) systems is an increasing concern as large-scale systems grow in size and, consequently, consume more energy. In response to this challenge, we propose new energy-aware load balancers that aim at reducing the energy consumption of parallel platforms running imbalanced scientific applications without degrading their performance. Our research explores dynamic load balancing, low power manycore platforms and DVFS techniques in order to reduce power consumption.
  - We propose the improvement of the performance and scalability of parallel seismic wave models through dynamic load balancing. These models suffer from load imbalance for two reasons. First, they add a specific numerical condition at the borders of the domain, in order to absorb the outgoing energy. The decomposition of the domain into a grid of subdomains, which are distributed among tasks, creates load differences between the tasks that simulate the borders and those responsible for the central subdomains. Second, the propagation of waves in the simulated area changes the workload on the subdomains on different time-steps. Therefore causing dynamic load imbalance. In order to evaluate the use of dynamic load balancing, we ported a seismic wave simulator to Adaptive MPI, to benefit from its load balancing framework. Our experimental results show that dynamic load balancers can adapt to load variations during the application's execution and improve performance by 36%.
  - we also focus on reducing the energy consumption of imbalanced applications through a combination of load balancing and Dynamic Voltage and Frequency Scaling (DVFS). Our strategy employs an Energy Daemon Tool to gather power information and a load balancing module that benefits from the load balancing framework available in the CHARM++ runtime system. We propose two variants of our energy-aware load balancer (ENERGYLB) to save energy on imbalanced workloads without considerably impacting the overall system performance. The first one, called Fine- Grained EnergyLB (FG-ENERGYLB), is suitable for plat- forms composed of few tens of cores that allow per-core DVFS. The second one, called Coarse-Grained EnergyLB (CG-ENERGLB) is suitable for current HPC platforms composed of several multi-core processors that feature per-chip DVFS.

- LIRIMA (IDASCO team)
  - The general objective of IDASCO project team is to develop models and tools that can be used to collect the huge amount of data produced by complex computational, biological, epidemiological or environmental systems, and extract knowledge from these data in order to better understand their structure and dynamics for decision making. From 2010 to 2015, the IDASCO activities were focused on the following main thematics : programming environments for parallel execution, parallel algorithms for datamining, social network analysis and trace mining. Some work on wireless sensor networks and geographic information systems with application to sustainable management of natural resources have also been developed. Ten PhD Theses were defended during this period with eight on them co-supervised. There were some industrial collaborations with a brewery company (SABC) on e-Learning platforms and with ORANGE Labs on online registration platforms. These collaborations were done in partnership of the ALOCO project team. The EPICAM project was also developed in partnership with MEDES France, Centre Pasteur Cameroun and the National Program for Fight against Tuberculosis.
  - Jean-François Méhaut is co-director with Maurice Tchuenté of the IDASCO team.
  - Thomas Messi Nguelé is currently preparing a PhD with the coadvising of Maurice Tchuenté. His research work is also part of the IDASCO team.
  - Ylies Falcone and Jean-François Méhaut spent two weeks in Cameroon (Yaoundé) in the context of LIRIMA and CETIC (African Center of Excellence for IT, http://www.cetic.cm/).

8.4.2. Inria Associate Teams not involved in an Inria International Labs

8.4.2.1. IOComplexity

Title: Automatic characterization of data movement complexity

International Partner (Institution - Laboratory - Researcher):

Ohio State University (United States) - P. Sadayappan

Start year: 2015

See also: https://team.inria.fr/corse/iocomplexity/

The goal of this project is to develop new techniques and tools for the automatic characterization of the data movement complexity of an application. The expected contributions are both theoretical and practical, with the ambition of providing a fully automated approach to I/O complexity characterization, in starking contrast with all known previous work that are stricly limited to pen-and-paper analysis.

I/O complexity becomes a critical factor due in large part to the increasing dominance of data movement over computation in energy consumption for current and emerging architectures. This project aims at enabling: 1. the selection of algorithms according to this new criteria (as opposed to the criteria on arithmetic complexity that has been used up to now); 2. the design of specific architectures in terms of cache size, memory bandwidth, GFlops etc. based on application-specific bounds on memory traffic; 3. higher quality feedback to the user, the compiler, or the run-time system about data traffic, a major performance and energy factor.

8.4.2.2. PROSPIEL

- Title: Profiling and specialization for locality
- International Partner (Institution - Laboratory - Researcher):

  Universidade Federal de Minas Gerais (Brazil) - Computer Science Department - Fernando Magno Quintão Pereira
- Start year: 2015

- See also: https://team.inria.fr/alf/prospiel/
- The PROSPIEL project aims at optimizing parallel applications for high performance on new throughput-oriented architectures: GPUs and many-core processors. Traditionally, code optimization is driven by a program analysis performed either statically at compile-time, or dynamically at run-time. Static program analysis is fully reliable but often over-conservative. Dynamic analysis provides more accurate data, but faces strong execution time constraints and does not provide any guarantee. By combining profiling-guided specialization of parallel programs with runtime checks for correctness, PROSPIEL seeks to capture the advantages of both static analysis and dynamic analysis. The project relies on the polytope model, a mathematical representation for parallel loops, as a theoretical foundation. It focuses on analyzing and optimizing performance aspects that become increasingly critical on modern parallel computer architectures: locality and regularity.

8.4.2.3. Exase

Title: Exascale Computing Scheduling Energy

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

Inria leader: Jean-Marc Vincent (Mescal)

Inria teams: Mescal, Moais, Corse

Corse participants: Jean-François Méhaut, François Broquedis, Frédéric Desprez

International Partner (Institution - Laboratory - Researcher):

Federal University of Rio Grande do Soul (UFRGS, Porto Alegre, Brazil) - Informatics Faculty - L. Schnoor, N. Maillard, P. Navaux

Pontifical University Minas (PUC Minas, Belo Horizonte, Brazil) - Computer Science faculty, Henrique Freitas

University of Sao Paulo (USP, Sao Paulo, Brazil), IME faculty, Alfredo Goldman

Start year: 2014

The main scientific goal of Exase for the three years is the development of state-of- the-art energy-aware scheduling algorithms for exascale systems. As previously stated, issues on energy are fundamental for next generation parallel platforms and all scheduling decisions must be aware of that. Another goal is the development of trace analysis techniques for the behavior analysis of schedulers and the applications running on exascale machines. We list below specific objectives for each development axis presented in the previous section. analysis.

- Fundamentals for the scaling of schedulers
- Design of schedulers for large-scale infrastructures
- Tools for the analysys of large scale schedulers

8.4.3. Participation In other International Programs

- LICIA
- HOSCAR
- EnergySFE (STIC Amsud)

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Thierry Jéron, Hervé Marchand, and Antoine Rollet visited Yliès Falcone during 1 week in January 2015.
- Ezio Bartocci (TU Vienna) visited Y. Falcone during two weeks in August 2015.
- Sylvain Hallé (University of Québec at Chicoutimi) visited Yliès Falcone during 1 week in December 2015.

8.5.2. Visits to International Teams

8.5.2.1. Research stays abroad

- Fabrice Rastello visited P. Sadayappan at Ohio State University two times one month (mai 2015 + September 2015) in the context of the INRIA Associate Team IOComplexity.
- Ylies Falcone visited the University of Illinois at Urbana Champaign (USA) from February to July 2015.
- Jean-François Méhaut visited M. Tchuenté at Yaoundé. (February 2015) in the context of LIRIMA (Idasco team).
- Jean-François Méhaut visited P. Navaux at UFRGS (October 2015) in the context of LICIA and the Inria associated team Exase.
- Jean-François Méhaut visited M. Castro and L. Pilla at UFSC (October 2015) in the context of the Stic Amsud EnergySFE project.

DREAMPAL Project-Team

8. Partnerships and Cooperations

8.1. International Initiatives

8.1.1. Inria International Partners

8.1.1.1. Informal International Partners

We have a long-lasting collaboration with the universities of Illinois at Urbana Champaign (USA) and Iasi (Romania), which has been particularly fruitful in 2015 with 5 co-signed articles published or accepted for publication in high-quality journals.

POSTALE Team

8. Partnerships and Cooperations

8.1. 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.
- **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, Konstantin Petrov.

8.2. International Initiatives

8.2.1. Inria Associate Teams not involved in an Inria International Labs

8.2.1.1. R-LAS

Title: Randomized Linear Algebra Software

International Partner (Institution - Laboratory - Researcher):

University of Tennessee, Knoxville (United States) - Innovative Computing Laboratory (ICL) - Jack Dongarra

Start year: 2014

See also: https://www.lri.fr/~baboulin/r-las.html

The objective of the associate team between Inria and University of Tennessee is to develop a class of fast algorithms and software based on randomization to enhance linear algebra calculations in high-performance computing (HPC) applications. The first application will focus on FFT-like randomization techniques to avoid pivoting in dense and sparse matrix factorizations and thus removing the communication cost due to pivoting. The second application is related to the computation of statistical condition estimates for linear algebra problems in order to assess the numerical quality of solutions computed by HPC applications. The targeted architectures are large scale multicore systems with accelerators. The ultimate goal of the project is to make the randomized solvers designed by the associate team accessible to end-users thanks to a public domain software library.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

- Masha Sosonkina, Old Dominion University, USA.
- Hartwig Anzt, University of Tennessee, USA.
- Nick Higham, University of Manchester, UK.
- Jean-Luc Gaudiot, UC Irvine, USA.

8.3.2. Visits to International Teams

8.3.2.1. Research stays abroad

- Marc Baboulin,
  - Invitation at Old Dominion University, Norfolk, USA, (October 2015)
  - Invitation at National Institute of Informatics, Tokyo, Japan (August 2015)
  - Invitation at Académie des Sciences de Prague, République Tchèque (June 2015)
  - Invitation at Inria Bordeaux- équipe Hiepacs (March 2015)

TASC Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. SmartCat

Participants: Eric Monfroy, Charlotte Truchet.

Title: Online optimization for chemical reactions.

Others partners: CEISAM.

The SmartCat project, started in 2015 on regional fundings, aims at developing an intelligent automatised tool for online chemistry. Contrarily to the traditional batch chemistry, where reactants are mixed in a glass, online chemistry consists in having a flow of reactants in a tube, possibly passing through ovens are pressure control mechanisms. This way, the reaction happens continuously and it can produce much more products within a system of reasonable size. SmartCat integrates a controller for which intelligent tools need to be developed. These tools will analyse the product of the reaction and adapt the conditions (stoechiometry, pressure, temperature, catalysis) in order to optimise the yield. TASC contributes to this project by developing these methods, based on local search techniques.

9.1.2. 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.

9.1.3. Search

Participants: Nicolas Galvez, Éric Monfroy, Frédéric Saubion.

Title: Hybrid Algorithms for Search Based Software Engineering.

Others partners: LERIA.

Topic: hybrid algorithms for search.

9.2. National Initiatives

9.2.1. 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).

9.2.2. 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). 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.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

Within the context of the First Future and Emerging Technologies (FET) Proactive projects under Horizon 2020 Framework Programme the GRACeFUL project started this year. From an application point of view the project develops scalable rapid assessment tools for collective policy making in global systems, and test these on climate-resilient urban design. From a technical point of view it provides domain specific languages that are embedded in functional programming and constraint programming languages. Within the project TASC is responsable for the constraint part.

9.4. International Initiatives

9.4.1. Inria Associate Teams not involved in an Inria International Labs

9.4.1.1. TASCMELB

Title: Synergy between Filtering and Explanations for Scheduling and Placement Constraints

International Partner (Institution - Laboratory - Researcher):

NICTA (Australia) - Optimisation Research Group (Optimisation) - Pascal van Hentenryck

Start year: 2014

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.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- One visit regarding time-series constraints of Mats Carlsson, Andreina Francisco RodriguezHelmut Simonis, Pierre Flener and Justin Pearson in Nantes.
- One visit in Nantes of Andreas Schutt from NICTA in the context of the TASCMELB associated team.

9.5.1.1. Internships

- Master thesis : Ekaterina Arafailova (February-June 2015), *reformulation of automata with accumulators as linear programs*.
- Master thesis : Julien Fradin (February-June 2015), *extensions to the GHOST library*.
- Master thesis : Adrien Bodineau (January-April 2015), *extensions to the GHOST library*.
- Internship : Guillaume Legru (April-May 2015), *IA for combat games*.

9.5.2. Visits to International Teams

Three visits to Insight Cork, Centre for Data Analytics and to Uppsala University were done to continue the work with Helmut Simonis, Pierre Flener and Mats Carlsson on time-series constraints. An extra visit took place in Nantes. Two visits of Nicolas Beldiceanu and Charlotte Truchet in Melbourne to Peter Stuckey and Marck Wallace took place.

AOSTE Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. CIM PACA Design Platform

Participant: Robert de Simone.

The objective of this platform, run by a French association under the same name, is to provide mutualized equipments and tools for the design of embedded connected objects, and in our case mostly EDA software for hardware and SoC synthesis at high-level. We collaborate to the definition of the user needs and the choice of purchases, mostly to promote the construction of collaborative R&D projects using those resources. ANR HOPE project is a good example of such project.

CIM PACA also runs the eSAME yearly forum, a meeting point for various partners in the field aroud Sophia-Antipolis, with our active contribution. Further moves towards embedded software and IoT design form the upcoming roadmap.

9.2. National Initiatives

9.2.1. ANR

9.2.1.1. 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 eSAME'2014, reflecting Ameni Khecharem ongoing PhD work.

9.2.1.2. 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).

As part of the project dissemination purpose we organize a community-building international workshop [47], whose third edition gathered a growing number of participants.

9.2.2. FUI

9.2.2.1. 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).

9.2.2.2. FUI CLISTINE

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

This project was started in Oct 2013, and provides 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 (known as "Dwarfs" in the literature), to provide benchmarks and evaluate the platform design options.

9.2.2.3. FUI Waruna

Participants: Liliana Cucu, Adriana Gogonel, Walid Talaboulma, Dorin Maxim.

This recent project was started in September 2015. It targets the creation of a framework allowing to connect different existing methods while enriching the description with Waruna results. This framework allows timing analyses for different application domains like avionics, railways, medical, aerospace, automotive, etc.

9.2.3. Investissements d'Avenir

9.2.3.1. DEPARTS

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Walid Talaboulma.

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.

9.2.3.2. CLARITY

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

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 the project is to develop and promote an open-source version of the ARCADIA Melody system design environment from Thales, renamed CAPPELLA for that purpose.
Our technical contributions to the project achievement are described in subsection 7.2 .

9.2.3.3. 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 the objective of the project is to study the relevance of Kalray-style MPPA processor array for real-time computation in the avionic domain (with partners such as Airbus for instance). The post-doc of Mihail Asavoae and the PhD of Walid Talaboulma are funded on this contract.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. FP7 PROXIMA

Participants: Liliana Cucu, Adriana Gogonel, Walid Talaboulma, Dorin Maxim, Cristian Maxim.

PROXIMA is a Integrated Project (IP) of the Seventh framework programme for research and technological development (FP7). The PROXIMA project provides industry ready software timing analysis using probabilistic analysis for many-core and multi-core critical real-time embedded systems and will enable cost-effective verification of software timing analysis including worst case execution time. Our technical results in this project are described in 7.13 .

9.3.2. Collaborations in European Programs, except FP7 & H2020

9.3.2.1. ITEA3 Assume

Project title: Affordable Safe And Secure Mobility Evolution

Duration: Oct. 2015 - Sept. 2018

Coordinator: Daimler AG (Germany)

Other partners: Airbus, Thales, Safran, Ansys/Esterel Technologies, Kalray, Sagem, UPMC, ENS Ulm, Inria (France). AbsInt, BTC, FZI. Kalrsruhe IT, Kiel U. Offis, Bosch, TU Muenchen (Germany), NXP, Recore, VDL, Verum, TU Eindhoven, U. Twente (Netherlands), Arcelik, Ericsson, Ford, Havelsan, KocSistem, Unit, Koc University (Turkey), Arcticus, FindOut, Scania, KTH, Malardalen U. (Sweden)

Abstract: ASSUME aims at providing a seamless engineering methodology for affordable, safe multi-core development that allows industry to deliver new trustworthy functions at competitive prices. The project started on September 1st, 2015, and the kick-off meeting was held on October 1-2. The project coordinator is Daimler AG. The expected constributions of the Aoste team-project include the improvement of the Lopht tool, with the definition of a back-end targeting the Kalray MPPA256 many-core, and the proof of its scheduling algorithms.

9.4. International Initiatives

9.4.1. Inria International Labs

LIAMA

Associate Team involved in the International Lab:

9.4.1.1. FM4CPS

Title: Formal Models and tools for Cyber-Physical Systems

International Partner (Institution - Laboratory - Researcher):

ECNU (China) - Artificial Intelligence Lab - Jifeng He

Start year: 2015

See also: https://project.inria.fr/fm4cps/

The FM4CPS Associated team is tighly linked to the SACCADES LIAMA project. It is also involved in the International Key Laboratory on Trustworthy Computing by ECNU Shanghai on the Chinese side.

FM4CPS addresses several facets of Formal Model-Driven Engineering for Cyber-Physical Systems and Internet of Things. The design of such large heterogeneous systems calls for hybrid modeling, and the combination of classes of models, most previously well-established in their own restricted area: Formal Models of Computations drawn from Concurrency Theory for the "cyber" discrete processors, timed extension and continuous behaviors for physical environments, requirement models and user constraints extended to non-functional aspects, new challenges for designing and analyzing large and highly dynamic communicating software entities. Orchestration and comparison of models, with their expressive power vs. their decidable aspects, shall be considered with the point of view of hybrid/heterogeneous modeling here. Main aspects are the various timing or quantitative structure extensions relying for instance on a hybrid logical clock model for the orchestration of underlying components.

The associated team aims at various level of research, from formal models, semantics, or complexity, to experimental tools development. This will start for example on one side with building a formal orchestration model for CPSs, based on an hybrid clock model that combine discrete and physical time, synchronous and asynchronous computations or communications. Another goal will be the study of expressiveness and decidability for CPS, based on dedicated sub-families of well-structured push-down systems, addressing both unbounded communication and time-sensitive models.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

9.5.1.1. Invited Professor

Qingguo XU

Date: July 2014 to June 2015

Institution: Shanghai University (China)

9.5.1.2. Internships

Nieto Luis Agustin

Date: Sep 2015 - Feb 2016

Institution: Universidad de Buenos Aires (Argentina)

9.5.2. Visits to International Teams

9.5.2.1. 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 Sakka Abid, Hugues Evrard, Frédéric Lang, Gwen Salaün [correspondent].

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 § 6.5.2) 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 assisted another LIG team, IIHM, in specifying human-machine interfaces formally using the LNT language and in verifying them using CADP (see § 6.5.6).

8.1.2. Competitivity Clusters

8.1.2.1. Bluesky for I-Automation

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

Bluesky for I-Automation is a project funded by the FUI (*Fonds Unique Interministériel*) within the *Pôle de Compétitivité* Minalogic. The project, led by Crouzet Automatismes (Valence), involves the SMEs (*Small and Medium Enterprises*) 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 and was extended for nine month until June 2016. The main contributions of CONVECS to Bluesky (see § 6.1.5 and § 6.5.3) 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 2015 with the following Inria project-teams:

- PAREO (Inria Nancy — Grand Est): Pierre-Etienne Moreau

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),
- Noël De Palma and Fabienne Boyer (LIG, Grenoble),
- Xavier Etchevers (Orange Labs, Meylan),
- Matthias Güdemann (Systerel, Aix-en-Provence),
- 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, José 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, and has been extended for five months until February 29, 2016. 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 § 6.5.4).

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]. H. Garavel and R. Mateescu are members of the FMICS board, H. Garavel being in charge of dissemination actions.

8.3. International Initiatives

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

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

8.3.1. Other International Collaborations

In 2015, we had scientific relations with several universities abroad, including:

- CWI, The Netherlands (Jurgen Vinju and Paul Klint),
- University of Málaga, Spain (F. Duran and C. Canal),
- University of Colorado, USA (Fabio Somenzi), and
- University of Utah, USA (Chris Myers and Zhen Zhang).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- The annual CONVECS seminar was held in Charavines (France) on May 27–29, 2015. The following invited scientists attended the seminar:
  - Eric Jenn (IRT Saint-Exupéry / Thales Avionics) gave on May 27, 2015 a talk entitled "*The INGEQUIP Project and the TwIRTee demonstrator*".
  - Alexandre Hamez (IRT Saint-Exupéry) gave on May 29, 2015 a talk entitled "*CAE-SAR.SDD*".
- Chris Myers (University of Utah, USA) visited us from June 8–12, 2015. He gave a talk entitled "*An Integrated Verification Architecture*" on June 9, 2015.
- Hernan Ponce de Leon (Aalto University, Finland) visited us from June 29 to July 1, 2015. He gave a talk entitled "*Unfolding Based Testing for Multithreaded Programs*" on June 29, 2015.

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 7.2 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 [32]. 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 – November 2015

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 – May 2016

Coordinator: EDF (France)

[0] http://www.s3pm.cominlabs.ueb.eu/

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 Research Visitors

7.4.1. Research stays abroad

Ayman Aljarbouh has visited for two months Walid Taha's team (http://www.hh.se/english/research/professors/walidmohamedtaha.10235.html) at Halmstad university in Sweden. He has been working on the implementation in the Accumen language of the regularization techniques he is developing in his PhD work.

MUTANT Project-Team

8. Partnerships and Cooperations

8.1. National Projects

8.1.1. ANR INEDIT Project

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 - November 2015

Coordinator: IRCAM (France)

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

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

8.1.2. ANR EFFICACe Project

Florent Jacquemard participates actively in the Efficace ANR Project. This project explores the relations between computation, time and interactions in computer-aided music composition, using OpenMusic and other technologies developed at IRCAM and at CNMAT (UC Berkeley). The participant consider computer-aided composition out of its traditional "offline" paradigm, and try to integrate compositional processes in structured interactions with their external context. These interactions can take place during executions or performances, or at the early compositional stages (in the processes that lead to the creation of musical material). There are particular focus on a number of specific directions, such as the reactive approaches for computer-aided composition, the notion of dynamic time structures in computation and music, rhythmic and symbolic time structures, or the interactive control, visualisation and execution of sound synthesis and spatialization processes [23].

8.1.3. 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 MuTant team is also an active member of the ANR CHRONOS Network by Gérard Berry, Collège de France).

8.2. European Initiatives

8.2.1. Collaborations in European Programs, except FP7 & H2020

Program: PHC Amadeus ()

Project acronym: LETITBE

Project title: Logical Execution Time for Interactive And Composition Assistance Music Systems

Duration: 01/2015 - 12/2016

Coordinator: Florent Jacquemard, Christoph Kirsch

Other partners: Department of Computer Sciences University of Salzburg, Austria

Abstract: The objective of this project is to contribute to the development of computer music systems supporting advanced temporal structure in music and advanced dynamics in interactivity. For this purpose we are proposing to re-design and re-engineer computer music systems (from IRCAM at Paris) using advanced notions of time and their software counterparts developed for safety-critical embedded systems (from University of Salzburg). In particular, we are applying the so-called logical execution time paradigm as well as its accompanying time safety analysis, real-time code generation, and portable code execution to computer music systems. Timing in music is obviously very important. Advanced treatment of time in safety-critical embedded systems has helped address extremely challenging problems such as predictability and portability of real-time code. We believe similar progress can be made in computer music systems potentially enabling new application areas. The objective of the project is ideally suited for a collaboration of partners with complementary expertise in computer music and real-time systems.

8.3. International Initiatives

8.3.1. Inria International Labs projects

MuTant team hosted a Master Level student from the Inria Chile Center in partnership with the *Pontificia Universidad Catolica de Chile*. The project, undertaken by Nicolas Schmidt Gubbins and supervised by Arshia Cont and Jean-Louis Giavitto, ended in the first prototype of an embedded *Antescofo* engine (see 7.7) with internal audio processing on Raspberry PI and UDOO mini-computers (See Presentation Video). A publication of preliminary results is underway and early results reported in [29].

8.3.2. Informal International Partners

- We are pursuing a long term collaboration with Masahiko Sakai (U. Nagoya) on term rewriting techniques and applications (in particular applications related to rhythm notation) [14], [17].
- We are collaborating with Slawek Staworko (LINKS, currently on leave at U. Edinburgh), and more generaly the Algomus group at Lille, in the context of our projects on rhythm transcription described at Sections 6.4 and 7.10 .
- MuTant team collaborates with *Bucharest Polytechnic University*, in the framework of Grig Burloiu's PhD Thesis on *AscoGraph* UIX design which has resulted in a the new design of AscoGraph (see 6.2) and two publications [12], [13].
- MuTant team collaborated with researchers at National Institute of Informatics of Tokyo on real-time Symbolic Alignment of music data resulting in the publication in [19].

8.4. International Research Visitors

Masahiko Sakai (Professor at the University of Nagoya) visited MuTant for two weeks in September 20154, for collaboration on term rewriting techniques applied to tree-structured symbolic representations of rhythm.

Slawek Staworko (LINKS, on leave at U. of Edinburgh) visited MuTant for two weeks in September and December 2015, for collaborations on the problem of automatic rhythm transcription.

Professor Miller Puckette (UCSD) visited MuTant for two weeks in May 2015, participating in the PhD defense of José Echeveste and collaborating with the team on the new Audio Processing engine for embedded mini-computers.

8.4.1. Internships

The MuTant team hosted an International Internship from *Pontificia Universidad Catolica de Chile*, Nicolas Schmidt, working on the first instances of embedded Antescofo Audio Engine (See Presentation Video) (see also 7.7) [29].

PARKAS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

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

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

ANR CAFEIN, 2013-2015. Marc Pouzet.

8.1.2. 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).

8.1.3. Others

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

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. Eurolab-4-HPC

Title: EuroLab-4-HPC: Foundations of a European Research Center of Excellence in High Performance Computing Systems

Program: H2020

Duration: September 2015 - September 2017

Coordinator: CHALMERS TEKNISKA HOEGSKOLA AB

Partners:

- Barcelona Supercomputing Center - Centro Nacional de Supercomputacion (Spain)
- Chalmers Tekniska Hoegskola (Sweden)
- Ecole Polytechnique Federale de Lausanne (Switzerland)
- Eidgenoessische Technische Hochschule Zuerich (Switzerland)
- Foundation for Research and Technology Hellas (Greece)
- Universitaet Stuttgart (Germany)
- Rheinisch-Westfaelische Technische Hochschule Aachen (Germany)
- Technion - Israel Institute of Technology (Israel)
- Universitaet Augsburg (Germany)
- The University of Edinburgh (United Kingdom)
- Universiteit Gent (Belgium)
- The University of Manchester (United Kingdom)

Inria contact: Albert Cohen

Europe has built momentum in becoming a leader in large parts of the HPC ecosystem. It has brought together technical and business stakeholders from application developers via system software to exascale systems. Despite such gains, excellence in high performance computing systems is often fragmented and opportunities for synergy missed. To compete internationally, Europe must bring together the best research groups to tackle the longterm challenges for HPC. These typically cut across layers, e.g., performance, energy efficiency and dependability, so excellence in research must target all the layers in the system stack. The EuroLab-4-HPC project's bold overall goal is to build connected and sustainable leadership in high-performance computing systems by bringing together the different and leading performance orientated communities in Europe, working across all layers of the system stack and, at the same time, fuelling new industries in HPC.

8.2.1.2. TETRACOM

Title: Technology Transfer in Computing Systems

Program: FP7

Duration: September 2013 - August 2016

Coordinator: RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN

Partners:

Imperial College of Science, Technology and Medicine (United Kingdom)

Rheinisch-Westfaelische Technische Hochschule Aachen (Germany)

Technische Universiteit Delft (Netherlands)

Tty-Saatio (Finland)

Universita di Pisa (Italy)

Inria contact: Albert Cohen

The mission of the TETRACOM Coordination Action is to boost European academia-to-industry technology transfer (TT) in all domains of Computing Systems. While many other European and national initiatives focus on training of entrepreneurs and support for start-up companies, the key differentiator of TETRACOM is a novel instrument called Technology Transfer Project (TTP). TTPs help to lower the barrier for researchers to make the first steps towards commercialisation of their research results. TTPs are designed to provide incentives for TT at small to medium scale via partial funding of dedicated, well-defined, and short term academia-industry collaborations that bring concrete R&D results into industrial use. This will be implemented via competitive Expressions-of-Interest (EoI) calls for TTPs, whose coordination, prioritization, evaluation, and management are the major actions of TETRACOM. It is expected to fund up to 50 TTPs. The TTP activities will be complemented by Technology Transfer Infrastructures (TTIs) that provide training, service, and dissemination actions. These are designed to encourage a larger fraction of the R&D community to engage in TTPs, possibly even for the first time. Altogether, TETRACOM is conceived as the major pilot project of its kind in the area of Computing Systems, acting as a TT catalyst for the mutual benefit of academia and industry. The projects primary success metrics are the number and value of coordinated TTPs as well as the amount of newly introduced European TT actors. It is expected to acquire around more than 20 new contractors over the project duration. TETRACOM complements and actually precedes the use of existing financial instruments such as venture capital or business angels based funding.

8.2.1.3. COPCAMS

Title: COgnitive & Perceptive CAMeraS

Program: FP7

Duration: April 2013 - March 2016

Coordinator: ___COORDINATOR___???

Partners:

Aselsan Elektroniknayi Ve Ticaret A.S. (Turkey)

Application Solutions (electronics and Vision) Ltd (United Kingdom)

Bs Spolka Z Ograniczona Odpowiedzialnoscia Spolka Komandytowa (Poland)

Concatel Sl (Spain)

Commissariat A L Energie Atomique et Aux Energies Alternatives (France)

Centre Tecnologic de Telecomunicacions de Catalunya (Spain)

Politechnika Gdanska (Poland)

Information and Image Management Systems (Spain)

Institut Jozef Stefan (Slovenia)

Iquadrat Informatica Sl (Spain)

"kolektor Group D.O.O., Vodenje in Upravljanje Družb" (Slovenia)

Queen Mary University of London (United Kingdom)

Danmarks Tekniske Universitet (Denmark)

Sogilis (France)

Squadrone System (France)

Stmicroelectronics Grenoble 2s (France)

Fundacion Tecnalia Research & Innovation (Spain)

Tedesys Global Sociedad Limitada (Spain)

Thales Communications & Securitys (France)

Thales (France)

Thales Research & Technology (uk) (United Kingdom)

Universidad de Cantabria (Spain)

Wavelens (France)

Inria contact: Albert Cohen

'Vision systems are becoming ubiquitous in our daily lives. Complex analysis of images from multiple cameras will become the norm in the future, from cars to industrial systems, from smart cities to facility monitoring, aimed at extracting meaningful, context-dependent information. Today's market is dominated by a combination of relatively simple, fixed function, configurable cameras that stream video to PC-based (and in some cases small embedded) gateways. These systems cannot scale beyond a certain size because of power consumption and the aggregate networking bandwidth required to stream videos to servers, where aggregated video analysis is performed. So the trend for visual analytics functions is that they get executed at the edge of these complex vision systems, e.g. in the cameras themselves. The Cognitive and Perceptive Camera Systems (COPCAMS) proposal leverages recent advances in embedded computing platforms to design, prototype and field-test full large-scale vision systems. It aims at exploiting a new many-core programmable accelerator platform to power a new generation of vision related devices (smart cameras and gateways), able to extract relevant information from captured images and autonomously react to the sensed environment by interoperating at large scale in a distributed manner. Date of approval by ARTEMIS JU: 7/04/2015.'

8.2.1.4. EMC2

Title: Embedded Multi-Core Systems for Mixed Criticality Applications in Dynamic and Changeable Real-Time Environments

Program: FP7

Duration: April 2014 - March 2917

Coordinator: Infineon Technologies

Partners:

- Aicas (Germany)
- Avl Software and Functions (Germany)
- Denso Automotive Deutschland (Germany)
- Elektrobit Automotive (Germany)
- Evision Systems (Germany)
- Nxp Semiconductors Germany (Germany)
- Tttech Computertechnik (Austria)
- "kompetenzzentrum - Das Virtuelle Fahrzeug, Forschungsgesellschaft Mbh" (Austria)
- Frequentis (Austria)
- Thales Austria (Austria)
- Blueice Bvba (Belgium)
- Freescale Polovodice Ceska Republika Sro (Czech Republic)
- Institut Mikroelektronickych Aplikaci S.R.O. (Czech Republic)
- Sysgo Sro (Czech Republic)
- Silkan Rt (France)
- "united Technologies Research Centre Ireland," (Ireland)
- Mbda Italia Spa (Italy)
- Fornebu Consulting As (Norway)
- Westerngeco As (Norway)
- Simula Research Laboratory As (Norway)
- Ixion Industry and Aerospace Sl (Spain)
- Visure Solutions Sl (Spain)
- Seven Solutions Sl (Spain)
- Telvent Energia (Spain)
- Instituto Tecnologico de Informatica (Spain)
- Ambar Telecomunicaciones Sl (Spain)
- Sics Swedish Ict (Sweden)
- Arcticus Systems (Sweden)
- Arccore (Sweden)
- Xdin Stockholm (Sweden)
- Systemite (Sweden)
- Stichting Imec Nederland (Netherlands)
- Tomtom International Bv (Netherlands)
- Infineon Technologies Uk Ltd (United Kingdom)
- Sundance Multiprocessor Technology Ltd (United Kingdom)
- Systonomy (United Kingdom)
- Ensilica Ltd (United Kingdom)
- Test and Verification Solutions Ltd (United Kingdom)
- Abb (Sweden)
- Ait Austrian Institute of Technology (Austria)

Alenia Aermacchi Spa (Italy)

Avl List (Austria)

Airbus Defence and Space (Germany)

Bayerische Motoren Werke Aktiengesellschaft (Germany)

Consorzio Interuniversitario Nazionale Per l'Informatica (Italy)

Critical Software (Portugal)

Chalmers Tekniska Hoegskola (Sweden)

Danfoss Power Electronics As (Denmark)

Ericsson (Sweden)

Centro Ricerche Fiat (Italy)

Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (Germany)

Hi Iberia Ingenieria Y Proyectos Sl (Spain)

Harokopio University (Greece)

Infineon Technologies Austria (Austria)

"inesc Id - Instituto de Engenhariade Sistemas E Computadores, Investigacao E Desenvolvimento Em Lisboa Associacao" (Portugal)

Infineon Technologies (Germany)

Integrasys (Spain)

Instituto Superior de Engenharia Do Porto (Portugal)

Kungliga Tekniska Hoegskolan (Sweden)

Lulea Tekniska Universitet (Sweden)

Magillem Design Servicess (France)

Nxp Semiconductors Netherlands Bv (Netherlands)

Offis E.V. (Germany)

Politecnico di Torino (Italy)

Philips Medical Systems Nederland Bv (Netherlands)

Quobis Networks Sl (Spain)

Rockwell Collins France (France)

Rigas Tehniska Universitate (Latvia)

Selex Es Spa (Italy)

Siemens Aktiengesellschaft (Germany)

Systematic Paris Region Association (France)

Sysgo (Germany)

Thales Alenia Space Italia Spa (Italy)

"thales Alenia Space Espana," (Spain)

Technolution B.V. (Netherlands)

Thales Avionicss (France)

Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (Netherlands)

Technische Universitaet Wien (Austria)

Technische Universiteit Eindhoven (Netherlands)

Technische Universitat Braunschweig (Germany)

Technische Universiteit Delft (Netherlands)

Technische Universitat Dortmund (Germany)

Universitetet I Oslo (Norway)

Technische Universitaet Kaiserslautern (Germany)

University of Limerick (Ireland)

Universita Degli Studi di Genova (Italy)

Universita Degli Studi Dell'aquila (Italy)

University of Bristol (United Kingdom)

The University of Manchester (United Kingdom)

"ustav Teorie Informace A Automatizace Av Cr, V.V.I." (Czech Republic)

Vector Fabrics Bv (Netherlands)

Volvo Technology (Sweden)

Vysoke Uceni Technicke V Brne (Czech Republic)

Inria contact: Albert Cohen

Embedded systems are the key innovation driver to improve almost all mechatronic products with cheaper and even new functionalities. Furthermore, they strongly support today's information society as inter-system communication enabler. Consequently boundaries of application domains are alleviated and ad-hoc connections and interoperability play an increasing role. At the same time, multi-core and many-core computing platforms are becoming available on the market and provide a breakthrough for system (and application) integration. A major industrial challenge arises facing (cost) efficient integration of different applications with different levels of safety and security on a single computing platform in an open context. The objective of the EMC^2 project (Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments) is to foster these changes through an innovative and sustainable service-oriented architecture approach for mixed criticality applications in dynamic and changeable real-time environments. The EMC2 project focuses on the industrialization of European research outcomes and builds on the results of previous ARTEMIS, European and National projects. It provides the paradigm shift to a new and sustainable system architecture which is suitable to handle open dynamic systems. EMC^2 is part of the European Embedded Systems industry strategy to maintain its leading edge position by providing solutions for: . Dynamic Adaptability in Open Systems . Utilization of expensive system features only as Service-on-Demand in order to reduce the overall system cost. . Handling of mixed criticality applications under real-time conditions . Scalability and utmost flexibility . Full scale deployment and management of integrated tool chains, through the entire lifecycle Approved by ARTEMIS-JU on 12/12/2013 for EoN. Minor mistakes and typos corrected by the Coordinator, finally approved by ARTEMIS-JU on 24/01/2014. Amendment 1 changes approved by ECSEL-JU on 31/03/2015.

8.2.2. Collaborations in European Programs, except FP7 & H2020

8.2.2.1. EMC2

Title: Affordable Safe & Secure Mobility Evolution – ASSUME

Program: Eureka ITEA3

Duration: April 2014 - March 2917

Coordinator: Siemens

Partners:

Inria

ENS Paris

Thales RT

Airbus

Esterel Technologies

Kalray

And many European partners

Inria contact: Dumitru Potop-Butucaru

Future mobility solutions will increasingly rely on smart components that continuously monitor the environment and assume more and more responsibility for a convenient, safe and reliable operation. In order to realize this vision, the need for computing power will drastically increase beyond what can be provided by conventional sequential single-core hardware. While the required efficiency and scalability makes it mandatory for future embedded micro-controllers to rely on multi- and many-core architectures, the change in hardware architecture also entails fundamental changes to state of the art software development methodology. Replacing today's essentially sequential technology by omnipresent communication between cores poses the tremendous challenge in software development to identify and exploit opportunities for concurrency in a way which still guarantees reliable and predictable behavior. Aside from the evolution of new hardware architectures, software development must address the increasing level of complexity of new highly automatic mobility solutions. For automotive, the self-driving car is the next big revolution and it is still unclear how functional and non-functional guarantees can be given for this new class of assistance functions. European industry heavily relies on the premium market segments. In these segments, innovative functions are the most important factor to influence buying decisions. New competitors, e.g. Google, enter the stage and challenge the established industry with eager visions. However, the single most important roadblock for this market is the ability to come up with an affordable, safe multi-core development methodology that allows industry to deliver trustworthy new functions at competitive prices. The ASSUME algorithm portfolio will be the key technology to bring innovative solutions from sandboxes into consumers' daily lives. ASSUME provides a seamless engineering methodology to overcome this roadblock. The problem is addressed on the constructive and on the analytic side. For efficient construction and synthesis of embedded systems, the project provides new tools, standards and methodologies to cover most of the challenges by design. In addition, ASSUME provides a well-integrated sound static analysis solution that allows proving the absence of problems even in a multi-core environment. New algorithms will be integrated in exploitable tools. New interoperability standards and requirements formalization standards will facilitate cooperation between different market players. The ASSUME consortium includes leading European industry partners for mobility solutions, tool and service providers for embedded system development as well as leading research institutes for static analysis for model-driven and traditional embedded systems development.

8.2.3. Collaborations with Major European Organizations

Albert Cohen is an external member of the ARTEMIS-IA Working Group. Collaborating on the writing of the association's Strategic Research Agenda (SRA), and the ECSEL JU Multi-Annual Research and Innovation Agenda (MASRIA).

https://artemis-ia.eu

8.3. International Initiatives

8.3.1. Inria Associate Teams not involved in an Inria International Labs

8.3.1.1. POLYFLOW

Title: Polyhedral Compilation for Data-Flow Programming Languages

International Partner (Institution - Laboratory - Researcher):

IISc Bangalore (India) - Department of Computer Science and Automation (CSA) - Uday Kumar Reddy Bondhugula

Start year: 2013

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.

An extension for 3 more years has been requested. It may be partly funded by CEFIPRA.

8.3.2. Inria International Partners

8.3.2.1. Informal International Partners

Prof. Uday Bondhugula, CSA department, Indian Institute of Science, India. See POLYFLOW associate team for details.

Prof. P. Sadayappan, CS department, Ohio State University, USA. Joint publications, frequent visits, occasionally for several weeks.

Prof. M. Sheeran, Computer Science and Engineering Department, Chalmers University of Technology, Sweden. Regular visits. Continuing exchanges on languages and compilation for synchronous and hybrid systems.

Prof. C. Tinelli, CS department, University of IOWA, USA. Regular visits. Continuing exchanges on the verification of synchronous languages and programs.

Prof. R. von Hanxleden, Director at the Department of Computer Science, Head of the Real-Time and Embedded Systems Group, Kiel University, Germany. Regular visits and scientific collaboration.

Prof. M. Mendler, Head of the Informatics Theory Group, Bamberg University, Germany. Regular visits and scientific collaboration.

Dr. Sven Verdoolaege, CS department, K. U. Leuven, Belgium. Joint steering of the Polly Labs initiative and contractual cooperation in this context.

Dr. Tobias Grosser in the group of Prof. Torsten Hoeffler, ETH Zürich. Joint steering of the Polly Labs initiative. See Polly Labs for details.

Pr. Peter Sewell, Computer Laboratory, University of Cambridge, UK. Regular visits and scientific collaboration.

Pr. Jan Vitek, College of Computer & Information Science Northeastern University, USA. Regular visits and scientific collaboration.

8.3.3. Participation In other International Programs

The POLYFLOW associate team has been extended for up to 3 years on January 1st 2016, in collaboration with CEFIPRA (http://cefipraonline.in).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Prof. Michael Mendler, Univ. Bamberg, Germany, spent one month as an invited professor in the team in March 2015.

Dr. Artjoms Sinkarovs, Heriot Watt University, UK, spent 2 months as an visiting scholar in Summer 2015.

8.4.1.1. Internships

Abhishek Jain, 4th year student from IIT Delhi, visited us for 1 and a half months in January 2015.

Chaitanya Malaviya, 3rd year student from Nanyang Technological University, visited us for 2 months in July and August 2015.

8.4.2. Visits to International Teams

8.4.2.1. Research stays abroad

Marc Pouzet spent 15 days in the group of Prof. M. Mendler at Bamberg University in July 2015.

Albert Cohen spent 1 month in the group of Prof. P. Sadayappan at Ohio State University, in April–May 2015. One paper was accepted to the ACM PLDI 2016 conference as a result of this collaboration.

Timothy Bourke spent 1 week in the group of Prof. C. Tinelli at The University of Iowa in December 2015.

POSET Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. SCRIME

The Studio de Création et de Recherche en Informatique et Musiques Expérimentales (SCRIME) located on Bordeaux University Campus, is a *Groupement d'Intérêt Scientifique et Artistique (GIS&A)* gathering Université de Bordeaux, CNRS, Bordeaux INP, Ministère de la Culture et de la Communication, Ville de Bordeaux and Région Aquitaine. It is a privileged partner of the PoSET project. Most PoSET artistic projects are organized in cooperation with the SCRIME.

9.1.2. Idex Bordeaux

- 4 *Arts & Science* projects of Bordeaux eventually granted in 2015 by the Initiative of Excellence (Idex) of Bordeaux,

9.2. National Initiatives

9.2.1. ANR

- ANR INEDIT, *Interactivité dans l'Ecriture De l'Interaction et du Temps*, coordinated by Ircam (Paris), 3 years, from 2012 to 2015, together with GRAME (Lyon); this project aimed at developing and integrating the existing formalisms to represent and perform interactive pieces of art,
- ANR OSSIA, *Open Scenario System for Interactive Application*, coordinated by GMEA (Albi), 3 years, from 2012 to 2015, together with Blue Yeti (Royan), ENJMIN (Poitiers), RSF (Toulouse); this project aimed at offering software services, especially within the Jamoma platform, to design, implement and perform open, non-linear and multi-user scenarios.

9.3. International Initiatives

9.3.1. Inria International Partners

PoSET members have regular though often informal collaboration with various international teams including:

- Camillo Rueda, Universidad Javaneria, Cali, Colombia,
- Paul Hudak, University of Yale, New-Haven, USA,
- Gregory M. Kobele, University of Chicago, USA,
- Makoto Kanazawa, National Institute of Informatics, Tokyo, Japan.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Shlomo Dubnov, UCSD (USA), visiting Scholar from November 2015 until June 2016,
- Eduardo Mirando, University of Plymouth, UK, invited professor from May the 15th until June the 15th.

9.4.2. Visits to International Teams

- D. Janin visiting Stuart Margolis, Bar Illan (Israël), April 2015,

SPADES Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR Projects

8.1.1.1. 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 ended in November 2015.

8.2. European Initiatives

8.2.1. Collaborations with Major European Organizations

We have a strong collaboration with the Technische Universität Braunschweig in Germany. In particular, Sophie Quinton actively participates in the CCC project (http://ccc-project.org/) to provide methods and mechanisms for the verification of software updates after deployment in safety-critical systems.

8.3. International Initiatives

8.3.1. Inria International Labs

Inria@SiliconValley
Associate Team involved in the International Lab:

8.3.1.1. RIPPES

Title: RIgorous Programming of Predictable Embedded Systems

International Partner (Institution – Laboratory – Researcher):

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

University of Auckland (New Zealand) – Electrical Computer Engineering Department (ECE) – Partha Roop

Start year: 2013

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. of Auckland (ECE Department). The planned research seeks to reconcile two contradictory objectives of embedded systems, more predictability and more adaptivity. We have addressed 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 (see Section 6.2.1), and (2) by starting from a very predictable model of computation (SDF) and enhancing it to provide more adaptivity (see Section 6.2.3).

8.3.2. Inria Associate Teams not involved in an Inria International Labs

8.3.2.1. Causalysis

Title: Causality Analysis for Safety-Critical Embedded Systems

International Partner (Institution – Laboratory – Researcher):

University of Pennsylvania (United States) – PRECISE center – Oleg Sokolsky

Start year: 2015

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

Today's embedded systems become more and more complex, while an increasing number of safety-critical functions rely on them. Determining the cause(s) of a system-level failure and elucidating the exact scenario that led to the failure is today a complex and tedious task that requires significant expertise. The CAUSALYSIS project will develop automated approaches to causality analysis on execution logs.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

- Atena Abdi has been a visitor in the team from October 2015 to June 2016. She is doing her PhD at the Amirkabir University of Technology in Teheran, Iran. In the SPADES team, she is working on multi-criteria scheduling for real-time embedded systems, addressing the complex interplay between reliability, power consumption, temperature, and execution time (see 6.3.2).
- Ismail Assayad has been a visitor in the team in September 2015. He is assistant professor at the University of Casablanca, Morocco. In the SPADES team, he is working on adaptive scheduling methods and admission control for dynamic embedded applications (see 6.3.2).

TEA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

Program: ANR

Project acronym: **Feever**

Project title: Faust Environment Everyware

Duration: 2014-2016

Coordinator: Pierre Jouvelot, Mines ParisTech

Other partners: Grame, Inria Rennes, CIEREC

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.

9.1.2. 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..

9.1.3. 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.

9.2. International Initiatives

9.2.1. International Project Grants

9.2.1.1. US Air Force 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.

9.2.1.2. Applied Science & Technology Research Institute (ASTRI, Hong Kong)

Title: Virtual Prototyping of Embedded Software Architectures

Inria principal investigator: Jean-Pierre Talpin

International Partner: ASTRI, Hong Kong

Duration: 2015 - 2016

Abstract: the topics of our present collaboration is essentially on heterogeneous time modelling for virtual prototyping in cyber-physical systems. Our project covers a wide spectrum of area of experience developed since 2012 and comprising

- model-based design and analysis of cyber-physical systems;
- system-level virtual prototyping and validation;
- design space exploration and system synthesis;

9.2.2. Inria International Labs

9.2.2.1. SACCADES

Title: Saccades

International Partner:

LIAMA

East China Normal University

Inria project-teams Aoste and Tea

Duration: 2003 - now

The SACCADES project is a LIAMA project hosted by East China Normal University and jointly led by Vania Joloboff (Inria) and Min Zhang (ECNU). The SACCADES project aims at improving the development of reliable cyber physical systems and more generally of distributed systems combining asynchronous with synchronous aspects, with different but complementary angles:

- develop the theoretical support for Models of Computations and Communications (MoCCs) that are the fundamentals basis of the tools.
- develop software tools (a) to enable the development and verification of executable models of the application software, which may be local or distributed and (b) to define and optimize the mapping of software components over the available resources.
- develop virtual prototyping technology enabling the validation of the application software on the target hardware platform.

The ambition of SACCADES project is to develop

- Theoretical Support for Cyber Physical Systems
- Software Tools for design and validation of CPS
- Virtual Prototyping of CPS

9.2.3. Inria International Partners

9.2.3.1. POLYCORE

Title: Models of computation for embedded software design

International Partner:

Virginia Tech Research Laboratories (USA)

University of Kanpur (India)

Duration: 2002 - now

Team TEA collaborates with Sandeep Shukla (now with IIT Kanpur) and his team at Virginia Tech, since 2002 (NSF-Inria BALBOA and Polycore projects, USAF OSR grant).

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 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 40 joint journal articles and conference papers.

This year, we published a joint paper at the 52nd. Digital Automation Conference in San Francisco [19].

9.2.3.2. VESA

Title: Virtual Prototyping of embedded software architectures

International Partner:

Applied Science & Technology Research Institute (ASTRI, Hong Kong)

The University of Hong Kong

Duration: 2012 - now

[0] ACM-IEEE MEMOCODE conference series
[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

We collaborate with John Koo, now with ASTRI, and LIAMA since 2012 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 in cyber-physical systems.

9.2.3.3. TIX

Title: Time In Cybernetic Systems

International Partner:

Rajesh Gupta, UCSD

Mani Srivastava, UCLA

Start year: 2015

The first topic of our collaboration is the formal definition of cross-domains clock models in system design and the formal verification of time stabilisation and synchronisation protocols used in distributed systems (sensor networks, data-bases). In this prospect, the NSF project Roseline is our basis of investigation (https://sites.google.com/site/roselineproject). Roseline aims at enabling robust, secure and efficient knowledge of time across the system stack.

Our second topic of collaboration is the refoundation of time modelling in high-level reactive and scripting languages, for application to the above using uni-kernels to cut through system stacks. We aim at applying the concepts of refinement types to formally specify and infer timing properties in CPS models from different system design view-point (physical, hardware, software) and using different levels of abstraction into multi-sorted 1st order logic (delta-decidability, linear arithmetic, Boolean logic, temporal logic).

9.3. International Research Visitors

9.3.1. Visits to International Teams

9.3.1.1. Research stays abroad

Jean-Pierre Talpin was awarded a visiting researcher grant by USAF OSR in 2014. In this context, he visited the Arlington and Falls Church VT campuses in Spring, Summer of 2015, and UC San Diego in Autumn 2015.

Thierry Gautier was invited to visit NUAA (Nanjing University of Aeronautics and Astronautics), Nanjing, China, in September 2015.

ANTIQUE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

7.1.1.1. 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 analyzed 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 ANASTASEC project 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.

7.1.1.2. 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.

7.1.1.3. 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 THESEE 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.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. 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)

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.

7.3. International Initiatives

7.3.1. EXEcutable Knowledge

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.

7.3.2. Active Context

Title: Active Context
Type: DARPA
Instrument: DARPA Program
Program: Communicating with Computers
Duration: July 2015 - December 2018
Coordinator: Harvard Medical School (Boston, USA)
Partner: University of California, (San Diego, USA), Inria Paris-Rocquencourt, École normale supérieure de Lyon Université Paris-Diderot,
Inria contact: Jérôme Feret
Abstract: The traditional approach to the curation of biological information follows a philatelic paradigm, in which epistemic units based on raw or processed data are sorted, compared and catalogued in a slow and all too often insufficiently coordinated process aimed at capturing the meaning of each specimen in isolation. The swelling bounty of data generated by a systematic approach to biology founded on high-throughput technologies appears to have only intensified a sense of disconnected facts, despite their rendering as networks. This is all the more frustrating as the tide of static data (sequences, structures) is giving way to a tide of dynamic data about (protein-protein) interaction that want to be interconnected and understood (think annotated) in terms of process, i.e. a systemic approach.

The barrier is the complexity of studying systems of numerous heterogeneously interacting components in a rapidly evolving field of science. The complexity comes from two kinds of dynamically changing context: the internal dynamics of a biological system, which provide the context for assessing the meaning of a protein-protein interaction datum, and the external dynamics of the very fact base used to define the system in the first place. We propose the integration of dynamic modeling into the practice of bioinformatics to address these two dynamics by coupling them. The external dynamics is at first handled by a novel kind of two-layered knowledge representation (KR). One layer contextualizes proteins and their interactions in a structure that incrementally constructs, in an open-ended dialogue with the user, its own semantics by piecing together fragments of knowledge from a variety of sources tapped by the Big Mechanism program. The other layer is a model representation (MR) that handles and prioritizes the many executable abstractions compatible with the KR. The internal dynamics is handled not only by execution but also by addressing the impedance mismatch between the unwieldy formal language(s) required for execution and the more heuristic, high-level concepts that structure the modeling discourse with which biologists reason about molecular signaling systems. To the extent that we are successful on both ends, users will be able to effectively deploy modeling for curating the very fact base it rests upon, hopefully achieving self-consistency.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Josef Widder, associate professor at TU Wien, Embedded Computing Systems group, visited Cezara Drăgoi for a week, from Oct 12 to Oct 17.

7.4.1.1. Internships

Jérôme Feret is supervizing the Internships of Ken Chanseau Germain (M2 student), on “approximated model reduction of differential semantics”, since november 2015.

CELTIQUE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. The ANR VERASCO project

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

Static program analysis, Certified static analysis

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

7.1.2. The ANR AnaStaSec project

Participants: Frédéric Besson, Sandrine Blazy, Thomas Jensen.

Static program analysis, Security, Secure compilation

The AnaStaSec project (2015–2018) aims at ensuring security properties of embedded critical systems using static analysis and security enhancing compiler techniques. The case studies are airborne embedded software with ground communication capabilities. The Celtique project focuses on software fault isolation which is a compiler technology to ensure by construction a strong segregation of tasks.

This is a joint project with the Inria teams ANTIQUE and PROSECCO, CEA-LIST, TrustInSoft, AMOSSYS and Airbus Group.

7.1.3. The ANR Binsec project

Participants: Frédéric Besson, Sandrine Blazy, Pierre Wilke.

Binary code, Static program analysis

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

Binsec is a joint project with the Inria CARTE team, CEA LIS, VERIMAG and EADS IW.

7.1.4. 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.

7.1.5. The ANR AJACS project

Participants: Martin Bodin, Gurvan Cabon, 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.

7.1.6. The ANR DISCOVER project

Participants: Sandrine Blazy, Delphine Demange, Thomas Jensen, David Pichardie, Yon Fernandez de Retana.

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.

7.1.7. Labex COMIN Labs Seccloud project

Participants: Frédéric Besson, Thomas Jensen, Alan Schmitt, Thomas Genet, Martin Bodin, Gurvan Cabon.

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

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

7.2. International Initiatives

7.2.1. Inria Associate Teams not involved in an Inria International Labs

7.2.1.1. JCERT

Title: Verified Compilation of Concurrent Managed Languages

International Partner (Institution - Laboratory - Researcher):

Purdue University (United States) - Suresh Jagannathan

Start year: 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#.

7.2.2. Inria International Partners

7.2.2.1. Declared Inria International Partners

Professor Philippa Gardner, Imperial College, UK, since December 2015.

7.2.2.2. Informal International Partners

Alan Schmitt is part of a Polonium Hubert Curien Partnership (PHC) with the University of Wrocław. This partnership is lead by Sergueï Lenglet, from Loria, Nancy, France.

7.3. International Research Visitors

7.3.1. Visits to International Teams

7.3.1.1. Sabbatical programme

Jensen Thomas

Date: Sep 2014 - Aug 2015

Institution: University of Copenhagen (Denmark)

7.3.1.2. Research stays abroad

Martin Bodin visited the Department of Computing at Imperial College London for three months.

DEDUCTEAM Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR Locali

We are coordinators of the ANR-NFSC contract Locali with the Chinese Academy of Sciences.

8.1.2. 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.

8.1.3. ANR Tarmac

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

8.2. International Research Visitors

8.2.1. Visits of International Scientists

Jim Lipton, professor at Wesleyan University (USA) has visited Deducteam from 9 to 14 March 2015.

8.2.1.1. Internships

Gaetan Gilbert did an internship with Arnaud Spiwack and Olivier Hermant.

Shuai Wang did an internship with Gilles Dowek.

Éric Uzena did an internship with Arnaud Spiwack and David Delahaye.

8.2.2. Visits to International Teams

8.2.2.1. Sabbatical programme

Olivier Hermant is a visiting professor at Wesleyan University (USA) since September 2015.

ESTASYS Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. 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.

7.1.2. 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. FP7 & H2020 Projects

7.3.1.1. ACANTO

Title: ACANTO: A Cyber physicAl social NeTwOrk using robot friends

Programm: H2020

Duration: February 2015 - August 2018

Coordinator: Universita di Trento

Partners:

- Atos Spain (Spain)
- Envitel Tecnologia Y Control S.A. (Spain)
- Foundation for Research and Technology Hellas (Greece)
- Servicio Madrileno Delud (Spain)
- Siemens Aktiengesellschaft Oesterreich (Austria)
- Telecom Italia Spa (Italy)
- Universita' Degli Studi di Siena (Italy)
- Universita Degli Studi di Trento (Italy)
- University of Northumbria At Newcastle. (United Kingdom)

Inria contact: Axel Legay

'Despite its recognised benefits, most older adults do not engage in a regular physical activity. The ACANTO project proposes a friendly robot walker (the FriWalk) that will abate a some of the most important barriers to this healthy behaviour. The FriWalk revisits the notion of robotic walking assistants and evolves it towards an activity vehicle. The execution of a programme of physical training is embedded within familiar and compelling every-day activities. The FriWalk operates as a personal trainer triggering the user actions and monitoring their impact on the physical and mental well-being. It offers cognitive and emotional support for navigation pinpointing risk situations in the environment and understanding the social context. It supports coordinated motion with other FriWalks for group activities. The FriWalk combines low cost and advanced features, thanks to its reliance on a cloud of services that increase its computing power and interconnect it to other assisted living devices. Very innovative is its ability to collect observations on the user preferred behaviours, which are consolidated in a user profile and used for recommendation of future activities. In this way, the FriWalk operates as a gateway toward a CyberPhysical Social Network (CPSN), which is an important contribution of the project. The CPSN is at the basis of a recommendation system in which users' profiles are created, combined into 'circles' and matched with the opportunity offered by the environment to generate recommendations for activities to be executed with the FriWalk support. The permanent connection between users and CPSN is secured by the FriPad, a tablet with a specifically designed user interface. The CPSN creates a community of users, relatives and therapists, who can enter prescriptions on the user and receive information on her/his state. Users are involved in a large number in all the phases of the system development and an extensive validation is carried out at the end.'

7.3.2. Danse

Program: FP7

Project acronym: DANSE

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

Duration: Octobre 2011 – March 2015

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.

7.3.3. Meals

Program: Marie Curie

Project acronym: Meals

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

Duration: Octobre 2012 – Octobre 2015

Coordinator: Germany (Saarbrucken) and Argentina (Corona)

Abstract: Collaborative action on the topic of quantitative systems

7.3.4. 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.

7.3.5. 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.

7.3.6. Collaborations with Major European Organizations

- Partner 1: Aalborg University, Computer Science, Denmark
- Statistical Model Checking, and Systems of Systems
- Partner 2: Rice University, Computer Science, USA
- Synthesis of components of Systems of Systems
- Partner 3: Namur University, Computer Science, Belgium
- Variability in software engineering
- Partner 4: Louvain University, Computer Science, Belgium
- Verification of Systems of Systems via Statistical Model Checking, especially train stations in collaboration with Alstom.
- Partner 5: Waterloo University, Computer Science, Canada
- Variability in Systems of Systems

7.4. International Initiatives

7.4.1. Visits of International Scientists

7.4.1.1. Internships

- Karin Quaas, PostDoc at Leipzig University
- Kim Larsen, Professor at Aalborg University
- Rafael Olochea, PhD student at Waterloo University
- Yusuke Yamamoto, Assistant Professor, Japan.

GALLIUM Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR projects

9.1.1.1. 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.

9.1.1.2. Verasco

Participants: Jacques-Henri Jourdan, Xavier Leroy.

The "Verasco" project (2012–2016) is coordinated by Xavier Leroy and funded by the *Ingéniérie Numérique et Sécurité* programme of *Agence Nationale de la Recherche*. The objective of this 4.5-year project is to develop and formally verify a static analyzer based on abstract interpretation, and interface it with the CompCert C verified compiler.

9.1.1.3. Vocal

Participants: Xavier Leroy, François Pottier.

The "Vocal" project (2015–2020) aims at developing the first mechanically verified library of efficient general-purpose data structures and algorithms. It is funded by *Agence Nationale de la Recherche* under its "appel à projets générique 2015".

The library will be made available to all OCaml programmers and will be of particular interest to implementors of safety-critical OCaml programs, such as Coq, Astrée, Frama-C, CompCert, Alt-Ergo, as well as new projects. By offering verified program components, our work will provide the essential building blocks that are needed to significantly decrease the cost of developing new formally verified programs.

9.1.2. FSN projects

9.1.2.1. ADN4SE

Participants: Damien Doligez, Martin Riener.

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.

9.1.2.2. CEEC

Participants: Maxime Dénès, Xavier Leroy.

The "CEEC" project (2011–2015) 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.

9.1.3. FUI Projects

9.1.3.1. Secur-OCaml

Participants: Damien Doligez, Fabrice Le Fessant.

The "Secur-OCaml" project (2015–2018) is coordinated by the OCamlPro company, with a consortium focusing on the use of OCaml in security-critical contexts, while OCaml is currently mostly used in safety-critical contexts. Gallium is invoved in this project to integrate security features in the OCaml language, to build a new independant interpreter for the language, and to update the recommendations for developers issued by the former LaFoSec project of ANSSI.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. Deepsea

Participants: Umut Acar, Vitalii Aksenov, Arthur Charguéraud, Mike Rainey, Filip Sieczkowski.

The Deepsea project (2013–2018) is coordinated by Umut Acar and funded by FP7 as an ERC Starting Grant. Its objective is to develop abstractions, algorithms and languages for parallelism and dynamic parallelism, with applications to problems on large data sets.

9.2.2. ITEA3 Projects

9.2.2.1. Assume

Participants: Xavier Leroy, Luc Maranget.

ASSUME (2015–2018) is an ITEA3 project involving France, Germany, Netherlands, Turkey and Sweden. The French participants are coordinated by Jean Souyris (Airbus) and include Airbus, Kalray, Sagem, ENS Paris, and Inria Paris. The goal of the project is to investigate the usability of multicore and manycore processors for critical embedded systems. Our involvement in this project focuses on the formalisation and verification of memory models and of automatic code generators from reactive languages.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. 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.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

9.4.1.1. Research stays abroad

From November 2014 to June 2015, Damien Doligez was on a sabbatical at Jane Street (New York, USA), a financial company (a 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

We are currently members of two projects funded by the French national agency for research funding.

- 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. European Initiatives

8.2.1. Collaborations in European Programs, except FP7 & H2020

Program: COST
Project acronym: CA15123EUTYPES
Project title: The European research network on types for programming and verification
Duration: 30 October 2015– 29 October 2019
Coordinator: Herman Geuvers (Radboud University, Nijmegen)
Other partners: List too long to repeat here.
Abstract: Types are pervasive in programming and information technology. A type defines a formal interface between software components, allowing the automatic verification of their connections, and greatly enhancing the robustness and reliability of computations and communications. In rich dependent type theories, the full functional specification of a program can be expressed as a type. Type systems have rapidly evolved over the past years, becoming more sophisticated, capturing new aspects of the behaviour of programs and the dynamics of their execution.

This COST Action will give a strong impetus to research on type theory and its many applications in computer science, by promoting (1) the synergy between theoretical computer scientists, logicians and mathematicians to develop new foundations for type theory, for example as based on the recent development of "homotopy type theory", (2) the joint development of type theoretic tools as proof assistants and integrated programming environments, (3) the study of dependent types for programming and its deployment in software development, (4) the study of dependent types for verification and its deployment in software analysis and verification. The action will also tie together these different areas and promote cross-fertilisation.

Europe has a strong type theory community, ranging from foundational research to applications in programming languages, verification and theorem proving, which is in urgent need of better networking. A COST Action that crosses the borders will support the collaboration between groups and complementary expertise, and mobilise a critical mass of existing type theory research.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

We have important collaborations with the team of Thierry Coquand at Chalmers and University of Göteborg.

We are setting up a collaboration with the team of Adam Chlipala at the Massachusetts Institute of Technology.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Isabela Dramnesc, from the University of Timişoara in Romania, visited our team in June and July to study proving techniques in the Coq context.

Tsvetan Dunchev, from the University of Bologna, visited our team in July to work on ELPI, the λ-prolog interpreter.

8.4.2. Visits to International Teams

Yves Bertot organised a meeting with representants of University of Pennsylvania, Princeton University, Yale University, Harvard University, and the Massachusetts Institute of Technology in Boston in April. Janet Bertot, Philippe Nain, and Matthieu Sozeau from Inria also attended this meeting. The agenda of the meeting was preliminary discussions for the creation of a consortium around the Coq software system.

Enrico Tassi visited the team of Jesper Bengtson at the IT University in Copenhagen for a week at the end of September.

Cyril Cohen visited Chalmers university in Febrary and October to work on cubical type theory.

Cyril Cohen was invited by AIST in Japan for a one-week stay in Tsukuba in November to work on formalization problems for robotics.

MEXICO Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives: IRT

9.1.1. SystemX

Participants: Simon Theissing, Yann Duplouy, Serge Haddad.

We participate in the projects

- 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, and
- the project SVA (*Simulation pour la Sécurité du Véhicule Autonome*), where the PhD Thesis of Yann Duplouy targets the application of formal methods to the development of embedded systems for autonomous vehicles.

9.2. National Initiatives

We have not yet been notified about acceptance of our ANR submissions.

9.3. European Initiatives

In preparation.

9.3.1. FP7 & H2020 Projects

Serge Haddad is participating in the ERC *EQualIS*, 'Enhancing the Quality of Interacting Systems', directed by Patricia Bouyer.

9.4. International Initiatives

9.4.1. Inria International Labs projects

LIA INFORMEL with CMI, Chennai, India ; see below.

9.4.2. Inria International Partners

9.4.2.1. 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 (defended in 2014).

   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* the computer science and electrical engineering departments at Newcastle University, UK , with visits in both directions; they involve in particular Maciej Koutny, Alex Yakovlev, Victor Khomenko and Andrey Mokhov, as well as Anil Wipat, co-director of the center for Synthetic Biology and the Bioeconomy at Newcastle University.

3. Exchanges are frequent with Rolf Hennicker from LMU and Javier Esparza at TUM, both in Munich, Germany.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- 5 – 31 March 2015: Prakash Saivasan (CMI) visits LSV to work with Paul Gastin on nested words for higher-order pushdown systems
- 19 May – 6 June 2015: S. Krishna and S. Akshay visit LSV to work with Paul Gastin on split-width techniques for the analysis of timed systems.
- 10 June – 4 July 2015: K. Narayan Kumar (CMI) visit France to pursue several collaborations: with Paul Gastin (LSV) on bounded time-stamping for message passing systems, with Ahmed Bouajjani (LIAFA) on analysis of multi-pushdown systems, and with Pascal Weil (LaBRI) on bounded reachability analysis for shared memory systems.

9.5.1.1. Internships

Georgios Christodoulis

Date: May 2015 - Jul 2015

Institution: National University Athens (Greece)

Supervisor: Stefan Haar

Sougata Bose

Date: May 2015 - Jul 2015

Institution: CMI (India)

Supervisor: Benedikt Bollig and Paul Gastin

9.5.2. Visits to International Teams

9.5.2.1. Short stays abroad

- In July 2015, Serge Haddad visited U of Turin, Italy, for a research cooperation with Prof. Giuliana Franceschinis.
- Stefan Haar visited Newcastle University (UK), TU of Eindhoven (NL) and University of Luxemburg for short visits.
- 29 November – 20 December 2015: Paul Gastin (LSV) visits S. Krishna and S. Akshay (IIT Bombay) to work on tree automata techniques for timed-systems.

PARSIFAL Project-Team

8. Partnerships and Cooperations

8.1. European Initiatives

8.1.1. FP7 & H2020 Projects

8.1.1.1. Proofcert

Title: ProofCert: Broad Spectrum Proof Certificates

Programm: FP7

Type: ERC

Duration: January 2012 - December 2016

Coordinator: Inria

Inria contact: Dale Miller

'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.'

8.2. International Research Visitors

8.2.1. Visits of International Scientists

Professor Chuck Liang visited the team from 25 May to 15 June 2015 in order to continue his collaborations with team members on basic questions of proof theory. This collaboration resulted in a paper that appears in LPAR 2015 on the topic of subexponentials and the Curry-Howard interpretation of logic.

8.2.1.1. Internships

Leonardo Lima is an intern funded by ProofCert during 1 Oct 2015 – 28 Feb 2016. He is a student of Prof. Vivek Nigam from Federal University of Paraíba, Brazil. He is working on formalizing the proof theory of linear logic within the Abella theorem prover.

8.2.2. Visits to International Teams

8.2.2.1. Research stays abroad

Graham-Lengrand spent 6 months, from March 2015 to August 2015 at SRI International, USA. This visit was to start a collaboration with N. Shankar and B. Dutertre on new algorithms and new architectures for automated and interactive theorem proving.

PI.R2 Project-Team

7. Partnerships and Cooperations

7.1. 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 Baelde 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-year 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 joint 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-year Cathre ANR project, started in January 2014. This project, giving the support for the PhD grant of Maxime Lucas, 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. This project is joint with members of the LAGA (Univ. Paris 13), the LIX (École Polytechnique), the ICJ (Univ. Lyon 1 and Univ. Saint-Étienne), the I2M (Univ. Aix-Marseille) and the IMT (Univ. Toulouse 3).

Pierre-Louis Curien, Yves Guiraud (local coordinator) and Matthieu Sozeau are members of the Groupement de Recherche Topologie Algébrique, federating French researchers working on classical topics of algebraic topology and homological algebra, such as homotopy theory, group homology, K-theory, deformation theory, and on more recent interactions of topology with other themes, such as higher categories, motivic homotopy, string theory.

Matthieu Sozeau, Hugo Herbelin, Lourdes del Carmen González Huesca and Yann Régis-Gianas were members of the ANR Paral-ITP, which started in November 2011 and ended in June 2015, and aimed at 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 and will end mid 2016. Récré is about realisability and rewriting, with applications to proving with side-effects and concurrency.

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.

Yann Régis-Gianas is a member of the ANR COLIS dedicated to the verification of Linux Distribution installation scripts. This project is joint with members of VALS (Univ Paris Sud) and LIFL (Univ Lille).

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. The PhD grant of Gabriel Lewertowski is funded by the CoqHoTT ERC.

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7 & H2020

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.

7.3. International Initiatives

7.3.1. Inria Associate Teams not involved in an Inria International Labs

Pierre-Louis Curien and Claudia Faggian (external collaborator) participate to the Associated Team CRECOGI (Concurrent, Resourceful and Effectful Computation, by Geometry of Interaction) between the project-team Focus (Bologna) and the University of Tokyo (principal investigators Ugo dal Lago and Ichiro Hasuo) (started in 2015).

7.3.2. Inria International Partners

7.3.2.1. Informal International Partners

The project-team has collaborations with University of Aarhus (Denmark), University of Oregon, University of Tokyo, University of Sovi Sad and the Institute of Mathematics of the Serbian Academy of Sciences, University of Nottingham, Institute of Advanced Study, MIT, the University of Cambridge, and Universidad Nacional de Córdoba.

7.3.3. Participation In other International Programs

Pierre-Louis Curien participates to the ANR International French-Chinese project LOCALI (Logical Approach to Novel Computational Paradigms), coordinated by Gilles Dowek.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Andrej Bauer (University of Novi Sad) visited πr^2 and PPS for one month in September 2015 to collaborate with Matthieu Sozeau.

7.4.2. Internships

Akira Yoshimizu had a six-month Inria international internship (Nov 2014 - April 2015). He worked on abstract machines for the geometry of synchronisation, a variation of Girard's geometry of interaction that incorporates synchronisation and that is fit for dealing with quantum primitives added to a functional language, and coauthored a paper at LICS 2015 with Ugo Dal Lago, Claudia Faggian, and Benoît Valiron [56].

SUMO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. 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 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.

9.1.2. 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.

We collaborate with B.Bérard (LIP6) on problems related to security.

We collaborate with Eric Rutten and Gwenael delaval on the control of reconfigurable systems as well as making the ling between Reax and Heptagon / BZR (http://bzr.inria.fr/)

9.2. International Initiatives

9.2.1. Inria International Labs

Éric 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.

9.2.2. Inria Associate Teams not involved in an Inria International Labs

9.2.2.1. DISTOL

Title: Distributed systems, stochastic models and logics

International Partner (Institution - Laboratory - Researcher):

CMI (India) - Madhavan Mukund

Start year: 2013

See also: http://www.irisa.fr/sumo/DISTOL/

The context of this project is formal modeling, and analysis of behaviors of distributed systems. We want to address verification and supervision of distributed systems through formal modeling and automated reasoning on models. By distributed systems, we mean software architectures made of several independent communicating entities. In the 90?s the kind of system addressed was mainly telecommunication protocols. Nowadays, distributed systems are frequently web-based systems such as Web Services, but several aspects of distributed systems can be found in biological applications. Within this context, a challenge is to propose formal tools with potential applications to real systems. We want to address this challenge along three main axes: The first one is realism of models. Models are often an abstraction of real systems. We want to build and study properties of models that are close enough from their implementations, and with robust properties. By robustness, we mean that properties checked on a model (for instance safety properties) should still hold for implementations of this model. The second one is quantitative analysis of systems. Rather that considering boolean answers to formal properties, one can consider the probability that such property holds on a run of the system, and return answers of probabilistic form ("almost surely, a call to a service is successful") or quantitative ("the average failure rate is lower than 0.01"). One possibility to obtain a probability is to compute its exact value. Such questions have answers for markovian models and some quantitative logics (PCTL). However, such computations are expensive, and one can divide the problem into sub-components at the cost of some approximation. We plan to develop efficient algorithms for quantitative analysis of systems. The third one is unification of control theories. There are many proposals for supervisory control, including distributed control with communications. However, none of them seems fully satisfactory. We want to consider connections between control theory, epistemic reasoning (which seems to solve some problems raised by communications between local supervisors), and game theory (which emphasizes the notion of goal to be achieved in a problem), and give a unified framework for supervision of distributed systems.

9.2.3. Inria International Partners

9.2.3.1. Informal International Partners

The team collaborates on runtime enforcement with the group of Prof. Stavros Tripakis (http://users.ics.aalto.fi/stavros/) at Aalto University (Finland), where our former PhD student Srinivas Pinisetty is doing a Post-doc.

In the context of LIRIMA, the Inria International Lab in Africa, we have strong collaborations with University of Yaoundé I on an artifact-centric model of workflow system based on guarded attribute grammars. In particular with the co-supervision of the PhD thesis of Robert Nsaibirni.

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

9.2.4. 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 games. In the context of this project, Miheer Dewaskar, a CMI (Chennai Mathematical Institute) master student did an internship in our team on the control of a population of Markov decision processes.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

S. Akshay visited the SUMO team for three weeks in May 2015.

Robert Nsaibirni (University of Yaoundé) visited SUMO from March to May 2015 on the use of the Guarded Attribute Grammar formalism for the description of the workspaces of actors of a disease surveillance system.

9.3.1.1. Internships

Achille Aknin

Date: May 2015 - July 2015

Institution: ENS Ulm (France)

Alexandre Blanche

Date: May 2015 - July 2015

Institution: ENS Rennes (France)

Miheer Dewaskar

Date: May 2015 - July 2015

Institution: Chennai Mathematical Institute (India)

André Gueney

Date: April 2015 - September 2015

Institution: CNAM (France)

9.3.2. Visits to International Teams

9.3.2.1. Research stays abroad

Eric Fabre visited Michele Pinna during 2 weeks (Univ. of Cagliari, Italy). This collaboration focuses on the design of compact unfoldings for Petri nets.

TOCCATA Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. ELFIC

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

ELFIC is a working group of the Digicosme Labex. S. Boldo is the principal investigator. It began in 2014 for one year and was extended for one year.

The ELFIC project 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).

9.2. National Initiatives

9.2.1. ANR CoLiS

Participants: Claude Marché [contact], Andrei Paskevich.

The CoLiS research project is funded by the programme "Société de l'information et de la communication" of the ANR, for a period of 48 months, starting on October 1st, 2015. http://colis.irif.univ-paris-diderot.fr/

The project aims at developing formal analysis and verification techniques and tools for scripts. These scripts are written in the POSIX or bash shell language. Our objective is to produce, at the end of the project, formal methods and tools allowing to analyze, test, and validate scripts. For this, the project will develop techniques and tools based on deductive verification and tree transducers stemming from the domain of XML documents.

Partners: Université Paris-Diderot, IRIF laboratory (formerly PPS & LIAFA), coordinator ; Inria Lille, team LINKS

9.2.2. ANR Vocal

Participants: Jean-Christophe Filliâtre [contact], Andrei Paskevich.

The Vocal research project is funded by the programme "Société de l'information et de la communication" of the ANR, for a period of 48 months, starting on October 1st, 2015.

The goal of the Vocal project is to develop the first formally verified library of efficient general-purpose data structures and algorithms. It targets the OCaml programming language, which allows for fairly efficient code and offers a simple programming model that eases reasoning about programs. The library will be readily available to implementers of safety-critical OCaml programs, such as Coq, Astrée, or Frama-C. It will provide the essential building blocks needed to significantly decrease the cost of developing safe software. The project intends to combine the strengths of three verification tools, namely Coq, Why3, and CFML. It will use Coq to obtain a common mathematical foundation for program specifications, as well as to verify purely functional components. It will use Why3 to verify a broad range of imperative programs with a high degree of proof automation. Finally, it will use CFML for formal reasoning about effectful higher-order functions and data structures making use of pointers and sharing.

Partners: team Gallium (Inria Paris-Rocquencourt), team DCS (Verimag), TrustInSoft, and OCamlPro.

9.2.3. 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).

9.2.4. 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).

9.2.5. 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.

9.2.6. 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.

9.2.7. 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 of 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 [104]. 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.

9.2.8. 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 and a half, 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, the project keeps 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).

9.3. European Initiatives

9.3.1. 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/.

9.3.2. Collaborations with Major European Organizations

Imperial College London (UK)

Certification of JavaScript, AJACS project

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Andrew Tolmach, from Portland State University, visited the team as a one-year Digiteo Chair, in collaboration with other groups in the Paris area (LRI/Univ. Paris-Sud, LIX/Polytechnique, Inria Saclay and Rocquencourt). The project is to 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 concerning both the use and the development of Coq. Initial results 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 [106].

VERIDIS Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

Participants: Pablo Dobal, Pascal Fontaine.

The PhD thesis of Pablo Federico Dobal was jointly funded by Région Lorraine and the ANR-DFG project SMArT (section 9.2) between September 2014 and August 2015.

9.2. National Initiatives

9.2.1. ANR-DFG Project SMArT

Participants: Haniel Barbosa, David Déharbe, Pablo 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 6.1) is mainly developed by Thomas Sturm. The SMT solver veriT (section 6.4), developed in Nancy, serves as an experimentation platform for theories, techniques and methods designed within this project.

In September 2014, Pablo Federico Dobal was hired as a PhD student in joint supervision with Saarland University, co-funded by the SMArT project and the Région Lorraine. For personal reasons, his thesis has been put on hold in September 2015.

More information on the project can be found on http://smart.gforge.inria.fr/.

9.2.2. ANR Project IMPEX

Participants: Manamiary Andriamiarina, Souad Kherroubi, 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. The work reported here also included a cooperation with Pierre Castéran from LaBRI Bordeaux.

Modeling languages provide techniques and tool support for the design, synthesis, and analysis of the models resulting from a given modeling activity, as part of a system development process. These languages quite successfully focused on the analysis of the designed system exploiting the expressed semantic power of the underlying modeling language. The semantics of this modeling languages are well understood by the system designers and the users of the modeling language, i.e. the semantics is implicit in the model. In general, modeling languages are not equipped with resources, concepts or entities handling explicitly domain engineering features and characteristics (domain knowledge) underlying the modeled systems. Indeed, the designer has to explicitly handle the knowledge resulting from an analysis of this application domain [28], i.e. explicit semantics. Nowadays, making explicit the domain knowledge inside system design models does not obey any methodological rules validated by practice. The users of modeling languages introduce these domain knowledge features through types, constraints, profiles, etc. Our claim is that ontologies are good candidates for handling explicit domain knowledge. They define domain theories and provide resources for uniquely identifying domain knowledge concepts. Therefore, allowing models to make references to ontologies is a modular solution for models to explicitly handle domain knowledge. Overcoming the absence of explicit semantics expression in the modeling languages used to specify systems models will increase the robustness of the designed system models. Indeed, the axioms and theorems resulting from the ontologies can be used to strengthen the properties of the designed models. The objective [13] is to offer rigorous mechanisms for handling domain knowledge in design models.

9.2.3. Inria Technological Development Action CUIC

Participants: Jasmin Christian Blanchette, Simon Cruanes.

Most "theorems" initially given to a proof assistant are incorrect, whether because of a typo, a missing assumption, or a fundamental flaw. Novices and experts alike can enter invalid formulas and find themselves wasting hours, or even days, on an impossible proof. This project, funded by Inria and running from 2015 to 2017, supports the development of a counterexample generator for higher-order logic. This new tool, called Nunchaku, will be integrated in various proof assistants, including Isabelle, Coq, and the TLA$^+$ Proof System. The project is coordinated by Jasmin Blanchette and also involves Inria Saclay (EPI Toccata) and Inria Rennes (EPI Celtique), among others. Simon Cruanes was hired in October 2015 and has started the development of Nunchaku, whereas Blanchette has developed a preliminary version of the Isabelle frontend. We expect a first release in early 2016.

9.2.3.1. Inria ADT PLM (2014-2016)

Participants: Martin Quinson, Matthieu Nicolas.

Joint work with Gérald Oster (project-team Coast, Inria Nancy – Grand Est).

The goal of this project is to establish an experimental platform for studying the didactics of informatics, specifically centered on introductory programming courses.

The project builds upon a pedagogical platform for supervising programming exercises developed for our own teaching, and improves this base in several ways. We want to provide more adapted feedback to the learners, and gather more data to better understand how beginners learn programming.

This year, we heavily refactored the software into a web application, to grow the user community amongst learners and thus gather more learning analytics. We also added the ability to solve PLM exercises by assembling code blocks as in Scratch. Finally, we started working on an integrated exercise editor in the hope of growing the user community amongst teachers that will be able to propose their own exercises on top of PLM.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. MEALS

Title: Mobility between Europe and Argentina applying Logics to Systems

Programm: FP7

Duration: October 2011 – September 2015

Coordinator: Université de la sarre

Partners:

- Imperial College of Science, Technology and Medicine (United Kingdom)
- Rheinisch-Westfälische Technische Hochschule Aachen (Germany)
- Technische Universiteit Eindhoven (Netherlands)
- Technische Universitaet Dresden (Germany)
- University of Leicester (United Kingdom)
- Universität des Saarlandes (Germany)
- Universidad de Buenos Aires (Argentina)
- Universidad Nacional de Córdoba (Argentina)
- Universidad Nacional de Rio Cuarto (Argentina)
- Instituto Tecnológico Buenos Aires (Argentina)

Inria contact: Castuscia Palamidessi

The MEALS project funds staff exchanges between institutions in Europe and Argentina. 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 2015, the project funded visits by Raúl Fervari and Guillaume Hoffmann in Nancy.

9.3.2. Collaborations with Major European Organizations

9.3.2.1. Cooperation with EPFL

Participants: Haniel Barbosa, Jasmin Christian Blanchette, Simon Cruanes, Pascal Fontaine.

We cooperate with Andrew Reynolds from the École polytechnique fédérale de Lausanne, Switzerland, on improving SMT solvers and bridging the gap between SMT solvers and proof assistants. This cooperation started in 2014 between Blanchette and Reynolds and has been pursued in 2015, with mutual one-week visits. The outcomes are manifold:

- We developed a decision procedure that combines reasoning about datatypes and codatatypes and implemented it in the SMT solver CVC4 [31]. This procedure is useful both for proving theorems and for model finding (counterexample generation).
- We designed an encoding of recursive and corecursive function definitions on datatypes and codatatypes that makes it possible to employ finite model finding techniques on functions with infinite domains, as long as they satisfy a wide, semantic criterion [36]. We started the development of a model finder for higher-order logic, called Nunchaku, based on this idea.
- We started work on a general framework for handling quantified formulas in SMT solving. Its focus is on the derivation of instances conflicting with a ground context, redefining the approach introduced by Reynolds et al. [68]. We enhanced the classical congruence closure algorithm so that it can handle free variables [34]. We expect the fruits of this research to be implemented in veriT and CVC4.

9.3.2.2. Cooperation with NUI Maynooth, Ireland

Participant: Dominique Méry.

The project *Building Reliable Systems: Software Refinement meets Software Verification* was a one-year project funded by PHC Ulysses. The academic Irish partner is Rosemary Monahan of NUI Maynooth. The verification of software requires the specification of preconditions and postconditions as well as other properties of the code. These properties are expressed as annotations 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. For validating this methodology, we have designed the Rodin plugin EB2RC that implements transformations of Event-B models into algorithms.

9.4. International Initiatives

9.4.1. Participation In other International Programs

9.4.1.1. STIC AmSud MISMT

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

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 9.3) and extends it to cooperation with UFRN.

The project is centered around Satisfiability Modulo Theories, with a focus on applications to Modal Logic [37]. Notably, the project supports the development of the veriT solver (section 6.4), of which David Déharbe and Pascal Fontaine are the main developers.

The project helped fund the stay of Haniel Barbosa in Natal (PhD in joint supervision between Nancy and Natal) from October to December, 2015. The project has been terminated prematurely due to funding problems.

9.4.1.2. Cooperation with NASA Ames Research Center, U.S.A.

Participant: Dominique Méry.

Joint work with Didier Fass of LORIA, Nancy.

Didier Fass and Dominique Méry have started a close working relationship with Brian Gore and his colleagues at the NASA Ames Reseach Center, Human Systems Integration Division (HSI). It is anticipated that collaboration among the researchers at NASA Ames and LORIA will lead to more formal understanding of the methods required to optimize human-systems integration issues in the design of complex human-automation systems.

CARTE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

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

8.2. National Initiatives

8.2.1. 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 well-known 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.

8.3. International Initiatives

8.3.1. Inria Associate Teams not involved in an Inria International Labs

- Submission of an Inria associate team proposal ACRA (Applications of Complexity to Resource Analysis) in collaboration with Computer Science and Engineering department, State University New York, Buffalo. The french principal investigator is Romain Péchoux, the US principal investigator is Marco Gaboardi.

8.3.2. Participation In other International Programs

- An Hubert Curien Partnership (PHC) PHC Imhotep from the French Ministry of Foreign Affairs and with the support of the French Ministry of National Education and Ministry of Higher Education and Research holds between members of EPC Carte and Alexandria E-Just University.
- Foundations of Quantum Computation: Syntax and Semantics (FoQCoSS), Regional Program STIC-AmSud. This 2-year project has been accepted in late 2015. The Argentinian-Brazilian-French consortium consists of: Pablo ARRIGHI (Université Aix-Marseille, France), Alejandro DIAZ-CARO (Universidad Nacional de Quilmes, Argentina), Gilles DOWEK (Inria, France), Juliana KAIZER VIZZOTTO (Universidade Federal de Santa Maria, Brazil), Simon PERDRIX (CNRS/Carte, France) and Benoît VALIRON (CentraleSupélec – LRI, France). The ultimate goal of this project is to study the foundations of quantum programming languages and related formalisms. With this goal in mind, we will study topics such as parallelism, probabilistic systems, isomorphisms, etc. The interest goes beyond having a working programming language for quantum computing; we are interested, on one hand, in its individual characteristics and its consequences for classical systems, and, on the other hand, in its implications for the foundations of quantum physics.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Walid Gomaa, associate professor at Alexandria E-Just University, was invited during two months (April and November) in the team.
- Daniel Leivant, professor at Indiana University in Bloomington, was invited in June and July.
- Mizuhito Ogawa was invited in the group to discuss about models of self-modifying code based on pushdown automata. He came back in October for further collaboration.

CASSIS Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- ANR SEQUOIA *Security properties, process equivalences and automated verification*, duration: 4 years, starting in October 2014, leader: Steve Kremer. 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.

9.1.2. 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.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

- 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.
- SPOOC (2015–2020)[0]— ERC Consolidator Grant on Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols.

  The goals of the Spooc project are to develop solid foundations and practical tools to analyze and formally prove security properties that ensure the privacy of users as well as techniques for executing protocols on untrusted platforms. We will
  - develop foundations and practical tools for specifying and formally verifying new security properties, in particular privacy properties;
  - develop techniques for the design and automated analysis of protocols that have to be executed on untrusted platforms;
  - apply these methods in particular to novel e-voting protocols, which aim at guaranteeing strong security guarantees without need to trust the voter client software.

[0] http://www.loria.fr/~cortier/ProSecure.html
[0] http://www.loria.fr/~skremer/spooc/index.html

Steve Kremer is the leader of the project.

9.3. International Initiatives

9.3.1. Inria International Partners

- Collaboration with Bogdan Warinschi (Bristol University) on defining game-based privacy for e-voting protocols and isolated execution environments.
- Collaboration with Myrto Arapinis (University of Edinburgh) on simplification results for the formal analysis of e-voting protocols.
- 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.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Carlos Castro (UTSM Valparaíso, Chile), July 2015 - June 2016

COMETE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. Large-scale initiatives

Project acronym: CAPPRIS

Project title: Collaborative Action on the Protection of Privacy Rights in the Information Society

Duration: September 2013 - September 2016

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.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. 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).

8.3. International Initiatives

8.3.1. Inria-MSR joint lab

8.3.1.1. 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.

8.3.2. Inria Associate Teams

8.3.2.1. PRINCESS

Title: Protecting privacy while preserving data access

Inria principal investigator: Catuscia Palamidessi

International Partners:

Geoffrey Smith, Florida International University (United States)

Carroll Morgan, NICTA (Australia)

Annabelle McIver, Maquarie University (Australia)

Duration: 2013 - 2015

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.

8.3.3. Inria International Partners

8.3.3.1. Informal International Partners

Moreno Falaschi, Professor, University of Siena, Italy

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

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

Daniel Gebler, PhD student at the Free University of Amsterdam, The Netherlands

Camilo Rueda, Professor, Universidad Javeriana Cali, Colombia

8.3.4. Participation In other International Programs

8.3.4.1. 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.

8.3.4.2. LOCALI

Program: ANR Blanc International

Project title: Logical Approach to Novel Computational Paradigms

Duration: January 2012 - December 2016

URL: http://www.agence-nationale-recherche.fr/?Project=ANR-11-IS02-0002

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.

8.3.4.3. 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.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Santiago Quintero, Undergraduate Student, Universidad Javeriana Cali, Colombia, Nov 2015 to Dec 2015

Camilo Rueda, Professor, Universidad Javeriana Cali, Colombia, Nov 2015 to Dec 2015

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil, Dec 2015

Annabelle McIver, Associate Professor, Macquarie University, Australia, Dec 2015

Carroll Morgan, Professor, University of New South Wales and NICTA, Australia, Dec 2015

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

8.4.2. Visits to International Teams

Frank Valencia visited the team of Camilo Rueda (AVISPA) at Pontifical Universidad Javeriana Cali, from Feb 2015 until Feb 2015

Frank Valencia visited the team of Camilo Rueda (AVISPA) at Pontifical Universidad Javeriana Cali, from July 2015 until July 2015

DECENTRALISE Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

We obtained ARED funding (40% of a PhD) from the region (starting 11-2015). The focus of the proposed research is how to preserve a free and independent quality press in the age of online distribution. We propose to tackle this challenge from two sides: First, we will broaden the online revenue stream by enabling convenient anonymous payments that preserve the reader's privacy and are more efficient and secure than traditional payment systems. Thus, the resulting system will allow for a larger fraction of the payment to arrive at the newspaper, and for a higher conversion of visitors to purchases. Second, we will consider an alternative means for distributing news, which integrates the typical Web-processes of third parties linking to, commenting on, translating and regurgitating stories while also enabling fair compensation of those involved in the creative process. A key challenge here will be to semi-automate the editorial process, leaving it to readers and decentralized, privacy-preserving algorithms to filter worthwile news. The ideal outcome will be a news distribution system that provides censorship resistance, financial compensation for quality (online) journalism and privacy for readers.

DICE Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. IXXI, Institute for Complex Systems

The Dice team is hosted in the Rhône-Alpes Institute for Complex Systems, IXXI, located in Ecole Normale Supérieure de Lyon. IXXI is promoting trans-disciplinary research, in particular with social sciences, thus facilitating the establishment of connections with researchers in fields such as economics, history, law, etc.

8.1.2. ARC6 "Innovative Services for Social Networks"

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

8.2. National Initiatives

8.2.1. ANR

DICE is involved in an ANR project, which started 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.

8.3. European Initiatives

8.3.1. 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.

8.4. International Initiatives

8.4.1. Inria International Labs

Dice is involved in IPL CityLab@Inria which studies ICT solutions for smart cities. Dice takes part in the *Platforms and City Governance* theme. Dice focuses on analysing and forecasting the role of intermediation platforms in the governance.

8.4.2. Inria International Partners

Dice is associated with the Institute of Massive Computing of ECNU, East China Normal University, in the framework of Joriss, associating ENS with ECNU. The project which focuses on "Promises of intermediation platforms for services frugal in resources" is headed by Aoying ZHOU on the ECNU side.

PRIVATICS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. FUI

8.1.1.1. 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.

8.1.1.2. HuMa

Title: HuMa.

Type: FUI.

Duration: Juin 2015 - Mai 2018.

Coordinator: INTRINSEC.

Others partners: Inria, SYDO, Wallix, INSA Lyon, CASSIDIAN Cybersecurity, Oberthur, INTRINSEC.

Abstract:

The goal of huMa is to improve the tools used to distinguish legitimate network flows from attacks in complex systems including IoT.

8.1.2. ANR

8.1.2.1. 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.

8.1.2.2. 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.

8.1.2.3. 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.

8.1.2.4. 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.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. PRIPARE

Title: PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Programm: FP7

Duration: October 2013 - September 2015

Coordinator: France-Trialog

Inria contact: Daniel Le Métayer

The mission of PRIPARE is twofold: facilitate the application of a privacy and security-by-design methodology that will contribute to the advent of unhindered usage of Internet against disruptions, censorship and surveillance, support its practice by the ICT research community to prepare for industry practice; foster risk management culture through educational material targeted to a diversity of stakeholders. To this end PRIPARE will specify a privacy and security-by-design software and systems engineering methodology, using the combined expertise of the research community and taking into account multiple viewpoints (advocacy, legal, engineering, business), prepare best practices material (guidelines, patterns, success stories) for the development and implementation of products and services of ICT-based systems and use-cases in the area of cloud computing, mobile services and the management of cyber incidents, support FP7 and Horizon 2020 research projects through training workshops and practical support in applying PRIPARE best practices in their environment. It also provides educational material on approaches for risk management of privacy and create awareness on the need for risk management culture among users. Material consistent with PRIPARE methodology will be structured in a modular way in order to fit to different targets (policy makers, users, ICT students and professional). Identify gaps and provide recommendations on privacy and security-by-design practices, support of unhindered usage of Internet and on the creation of a risk management culture. A research agenda will be proposed. PRIPARE consists of a consortium of 11 partners with strong links with the privacy community (data protection authorities/policy makers, privacy advocacy organisations, technology, engineering). In order to prepare for the longer term adoption by the industry, a representative advisory board will be set up. The support action duration is 24 months.

8.2.2. Collaborations in European Programs, except FP7 & H2020

8.2.2.1. COPES

Title: COnsumer-centric Privacy in smart Energy gridS

Programm: CHISTERA

Duration: December 2015 - december 2018

Coordinator: KTH Royal Institute of Technology

Inria contact: Cédric Lauradoux

Smart meters have the capability to measure and record consumption data at a high time resolution and communicate such data to the energy provider. This provides the opportunity to better monitor and control the power grid and to enable demand response at the residential level. This not only improves the reliability of grid operations but also constitutes a key enabler to integrate variable renewable generation, such as wind or solar. However, the communication of high resolution consumption data also poses privacy risks as such data allows the utility, or a third party, to derive detailed information about consumer behavior. Hence, the main research objective of COPES is to develop new technologies to protect consumer privacy, while not sacrificing the ”smartness”, i.e., advanced control and monitoring functionalities. The core idea is to overlay the original consumption pattern with additional physical consumption or generation, thereby hiding the consumer privacy sensitive consumption. The means to achieve this include the usage of storage, small scale distributed generation and/or elastic energy consumptions. Hence, COPES proposes and develops a radically new approach to alter the physical energy flow, instead of purely relying on encryption of meter readings, which provides protection against third party intruders but does not prevent the use of this data by the energy provider.

8.3. Regional Initiatives

8.3.1. 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.

8.3.2. 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.

8.3.3. AMNECYS

- Title: AMNECYS
- Duration: 2015 - .
- Coordinator: CESICE, UPMF.
- Others partners: Inria/Privatics and LIG/Moais, Gipsa-lab, LJK, Institut Fourier, TIMA, Vérimag, LISTIC (Pole MSTIC) .
- Abstract: Privatics participates to the creation of an Alpine Multidisciplinary NEtwork on CYbersecurity Studies (AMNECYS). The academic teams and laboratories participating in this project have already developed great expertise on encryption technologies, vulnerabilities analysis, software engineering, protection of privacy and personal data, international & European aspects of cybersecurity. The first project proposal (ALPEPIC ALPs-Embedded security: Protecting Iot & Critical infrastructure) focuses on the protection of the Internet of Things (IoT) and Critical Infrastructure (CI).

PROSECCO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. 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.

9.1.1.2. 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.

9.1.2. FUI

9.1.2.1. 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

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. CRYSP

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

Programm: FP7

Duration: November 2010 - October 2015

Coordinator: Inria

Inria contact: Anne-Lise Chenet-Pflieger

The goal of CRYSP is to use recent advances in software verification and dependent type systems and apply them to the verification of cryptographic protocol implementations written in a variety of languages. We want to enable the collaborative development of such programs and their specifications. Our target is to be able to verify mainstream implementations of the Transport Layer Security Protocol.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

We have a range of long- and short-term collaborations with various universities and research labs. We summarize them by project:

- **F***: Microsoft Research (Cambdridge, Redmond), IMDEA (Madrid)
- **TLS analysis**: Microsoft Research (Cambridge), Johns Hopkins University, University of Michigan, University of Pennsylvania
- **Web Security**: Microsoft Research (Cambridge, Redmond), Imperial College (London)
- **Micro-Policies**: University of Pennsylvania, Portland State University

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Deepak Garg from the Max Planck Institute for Software Systems in Saarbruecken visited the group from 10-12 June and gave a seminar.
- Udit Dhawan from the University of Pennsylvania visited the group from 10-14 March and gave a seminar.
- Cedric Fournet and Nikhil Swamy from Microsoft Research visited the group multiple times to work on joint projects.