RESEARCH CENTER

FIELD

Algorithmics, Programming, Software and Architecture

Activity Report 2016

Section Partnerships and Cooperations

Edition: 2017-08-25

Algorithmics, Computer Algebra and Cryptology

Architecture, Languages and Compilation

Embedded and Real-time Systems

Proofs and Verification

SECURITY AND CONFIDENTIALITY

ARIC Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

ARC6 PHD PROGRAMME. The PhD grant of Valentina Popescu is funded since September 2014 by Région Rhône-Alpes through the “ARC6” programme.

PALSE PROJECT. Benoît Libert was awarded a 500keur grant (from July 2014 to November 2016) for his PALSE (Programme d’Avenir Lyon Saint-Etienne) project *Towards practical enhanced asymmetric encryption schemes*.

8.2. National Initiatives

8.2.1. ANR HPAC Project

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

“High-performance Algebraic Computing” (HPAC) was a four year ANR project that started in January 2012 and was extended till mid-2016. The final report has been sent in July 2016. The Web page of the project is http://hpac.gforge.inria.fr/. HPAC has been headed by Jean-Guillaume Dumas (CASYS team, LJK laboratory, Grenoble); it was involving 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 was 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 has been 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 has conducted researches along three axes:

- A domain specific parallel language (DSL) adapted to high-performance algebraic computations;
- Parallel linear algebra kernels and higher-level mathematical algorithms and library modules;
- Library composition, their integration into state-of-the-art software, and innovative high-performance solutions for cryptology challenges.

8.2.2. ANR DYNA3S Project

Participants: Guillaume Hanrot, Gilles Villard.

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

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

8.2.3. ANR FastRelax Project

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

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

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

8.2.4. 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.

8.2.5. ANR ALAMBIC Project

Participants: Benoît Libert, Fabien Laguillaumie.

ALAMBIC is a four-year project (started in October 2016) focused on the applications of cryptographic primitives with homomorphic or malleability properties. The web page of the project is https://crypto.di.ens.fr/projects:alambic:description. It is headed by Damien Vergnaud (ENS Paris and CASCADE team) and, besides AriC, also involves teams from the XLIM laboratory (Université de Limoges) and the CASCADE team (ENS Paris). The main goals of the project are: (i) Leveraging the applications of malleable cryptographic primitives in the design of advanced cryptographic protocols which require computations on encrypted data; (ii) Enabling the secure delegation of expensive computations to remote servers in the cloud by using malleable cryptographic primitives; (iii) Designing more powerful zero-knowledge proof systems based on malleable cryptography.

8.3. European Initiatives

8.3.1. 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.

8.4. International Research Visitors

8.4.1. Visiting Scientists

- George Labahn, Professor at U. Waterloo, Ontario, Canada spent the month of April with our team.

- Elena Kirshanova, PhD student at Ruhr-U. Bochum, Germany spent one month with our team, from mid-February to mid-March.
- Jiantao Li, PhD student at East China Normal U., China spends a year with our team. He arrived in September.

8.4.2. Internships

Willy Quach

Date: February 2016–June 2016

Institution: ENS de Lyon

Supervisor: Damien Stehlé

Balthazar Bauer

Date: March 2016–August 2016

Institution: Paris 7

Supervisor: Benoît Libert

Qian Chen

Date: March 2016–August 2016

Institution: ENS Rennes

Supervisors: Fabien Laguillaumie and Benoît Libert

Thi Xuan Vu

Date: May 2016–July 2016

Institution: ENS de Lyon

Supervisors: Claude-Pierre Jeannerod and Vincent Neiger

AROMATH Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Inria SAM Action Transverse

Participants: Paul Görlach, Evelyne Hubert.

Finding biomarkers of abnormalities of the white matter is one important problem in dMRI processing. As these biomarkers need to be independent of the orientation of the head, they are functions of the rotational invariants of the shapes that characterize the diffusion probabilities in the white matter. While the situation is well understood for second order tensors, these are not powerful enough to represent crossings in the white matter. Acquisitions made with the HARDI scheme allow for a richer description of probabilities. In particular, the project-team ATHENA has modelled them as (positive) ternary quartics (symmetric tensors of order 4). But invariants of these quartics are not well known. For a long period, only six were known, when there should be at least 12. Strategies were developed in the project-team ATHENA to compute more invariants, either algebraic [25] or polynomial [21]. The former suffered some instability issues in their evaluations, the latter did not form a minimal set. The goal of this "Transverse action" was to team up with expertise in algebraic computation and leverage the methods [23], [24], [22] [19], [7] developed in the project team AROMATH to gain more insight in this problem of rotational invariants of ternary quartics.

This action is done in collaboration with Théodore Papadopoulo (ATHENA team).

7.1.2. CIMI thematic project

Participant: Evelyne Hubert.

Labex CIMI Toulouse supports the project *Joint Implicit and Parametric Representation based on Skeleton* where the PI are Géraldine Morin (IRIT, Vortex team) and Evelyne Hubert. This project aims at developing a mathematical model and software for surfaces, based on a joint parametric and implicit representation, with a skeleton.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Program: Marie Skłodowska-Curie ITN

Project acronym: ARCADES

Project title: Algebraic Representations in Computer-Aided Design for complEx Shapes

Duration: January 2016 - December 2019

Coordinator: I.Z. Emiris (NKUA, Athens, Greece, and ATHENA Research Innovation Center)

Scientist-in-charge at Inria: L. Busé

Other partners: U. Barcelona (Spain), Inria Sophia-Antipolis (France), J. Kepler University, Linz (Austria), SINTEF Institute, Oslo (Norway), U. Strathclyde, Glascow (UK), Technische U. Wien (Austria), Evolute GmBH, Vienna (Austria).

Webpage: http://arcades-network.eu/

Abstract: ARCADES aims at disrupting the traditional paradigm in Computer-Aided Design (CAD) by exploiting cutting-edge research in mathematics and algorithm design. Geometry is now a critical tool in a large number of key applications; somewhat surprisingly, however, several approaches of the CAD industry are outdated, and 3D geometry processing is becoming increasingly the weak link. This is alarming in sectors where CAD faces new challenges arising from fast point acquisition, big data, and mobile computing, but also in robotics, simulation, animation, fabrication and manufacturing, where CAD strives to address crucial societal and market needs. The challenge taken up by ARCADES is to invert the trend of CAD industry lagging behind mathematical breakthroughs and to build the next generation of CAD software based on strong foundations from algebraic geometry, differential geometry, scientific computing, and algorithm design. Our game-changing methods lead to real-time modelers for architectural geometry and visualisation, to isogeometric and design-through-analysis software for shape optimisation, and marine design & hydrodynamics, and to tools for motion design, robot kinematics, path planning, and control of machining tools.

7.3. International Initiatives

7.3.1. Participation in Other International Programs

7.3.1.1. PICS project

Participant: Laurent Busé.

We participate to a bilateral collaboration between France and Spain which is supported as a PICS from CNRS. This project, titled *Diophantine Geometry and Computer Algebra*, aims at exploring interactions between diophantine geometry and computer algebra by stimulating collaborations between experts in both domains. The research program focuses 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.

The Spanish partner is the University of Barcelona, with participants J. Burgos, C. D'Andrea, Martin Sombra, and the French partners are the university of Caen, with participants F. Amoroso and M. Weimann, the University of Paris 6, with participants M. Chardin and P. Philippon and the Inria project-team AROMATH, with participant L. Busé.

7.3.1.2. SYRAM project

Participants: Laurent Busé, Bernard Mourrain, André Galligo.

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

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 the Inria project-team AROMATH.

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 focuses on rational maps in low dimension, typically parameterizations of curves and surfaces embedded in the projective space of dimension three, 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.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Cordian Riener (University of Konstanz, Germany) visited from September 4-9th, 2016 to collaborate on symmetry, orthogonal polynomials and cubature with Evelyne Hubert and Bernard Mourrain.

Lan Nguyen (University of Vietnam at Hanoï) visited to collaborate on implicitization of rational maps with Laurent Busé. His visits received the financial support of LIAFV (International Laboratory for France-Vietnam collaborations in mathematics).

Aron Simis (University of Pernambuco, Brazil) visited to collaborate on syzygies of rational maps with Laurent Busé.

Nicolas Botbol (Universidad de Buenos Aires, Argentina) visited to collaborate on distance function to rational curves and surfaces with Laurent Busé.

7.4.1.1. Internships

Paul Görlach (University of Bonn) came to work on the *CRISAM - Transverse action* between the project teams AROMATH and ATHENA (August-December).

Akshit Goyal and Deepak Bhatt (IIT Dehli) worked during their internship on “Meshing Singular Isosurfaces” and “Isosurface of the distance function” (May-July).

Antoine Deharveng, student at the engineer school of the University of Nice Sophia Antipolis, came since June 15 to work on the extraction of geometric primitives in a 3D point cloud under the supervision of Laurent Busé.

7.4.2. Visits to International Teams

7.4.2.1. Sabbatical programme

Evelyne Hubert was in Ontario from September 1st 2015 to February 29th 2016, with the sabbatical programme of Inria DPEI. For the period of January and February 2016 she was hosted and supported by University of Waterloo, visiting the Symbolic Computation Lab, and more particularly Pr. George Labahn.

Bernard Mourrain was invited at Univ. of Texas, Austin, for a collaboration with Pr. Chandajit Bajaj (7th-19th May).

CARAMBA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. PEPS JCJC INS2I SPICE

The SPICE proposal ("Systèmes Polynomiaux et calcul d'Indice sur les Courbes Elliptiques : indicateurs de complexité en petite caractéristique") has been accepted in the PEPS JCJC INS2I program in 2016. It involves Pierre-Jean Spaenlehauer (CARAMBA) and Vanessa Vitse (Université Joseph Fourier). This project is coordinated by Vanessa Vitse.

CASCADE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives with Industrials

7.1.1. 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.

7.1.2. CryptoComp

Program: FUI

Duration: October 2014 – November 2018

Coordinator: CryptoExperts

Partners:

CEA

CNRS

Kalray

Inria

Dictao

Université de Limoges

VIACESS

Bertin technologies

GEMALTO

Local coordinator: David Pointcheval

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: ENS Lyon, Université de Limoges

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. 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.

7.2.3. EfTrEC

Title: Efficient Transferable E-Cash

Program: ANR JCJC

Duration: October 2016 – September 2020

PI: Georg Fuchsbauer

Partners:

Univ. Paris 2

This project deals with e-cash systems which let users transfer electronic coins between them offline. The main objectives of this project are:

- establish a clean formal model for the primitive;
- construct schemes which are practically efficient;
- develop schemes that are even resistant to attacks on quantum computers.

7.2.4. ALAMBIC

Title: AppLicAtions of MalleaBIlity in Cryptography

Program: ANR PRC

Duration: October 2016 – September 2020

PI: Damien Vergnaud

Partners:

ENS Lyon

Univ. Limoges

The main objectives of the proposal are the following:

- Define theoretical models for "malleable" cryptographic primitives that capture strong practical attacks (in particular, in the settings of secure computation outsourcing, server-aided cryptography, cloud computing and cryptographic proof systems);
- Analyze the security and efficiency of primitives and constructions that rely on malleability;
- Conceive novel cryptographic primitives and constructions (for secure computation outsourcing, server-aided cryptography, multi-party computation, homomorphic encryption and their applications);
- Implement these new constructions in order to validate their efficiency and effective security.

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: Michel Abdalla

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)

IBM Research Zurich (Switzerland)

Local coordinator: Michel Abdalla

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. International Research Visitors

- Sanjam Garg (UC Berkeley)
- Yuval Ishai (UCLA/Technion)
- Gregory Neven (IBM Zurich)
- Ryo Nishimaki (NTT)
- Claudio Orlandi (Aarhus)
- Rafael Pass (Cornell)
- Leonid Reyzin (Boston University)
- Alessandra Scafuro (postdoc, BU/NEU)
- Victor Shoup (NY University)
- Vinod Vaikuntanathan (MIT)
- Daniel Wichs (Northeastern University)

DATASHAPE Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. ANR TOPDATA

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

- Acronym : TopData.

- Type : ANR blanc.

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

- Coordinator : Frédéric Chazal (DATASHAPE).

- 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. Inria Associate Teams Not Involved in an Inria International Labs

9.3.1.1. 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 (April and November 2016)

Arijit Ghosh, Indian Statistical Institute, Kolkata (April and November 2016)

Jose Carlos Gomez Larranaga, CIMAT, Guanajuato, Mexico (September 2016)

Kim Jisu, CMU, Pittsburgh, USA (May and December 2016).

Antony Bak, Palantir company, USA (October 2016)

9.4.1.1. Internships

Uday Kusupati, Indian Institute of Technology, Bombay (May-July 2016)

Sandip Banerjee (bourse Charpak), Indian Statistical Institute, Kolkata (March-August 2016)

Sameer Desai, Indian Statistical Institute, Kolkata (October-December 2016)

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

Steve Oudot and Jérémy Cochoy spent 3 months (Sept.-Nov.) at the Institute for Computational and Experimental Research in Mathematics (ICERM) at Brown University. They were invited there for the semester program entitled *Topology in Motion* (see https://icerm.brown.edu/programs/sp-f16/).

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 economique de Bitcoin) was accepted as interdisciplinary research for a PEPS (Projet exploratoire Premier Soutien) cofunded by the CNRS and Universite 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.

One M2 intern, E. Palazzollo, was intern in Sceaux, with aim to qualify the nature of bitcoin, as an asset, curency, etc.

This project ended in March 2016

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 [25], 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.

The last year of the 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 [28].

9.1.3. IRT System-X

D. Augot is co-advising a PhD candidate, H.-M. Bisserier, on "les relations contractuelles de droit privé à l'épreuve de la technologie des blockchains", i.e. on (French) law and so-called "smart contracts". D. Augot will mainly help H.-M. Bisserier to clarify the essential computer science topics and issues relevant to the most important blockchains (bitcoin, ethereum). Then H.-M. Bisserier will be advised by C. Zolynksi for remaining two years, fixing research directions.

9.2. National Initiatives

9.2.1. ANR

MANTA (accepted July 2015, starting March 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. The kickoff was a one week-retreat in Dordogne (20 participants), and we had another four day meeting in Saclay in November 17. See http://anr-manta.inria.fr/.

9.2.2. DGA

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.

Our team is engaged in WP3.3 “advanced applications for the cloud”. We envision to focus essentially on secure multiparty computation, essentially the information theoretically secure constructions, who are naturally secure against a quantum computer invoked on classical queries. We will study whether these protocols still resist quantum queries. This work sub package started March 2015, and is dealt with by D. Augot.

7. Partnerships and Cooperations

7.1. National Initiatives

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

Participants: Guilhem Castagnos, Damien Robert.

http://simpatic.orange-labs.fr

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.

The SIMPATIC project has ended in August 2016. The project has shown that pairings can now efficiently be integrated into smart cards publicly deployed, by obtaining performances that outperform the state of the art. Cryptographic tools designed by the project are moreover capable of combining complex functionalities and efficiency in many areas such as digital signatures, minimization of personal data in contactless services, pay TV, or protecting data stored in an untrusted cloud.

7.1.2. ANR Alambic – AppLicAtions of MalleaBIlity in Cryptography

Participant: Guilhem Castagnos.

https://crypto.di.ens.fr/projects:alambic:main

The ALAMBIC project is a research project formed by members of the Inria Project-Team CASCADE of ENS Paris, members of the AriC Inria project-team of ENS Lyon, and members of the CRYPTIS of the university of Limoges. G. Castagnos is an external member of the team of Lyon for this project.

Non-malleability is a security notion for public key cryptographic encryption schemes that ensures that it is infeasible for an adversary to modify ciphertexts into other ciphertexts of messages which are related to the decryption of the first ones. On the other hand, it has been realized that, in specific settings, malleability in cryptographic protocols can actually be a very useful feature. For example, the notion of homomorphic encryption allows specific types of computations to be carried out on ciphertexts and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintexts. The homomorphic property can be used to create secure voting systems, collision-resistant hash functions, private information retrieval schemes, and for fully homomorphic encryption enables widespread use of cloud computing by ensuring the confidentiality of processed data.

The aim of the ALAMBIC project to investigate further theoretical and practical applications of malleability in cryptography. More precisely, this project focuses on three different aspects: secure computation outsourcing and server-aided cryptography, homomorphic encryption and applications and << paradoxical >> applications of malleability.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. ANTICS

Title: Algorithmic Number Theory in Computer Science

Program: 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.'

Title: OpenDreamKit

Program: H2020

Duration: January 2016 - December 2020

Inria contact: Karim Belabas

Description http://cordis.europa.eu/project/rcn/198334_en.html, http://opendreamkit.org

7.3. International Initiatives

7.3.1. Inria International Labs

7.3.1.1. International Laboratory for Research in Computer Science and Applied Mathematics

MACISA

Title: Mathematics Applied to Cryptology and Information Security in Africa

International Partner (Institution - Laboratory - Researcher):

> Université des Sciences et Techniques de Masuku (Gabon) - Faculté des Sciences - Dpt de Mathématiques et Informatique - Tony Ezome

Duration: 2012 - 2016

The projects aims at understanding the role played by algebraic maps in public key cryptography. Since this is a very broad topic, we will focus on objects of dimension zero (finite sets and rings) and one (algebraic curves, their differentials and jacobians). The proposed project-team consists of African and French researchers working in mathematical and statistical aspects of public-key cryptology. The French researchers work in the Inria project-team LFANT in Bordeaux, and the IRMAR (Institut de Recherche en Mathématiques et Applications de Rennes) in Rennes. The African researchers already cooperate in the project PRMAIS (Pole of Research in Mathematics and their Applications in Information Security in Sub-Saharan Africa) supported by the Simons' foundation.

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 Bamenda with the International Center for Pure and Applied Mathematics (ICPAM/CIMPA), June 2016;
- The visit of Abdoulaye Maiga in Bordeaux to work with D. Robert on canonical lifts of genus 2 curves.

2016 was the last year of Macisa. A new project FAST "(Harder Better) FAster STronger cryptography" has been proposed as an associated team between LFANT and the PREMA (Pole of Research in Mathematics and Applications in Africa) Simon's foundation project.

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 Enea Milio (Inria Nancy Grand Est), Gregor Seiler (ETH Zurich), Aurélien Focqué (Industry) and Razvan Barbulescu (University Paris 6). Researchers visting the team for collaboration include Bernadette Perrin-Riou (Paris-Sud).

7.4.2. Visits to International Teams

F. Johansson visited during 1 week the PolSys team at LIP6, Pierre et Marie Curie University.

F. Johansson visited during 1 week (two times) with the Computer Algebra group, TU Kaiserslautern.

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).
- **PIA grant RISQ: Regroupement of the Security Industry for Quantum-Safe security (2017-2020).** The goal of the RISQ project is to prepare the security industry to the upcoming shift of classical cryptography to quantum-safe cryptography. (J.-C. Faugère [contact], and L. Perret).

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: COST

Project acronym: CryptoAction

Project title: Cryptography for Secure Digital Interaction

Duration: 04 2014 - 04 2018

Coordinator: 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.

Program: COST

Project acronym: CRYPTACUS

Project title: Cryptanalysis of ubiquitous computing systems

Duration: 12 2014 - 12 2018

Coordinator: 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.

8.3. International Initiatives

8.3.1. Inria International Labs

8.3.1.1. 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.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Carlos Améndola Cerón

Date: May 2016

Institution: Technische Universität Berlin, Germany

Christoph Koutschan

Date: Nov. 2016

Institution: Österreichische Akademie der Wissenschaften, Linz

Didier Henrion

Date: Nov. 2016

Institution: LAAS, CNRS

Simone Naldi

Date: Nov. 2016

Institution: TU Univ. Dortmund, Germany.

Ioannis Psarros

Date: May. 2016

Institution: University of Athens, Greece.

8.4.1.1. Internships

Vincent Guisse

Date: Apr. 2016 - Jul. 2016

Institution: Université Paris – Diderot

Supervisor: Jean-Charles Faugère, Jérémy Berthomieu

Ramon Ronzon

Date: Mar. 2016 - Sep. 2016

Institution: École polytechnique

Supervisor: Jean-Charles Faugère, Ludovic Perret

Sènan Dossa

Date: Mar. 2016 - Sep. 2016

Institution: ENS Lyon

Supervisor: Jean-Charles Faugère, Ludovic Perret

SECRET Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- **ANR BLOC** $(10/11 \rightarrow 03/16)$
  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** $(12/11 \rightarrow 02/16)$
  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 BRUTUS** $(10/14 \rightarrow 09/18)$
  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.
- **ANR DEREC** $(10/16 \rightarrow 09/21)$
  Relativistic cryptography
  ANR Program: jeunes chercheurs
  244 kEuros
  The goal of project DEREC is to demonstrate the feasibility of guaranteeing the security of some cryptographic protocols using the relativistic paradigm, which states that information propagation is limited by the speed of light. We plan to study some two party primitives such as bit commitment and their security against classical and quantum adversaries in this model. We then plan to the integration of those primitives into larger cryptosystems. Finally, we plan on performing a demonstration of those systems in real life conditions.

9.1.2. Others

- **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.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: Technische Universiteit Eindhoven (NL)

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

Nxp Semiconductors Belgium Nv (Belgium)

Ruhr-Universität 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.

9.2.1.2. QCALL

Title: Quantum Communications for ALL

Programm: H2020-MSCA-ITN-2015

Duration: December 2016 - November 2020

Coordinator: University of Leeds (UK)

Other partners: see http://www.qcall-itn.eu/

Inria contact: Anthony Leverrier

QCALL is a European Innovative Training Network that endeavors to take the next necessary steps to bring the developing quantum technologies closer to the doorsteps of end users. QCALL will empower a nucleus of 15 doctoral researchers in this area to provide secure communications in the European continent and, in the long run, to its connections worldwide.

9.2.2. 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. She co-organized a 2-day workshop for PhD students and early-career researchers in symmetric cryptography, DISC 2016 (Bochum, Germany, March 23-24 2016).

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Declared Inria International Partners

Title: Discrete Mathematics, Codes and Cryptography

International Partner (Institution - Laboratory - Researcher):

Indian Statistical Institute (India) - Cryptology Research Group - Bimal Roy

Duration: 2014 - 2018

Start year: 2014

Today's cryptology offers important challenges. Some are well-known: Can we understand existing cryptanalysis techniques well enough to devise criterion for the design of efficient and secure symmetric cryptographic primitives? Can we propose cryptographic protocols which offer provable security features under some reasonable algorithmic assumptions? Some are newer: How could we overcome the possible apparition of a quantum computer with its devastating consequences on public key cryptography as it is used today? Those challenges must be addressed, and some of the answers will involve tools borrowed to discrete mathematics, combinatorics, algebraic coding theory, algorithmic. The guideline of this proposal is to explore further and enrich the already well established connections between those scientific domains and their applications to cryptography and its challenges.

9.3.1.2. 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.
- Ruhr-Universität Bochum (Germany): design and cryptanalysis of symmetric primitives.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Leo Perrin, University of Luxemburg, visiting PhD student, June 2016.
- Thomas Peyrin, NTU Singapore, visiting scientist, Feb.-March 2016 and June 2016.

9.4.1.1. Internships

- Xavier Bonnetain, MPRI and Telecom ParisTech, March-Aug. 2016
- Rémi Bricout, MPRI and ENS Paris, March-Aug. 2016
- Thomas Debris, MPRI and ENS Cachan, March-Aug. 2016
- Ghazal Kachigar, Master cryptographie et mathématiques de l'information, Univ. Rennes, March-Sept. 2016
- Vivien Londe, Master de mathématiques, UPMC, April-July 2016

9.4.2. Visits to International Teams

9.4.2.1. Short Research Stays Abroad

- Ruhr-Universität Bochum, Bochum, Germany, January 18-22, work with Gregor Leander (G. Leurent)
- Instituto Superior Tecnico, Lisbon, Portugal, May 18-20, 2016, invitation to visit the group of quantum computation of Paulo Mateus (A. Leverrier)
- University of Oxford Mathematical Institute, Oxford, UK, May 25-26, invitation to the cryptography seminar (G. Leurent)

SPECFUN Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

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: Assia 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.

8.3. International Research Visitors

8.3.1. Research Stays Abroad

- Thomas Sibut-Pinote has spent two months at Microsoft Research Cambridge, visiting Georges Gonthier and working on mathematical libraries for the Lean proof assistant. He also participated in a hackathon internal to Microsoft Research with the goal to apply formal methods to the verification of the smart contracts involved in the Ethereum framework for cryptocurrency.

VEGAS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

We organized, with IECL, a «journée Charles Hermite» about geometry and probability. A regular working group on the topic was started in november.

8.2. National Initiatives

8.2.1. 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 ended in March 2016. It is coordinated by Xavier Goaoc who moved from the Vegas team to Marne-la-Vallée university in 2013.

Project website: https://members.loria.fr/GMoroz/ANR-Presage/.

8.2.2. 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.

The project funded the postdoc position of Rémi Imbach from November 2014 until October 2016. We organized two workshops in 2016 with the OPTI team in Nantes, on certified surface continuation.

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

8.3. International Initiatives

8.3.1. Participation in Other International Programs

8.3.1.1. Nancy Emerging Associate Team Astonishing

The objectives of the *ASsociate Team On Non-ISH euclIdeaN Geometry* is to study various structures and algorithms in non-Euclidean spaces, from a computational geometry viewpoint. Proposing algorithms operating in such spaces requires a prior deep study of the mathematical properties of the objects considered, which raises new fundamental and difficult questions that we want to tackle.

A key characteristic of the project is its interdisciplinarity: it gathers approaches, knowledge, and tools in mathematics and computer science. A mathematical study of the considered objects will be performed, together with the design of algorithms when applicable. Algorithms will be analyzed both in theory and in practice after prototype implementations. In the long term, implementations should be improved whenever it makes sense to target longer-term integrations into CGAL, in order to disseminate our results to end-users.

The partners are the Johann Bernouilli Institute of Mathematics and Computer Science of University of Groningen, the Mathematics Research Unit of University of Luxembourg, and the Talgo team of École Normale Supérieure. The project is coordinated by Monique Teillaud and supported by Inria Nancy - Grand Est.

Project website: https://members.loria.fr/Monique.Teillaud/collab/Astonishing/.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Invited Professor

Gert Vegter, Professor at Univerity of Groningen, was awarded an invited professor position by University of Lorraine and spent one month in the group in May. He is coordinating the NEAT Astonishing on the Dutch side.

8.4.1.2. PhD Visitor

Sény Diatta, Senegalese PhD student co-advised by Guillaume Moroz, Daouda Niang Diatta (Ziguinchor) and Marie-Françoise Roy (Rennes), obtained a bourse Eiffel from Campus France, which includes a salary for 10 months to visit LORIA.

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

Iordan Iordanov spent one month at University of Luxembourg in June. The visit was partially supported by by University of Luxembourg and by the NEAT Astonishing.

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 CAIRN and 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. CAIRN goal is the technological transfer of the methods proposed by the team that enable the rapid prototyping of digital radios.

8.2. National Initiatives

8.2.1. ANR Blanc - PAVOIS (2012–2016)

Participants: Arnaud Tisserand, Emmanuel Casseau, Jérémie Métairie, Karim Bigou, Pierre Guilloux.

PAVOIS is a project on Arithmetic Protections Against Physical Attacks for Elliptic Curve based Cryptography that will provide novel implementations of curve based cryptographic algorithms on custom hardware platforms. A specific focus is placed on trade-offs between efficiency and robustness against physical attacks. It involves IRISA-CAIRN (Lannion) and LIRMM (Perpignan and Montpellier). Theoretical aspects 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 design innovative cryptographic hardware architectures of a specific processor based on the theoretical advancements described above to implement curve based protocols. For more details see http://pavois.irisa.fr.

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

Participants: Arnaud Tisserand, Pierre Guilloux.

ARDyT 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. For more details see http://ardyt.irisa.fr.

8.2.3. Labex CominLabs - BoWI (2012-2016)

Participants: Olivier Sentieys, Arnaud Carer.

The BoWi project (Body Wold Interactions) project aims at designing an accurate gesture and body movement estimation using very-small and low-power wearable sensor nodes, to propose pioneer interfaces for an emerging interacting world based on smart environments (house, media, information and entertainment systems...). Relying on Wireless Body Areas Sensor Networks, we propose an accurate Gesture and Body Movement estimation with extremely severe constraints in terms of footprint and energy consumption. The BoWI geolocation approach will combine radio communication distance measurement and inertial sensors and will also strongly benefit from cooperative techniques based on multiple observations and distributed computation. Different types of applications, such as health care, activity monitoring and environment control, are considered and prototyped. BoWI involves CAIRN, IRISA Granit (Lannion), IETR (Rennes), and Lab-STICC (Brest, Lorient, Vannes). For more details see http://www.bowi.cominlabs.ueb.eu.

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

Participants: Olivier Sentieys, Daniel Chillet, Cédric Killian, Jiating Luo, Van Dung Pham, Ashraf El-Antably.

3DCORE (3D Many-Core Architectures based on Optical Network on Chip) is a project investigating new solutions based on silicon photonics 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. Moreover, 3DCore will take advantage of 3D technologies to design a specific optical layer suitable for a flexible and energy efficient high-speed optical network on chip (ONoC). 3DCORE involves CAIRN, FOTON (Rennes, Lannion) and Institut des Nanotechnologies de Lyon. For more details see http://www.3d-opt-many-cores.cominlabs.ueb.eu.

8.2.5. Labex CominLabs - RELIASIC (2014-2018)

Participants: Emmanuel Casseau, Arnaud Tisserand.

RELIASIC (Reliable Asic) will address the issue of fault-tolerant computation 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. RELIASIC involves CAIRN, Lab-STICC (Lorient) and IETR (Rennes). For more details see http://www.reliasic.cominlabs.ueb.eu In this project, CAIRN is in charge of the analysis and design of arithmetic operators for fault tolerance. We focus on the hardware implementations of conventional arithmetic operators such as adders, multipliers and MACs but also higher level operators like butterfly computation operator for FFT algorithm.

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

Participants: Arnaud Tisserand, Karim Bigou, Gabriel Gallin, Audrey Lucas.

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 will provide novel implementations of HECC based cryptographic algorithms on custom hardware platforms. H-A-H involves CAIRN (Lannion) and IRMAR (Rennes). For more details see http://h-a-h.inria.fr/.

8.3. European Initiatives

8.3.1. H2020 ARGO

Participants: Steven Derrien, Olivier Sentieys, Imen Fassi, Ali Hassan El-Moussawi.

Program: H2020-ICT-04-2015

Project acronym: ARGO

Project title: WCET-Aware Parallelization of Model-Based Applications for Heterogeneous Parallel Systems

Duration: Feb. 2016 - Feb. 2019

Coordinator: KIT

Other partners: KIT (DE), UR1/Inria/CAIRN (FR), Recore Systems (NL), TEI-WG (GR), Scilab Ent. (FR), Absint (DE), DLR (DE), Fraunhofer (DE)

Increasing performance and reducing cost, while maintaining safety levels and programmability are the key demands for embedded and cyber-physical systems, 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 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 cross-layer 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.

8.3.2. ANR International ARTEFaCT

Participants: Olivier Sentieys, Benjamin Barrois, Tara Petric, Tomofumi Yuki.

Program: ANR International France-Switzerland

Project acronym: ARTEFaCT

Project title: AppRoximaTivE Flexible Circuits and Computing for IoT

Duration: Feb. 2016 - Dec. 2019

Coordinator: CEA

Other partners: CEA-LETI (FR), CAIRN (FR), EPFL (SW)

The ARTEFaCT project aims to build on the preliminary results on inexact and exact near-threshold and sub-threshold circuit design to achieve major energy consumption reductions by enabling adaptive accuracy control of applications. ARTEFaCT proposes to address, in a consistent fashion, the entire design stack, from physical hardware design, up to software application analysis, compiler optimizations, and dynamic energy management. We do believe that combining sub-near-threshold with inexact circuits on the hardware side and, in addition, extending this with intelligent and adaptive power management on the software side will produce outstanding results in terms of energy reduction, i.e., at least one order of magnitude, in IoT applications. The project will contribute along three research directions: (1) approximate, ultra low-power circuit design, (2) modeling and analysis of variable levels of computation precision in applications, and (3) accuracy-energy trade- offs in software.

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) - Reconfigurable Computing Group - Russel Tessier

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 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. HARAMCOP

Title: Hardware accelerators modeling using constraint-based programming

International Partner (Institution - Laboratory - Researcher):

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

8.4.2.1.3. 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), Fault-tolerant computing architectures.

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

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, Worst-Case Execution Time, 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. Maciej Cieselski, University of Massachusetts, Amherst, US, for three weeks in July. This visit was partly funded by HARDIESSE Inria Associate Team.

Prof. Daniel Massicotte, Université du Québec à Trois-Rivières, CA, for three weeks in December. This visit was funded by ISTIC.

Maroua Gam, LabTim (Technologie Imagerie Médicale), Monastir, Tunisia, for one month in March.

8.5.2. Visits to International Teams

Angeliki Kritikakou visited University of Patras, Greece, for 1 week in November. This visit was funded by U. Rennes 1.

Patrice Quinton visited University of Massachusetts, Amherst, US, for 1 week in December. This visit was funded by HARDIESSE Inria Associate Team.

Tomofumi Yuki visited University of Arizona, US, in June.

8.5.2.1. Sabbatical programme

Casseau Emmanuel

Date: Aug 2016 - Jul 2017

Institution: University of Auckland (New Zealand), Parallel and Reconfigurable Research Lab. of the Electrical and Computer Engineering department.

The goal of the project is to propose dynamic mapping and scheduling algorithms dedicated to unreliable heterogeneous platforms, enabling self-adaptive and resource-aware computing.

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 PACAP, 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
- University of Batna, Algeria
- Ohio State University, Colombus, USA
- Louisiana State University, Baton Rouge, USA
- Colorado State University, Fort Collins, USA
- Indian Institute of Science (IIIS) Bangalore, India

9.3. International Research Visitors

9.3.1. Visits of International Scientists

9.3.1.1. Researchers

Rachid Seghir

Date: April 30 - May 14

Institution: University of Batna, Algeria

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

COMPSYS Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

Compsys followed or participated 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 had organized in 2013 a thematic quarter on compilation (http://labexcompilation.ens-lyon.fr). A second thematic quarter on high performance computing (HPC) was organized in 2016, initiated by Violaine Louvet (Institute Camille Jordan), with the participation of the LIP teams Aric, Avalon, Compsys, and Roma. Among other events, it included a CNRS inter-disciplinary spring school (https://mathsinfohpc.sciencesconf.org) co-organized by Compsys, connecting mathematics (HPC numerical analysis) and computer science (polyhedral optimizations for HPC) that can be seen as a follow-up of the first polyhedral school organized by Compsys in 2013. See details in Section 10.1 .

Alain Darte, Alexandre Isoard, and Tomofumi Yuki had also some 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.

9.2. 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 11th event has been organized in Sep. 2016). The community is animated by Laure Gonnord and Fabrice Rastello since 2010, and now also by Florian Brandner (ex-Compsys too). Alain Darte and Tomofumi Yuki participated to the 11th edition.

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 half-day lecture at the 2016 edition (http://ejcp2016.univ-lille1.fr/), following his 2015 course.

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 previous reports). The results of Sections 7.2 and 7.1 are related to this collaboration. Now that Compsys has been stopped, Paul Feautrier is affiliated to Parkas, in addition to his emeritus position at ENS-Lyon.

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 7.5 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). The main result has been the determination of the *happens before* relation of clocked X10, a prerequisite for the detection of races in clocked programs. The resulting formula has been proved correct using the Coq proof assistant. Publishing formal proofs is known to be difficult, but we will give it a try soon.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

After the participation to a (rejected) H2020 proposal in 2015, Compsys did not try any effort in this direction as the team was going to be stopped.

9.3.2. Collaborations in European Programs, Except FP7 & H2020

Same situation.

9.3.3. 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), 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. Collaboration with Colorado State University

Compsys had always kept strong connections with Colorado State University (CSU):

- In July 2016, Guillaume Iooss defended his joint ENS-Lyon/CSU PhD thesis [16]. He was co-advised by both Sanjay Rajopadhye (CSU) and Christophe Alias (with supplementary support by Alain Darte for administrative reason, as he has no HDR yet).
- Tomofumi Yuki, who did his PhD with Sanjay Rajopadhye, then a post-doc in the Cairn team in Rennes, continued his collaboration with these two groups, as the results described in Section 7.5 illustrate. He also participates regularly, over the net, to the reading group "Melange" of S. Rajodapdhye's group, with CSU students. Due to the stop of Compsys, Tomofumi Yuki has now returned to the Cairn team.
- Waruna Ranasinghe, a PhD student from S. Rajopadhye's team, visited Compsys, to work with Tomofumi Yuki, for 2 months (see Section 9.5).

9.4.2. Polyhedral Community

In 2011, as part of the organization of the workshops at CGO'11, Christophe Alias (with Cédric 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 of the 2015 edition in Amsterdam, and Tomofumi Yuki of the 2016 edition in Prague.

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 by Alain Darte of the first school on polyhedral code analysis and optimizations (http://labexcompilation.ens-lyon.fr/polyhedral-school/). A second polyhedral school (https://mathsinfohpc.sciencesconf.org), more open, because involving themes and researchers from numerical analysis (users of HPC), was organized in 2016 by Alain Darte (for the compiler side) and Violaine Louvet (for the HPC side). See details in Section 10.1 .

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 7.7 .

9.5. International Research Visitors

9.5.1. Visits of International Scientists

9.5.1.1. Visiting PhD students

- Emna Hammami (Tunis University, with Yosr Slama) visited Compsys from April to June 2016 to refine her PhD topic with Compsys members. She also participated to the spring school on numerical simulation and polyhedral compilation.
- Waruna Ranasinghe (Colorado State University, with Sanjay Rajopadhye) visited Compsys from end of June to mid August 2016 to work with Tomofumi Yuki on extending cache oblivious techniques to polyhedral programs.

9.5.1.2. Internships

- Julien Versaci, M2 student from Lyon 1 University, from both physics and computer science departments, worked from April to June 2016 in Compsys, to work on the parallelization of a model of quantum physics. Julien was co-supervised by Jean-Philippe Guillet (physicist) and Tomofumi Yuki, the second part of his internship (until mid August) being done affiliated to Annecy physics laboratory (LAPTH). Julien also participated to the spring school on numerical simulation and polyhedral compilation.

9.5.2. Visits to International Teams

No long (more than one month) stay abroad in 2016.

CORSE Project-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.

8.1.3. AGIR DEREVES

- Title: DEcentralised Runtime Verification and Enforcement of distributed and cyber-physical Systems
- DEREVES leader: Ylies Falcone
- CORSE participants: Ylies Falcone, Antoine El-Hokayem, Raphaël Jakse
- DEREVES aims at advancing the theory of decentralised runtime verification and enforce- ment for distributed systems, with the objective of proposing realistic monitoring and monitor-synthesis algorithms for expressive specifications that can be used for the efficient monitoring of multi-threaded, dis- tributed and cyber-physical systems. The project shall help transferring runtime verification and enforcement to a wider audience of programmers of distributed systems by providing them techniques and tools to help them guaranteeing the correctness of their systems.

8.2. National Initiatives

8.2.1. IPL C2S@Exa

- Title: Computer and Computational Sciences at Exascale
- C2S@Exa leader: Stéphane Lanteri
- CORSE participants: François Broquedis, Frédéric Desprez, Jean-François Méhaut, Brice Videau, Philippe Virouleau, Nora Hagmeyer

- 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.

8.2.2. 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-Blanc2

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

Program FP7

Duration: 01/10/2013 - 31/01/2017

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.

8.3.1.2. EoCoE

Title: Energy oriented Centre of Excellence for computer applications

Programm: H2020

Duration: October 2015 - October 2018

Coordinator: CEA

Partners:

Barcelona Supercomputing Center - Centro Nacional de Supercomputacion (Spain)

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

Centre Europeen de Recherche et de Formation Avancee en Calcul Scientifique (France)

Consiglio Nazionale Delle Ricerche (Italy)

The Cyprus Institute (Cyprus)

Agenzia Nazionale Per le Nuove Tecnologie, l'energia E Lo Sviluppo Economico Sostenibile (Italy)

Fraunhofer Gesellschaft Zur Forderung Der Angewandten Forschung Ev (Germany)

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk (Poland)

Forschungszentrum Julich (Germany)

Max Planck Gesellschaft Zur Foerderung Der Wissenschaften E.V. (Germany)

University of Bath (United Kingdom)

Universite Libre de Bruxelles (Belgium)

Universita Degli Studi di Trento (Italy)

Inria contact: Michel Kern

The aim of the present proposal is to establish 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.

8.3.1.3. HPC4E

Title: HPC for Energy (HPC4E)

Programm: H2020

Duration: December 2015 - November 2017

Program FP7

Coordinator: Barcelona Supercomputing Center

Partners:

Centro de Investigaciones Energeticas, Medioambientales Y Tecnologicas-Ciemat (Spain)

Iberdrola Renovables Energia (Spain)

Repsol (Spain)

Total S.A. (France)

Lancaster University (United Kingdom)

Inria contact: Stephane Lanteri

CORSE particpants: Jean-François Méhaut, Frédéric Desprez, Emmanuelle Saillard (Post-Doct since Dec 2016)

This project aims to apply the new exascale HPC techniques to energy industry simulations, customizing them, and going beyond the state-of-the-art in the required HPC exascale simulations for different energy sources: wind energy production and design, efficient combustion systems for biomass-derived fuels (biogas), and exploration geophysics for hydrocarbon reservoirs. For wind energy industry HPC is a must. The competitiveness of wind farms can be guaranteed only with accurate wind resource assessment, farm design and short-term micro-scale wind simulations to forecast the daily power production. The use of CFD LES models to analyse atmospheric flow in a wind farm capturing turbine wakes and array effects requires exascale HPC systems. Biogas, i.e. biomass-derived fuels by anaerobic digestion of organic wastes, is attractive because of its wide availability, renewability and reduction of CO2 emissions, contribution to diversification of energy supply, rural development, and it does not compete with feed and food feedstock. However, its use in practical systems is still limited since the complex fuel composition might lead to unpredictable combustion performance and instabilities in industrial combustors. The next generation of exascale HPC systems will be able to run combustion simulations in parameter regimes relevant to industrial applications using alternative fuels, which is required to design efficient furnaces, engines, clean burning vehicles and power plants. One of the main HPC consumers is the oil & gas (O&G) industry. The computational requirements arising from full wave-form modelling and inversion of seismic and electromagnetic data is ensuring that the O&G industry will be an early adopter of exascale computing technologies. By taking into account the complete physics of waves in the subsurface, imaging tools are able to reveal information about the Earth's interior with unprecedented quality.

8.3.2. Collaborations in European Programs, Except FP7 & H2020

Program: COST

Project acronym: ArVI

Project title: Runtime Verification beyond Monitoring

Duration: December 2014 - May 2017

Coordinator: Martin Leucker, University of Lubeck

Abstract: Runtime verification (RV) is a computing analysis paradigm based on observing a system at runtime to check its expected behavior. RV has emerged in recent years as a practical application of formal verification, and a less ad-hoc approach to conventional testing by building monitors from formal specifications.

There is a great potential applicability of RV beyond software reliability, if one allows monitors to interact back with the observed system, and generalizes to new domains beyond computers programs (like hardware, devices, cloud computing and even human centric systems). Given the European leadership in computer based industries, novel applications of RV to these areas can have an enormous impact in terms of the new class of designs enabled and their reliability and cost effectiveness.

This Action aims to build expertise by putting together active researchers in different aspects of runtime verification, and meeting with experts from potential application disciplines. The main goal is to overcome the fragmentation of RV research by (1) the design of common input formats for tool cooperation and comparison; (2) the evaluation of different tools, building a growing sets benchmarks and running tool competitions; and (3) by designing a road-map and grand challenges extracted from application domains.

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.

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 (LIG, UFRGS Brazil)
- EnergySFE (STIC Amsud)
  - Leader: University Federal of Santa Catarina (UFSC): Màrcio Castro
  - Partners: UFSC (Florianapolis, Brazil), UFRGS (Porto Alegre, Brazil), ESPE (Ecuador), CNRS (LIG/CORSE, TIMA, LSPSC)
  - Duration: January 2016 - December 2017
  - CORSE participants: Jean-François Méhaut, François Broquedis, Frédéric Desprez
  - The main goal of the EnergySFE research project is to propose fast and scalable energy-aware scheduling and fault tolerance techniques and algorithms for large-scale highly parallel architectures. To achieve this goal, it will be crucial to answer the following research questions:

- How to schedule tasks and threads that compete for resources with different constraints while considering the complex hierarchical organization of future Exascale supercomputers?
- How to tolerate faults without incurring in too much overhead in future Exascale supercomputers?
- How scheduling and fault tolerance approaches can be adapted to be energy-aware?

The first EnergySFE workshop was organized by the CORSE team a the Inria Minatec building in September 2016.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Louis-Noël Pouchet (OSU), visited CORSE two times one month
- Julien Langou (UCDenver) is visiting professor since September 2016
- Mohamad Jaber (AUB) visited CORSE two weeks in January 2016
- Sylvain Hallé (U of Québec) visited CORSE one week in August 2016
- Christian Colombo (U of Malta) visited CORSE two weeks in March 2016
- Henrique Freitas (PUC Minas) visited CORSE one year since July 2015 until July 2016

7. Partnerships and Cooperations

7.1. International Initiatives

7.1.1. Inria International Partners

7.1.1.1. Informal International Partners

In 2016 we have continued our strong and long-term collaboration with Prof. Dorel Lucanu's group Univ. Iasi as witnessed by the co-authored publications (3 journals and 1 conference). Vlad Rusu serves as "external advisor for PhD students" in Prof. Lucanu's group. In 2016 we have also had notable interactions with Prof. José Meseguer (Univ. Illinois at Urbana Champaign, USA), which consisted in sharing ideas and mutual reading and commenting advanced drafts prior to submission in journals/conferences.

PACAP 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, Viet Anh Nguyen, Sébastien Martinez.

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 at Work, Dassault Aviation, Eurocopter, MBDA, ProbaYes, IRIT, Onera, Verimag, Inria, Irisa, Tima and Armines.

9.1.2. Multicore: Inria Project Lab, 2013-2016

Participants: Erven Rohou, Nabil Hallou.

Multicore is an Inria Project Lab (IPL, formerly *Action d'Envergure*) started in 2013. It is entitled "Large scale multicore virtualization for performance scaling and portability". Partner project-teams include: PACAP, 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. ANR Continuum 2015–2019

Participants: Erven Rohou, Rabab Bouziane.

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.

9.1.4. ANR CHIST-ERA SECODE 2016-2018

Participants: Nicolas Kiss, Damien Hardy, Erven Rohou.

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).

9.1.5. ANR W-SEPT 2012-2016

Participants: 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.

9.1.6. PEPS INS2I gDGA

Participant: Sylvain Collange.

This interdisciplinary project aims at extending the definition and the range of applicability of distance geometry, with a particular attention to its discretization. As it is already possible to remark from recent publications in the scientific literature, the distance geometry can nowadays be seen as a classical problem in operational research, with a wide range of potential applications. Among the possible extensions, this project will mainly focus on dynamical problems, motivated by a certain number of novel applications that we have identified. These include interaction motion adaptation, the simulation of crowd behaviors, and the conception of recommender systems that are able to satisfy modern privacy regulations. The classical application of the distance geometry arising in the biological field will also be considered in this project. The necessity of a strong computational power for the mentioned applications motivates the need of implementing our algorithms in environments capable of exploiting the resources in GPU cards.

Partners are: Inria, Unviersité de Rennes 2, INSA Rennes, Université d'Avignon, CNRS.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. ANTAREX

Participants: Erven Rohou, Imane Lasri.

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)

Dompé Farmaceutici Spa (Italy)

Eidgenoessische Technische Hochschule Zürich (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)

École Polytechnique Federale de Lausanne (Switzerland)

Foundation for Research and Technology Hellas (Greece)

Universität 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, Sylvain Collange, Erven Rohou, André Seznec, Arthur Perais, Sajith Kalathingal, 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.

Argo also involves Steven Derrien, Angeliki Kritikakou, and Imen Fassi from the CAIRN team.

9.2.2. Collaborations in European Programs, Except FP7 & H2020

9.2.2.1. COST Action TACLe - Timing Analysis on Code-Level 10-2012/09-2016

Participants: Damien Hardy, Isabelle Puaut, Benjamin Rouxel.

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. HiPEAC4 NoE

Participants: Pierre Michaud, Erven Rohou, André Seznec.

P. Michaud, A. Seznec and E. Rohou are members of the European Network of Excellence HiPEAC4.

HiPEAC4 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. PHC IMHOTEP

Participant: Erven Rohou.

Title: Thoth – An Automatic Dynamic Binary Parallelisation System

International Partner (Institution - Laboratory - Researcher):

Egypt-Japan University of Science and Technology - Prof. Ahmed ElMahdy.

Dates: 2016–2017

With the current global trend towards utilizing cloud computing and smart devices, executing the same application across becomes a necessity. Moreover, parallelism is now abundant with various forms that include thread- and data-parallel execution models. Such diversity in ISA and explicit parallelism makes software development cost prohibitive, especially for natively optimized binaries. This project leverages dynamic binary translation technology to provide for exploiting the underlying parallel resources without the need of having the source code of the application. In particular the project integrates low overhead dynamic profiling, novel OSR parallel de-optimization and a retargetable parallelization modules to allow for dynamic parallelization of binaries.

9.3.2. Inria Associate Teams Not Involved in an Inria International Labs

9.3.2.1. PROSPIEL

Participant: Sylvain Collange.

Title: Profiling and specialization for locality

International Partner (Institution - Laboratory - Researcher):

Universidade Federal de Minas Gerais (Brazil) - DCC - Fernando Magno Quintão Pereira

Start year: 2015

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

9.3.3. Inria International Partners

9.3.3.1. Informal International Partners

The PACAP 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 Uppsala (Pr Hagersten), University of Cyprus (Pr Sazeides), the Egyptian-Japanese University of Science and Technology (Pr Ahmed El-Mahdy), Intel Haifa (Dr Zaks, Eng Nuzman), Barcelona Supercomputing Center (Dr Cazorla, Dr Abella), ISEP Porto (Dr Nelissen, Dr Nélis).

9.4. International Research Visitors

9.4.1. Visits of International Scientists

9.4.1.1. Internships

Rubens Emilio Alves Moreira, student at Universidade Federal de Minas Gerais, visited from Feb 2016 to May 2016 within the context of the PROSPIEL associated team.

Stefano Cherubin, PhD student at Politecnico di Milano for one month in Oct 2016, within the context of the ANTAREX H2020 project.

Anita Tino, PhD student at Ryerson University, visited from Oct 2016 within the context of a MITACS grant.

TASC Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. EPOC

With the emergence of the Future Internet and the dawning of new IT models such as cloud computing, the usage of data centers (DC), and consequently their power consumption, increase dramatically. Besides the ecological impact, the energy consumption is a predominant criteria for DC providers since it determines the daily cost of their infrastructure. As a consequence, power management becomes one of the main challenges for DC infrastructures and more generally for large-scale distributed systems. In this paper, the EPOC project which focuses on optimising the energy consumption of mono-site DCs connected to the regular electrical grid and to renewable energy sources.

9.1.2. 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.

9.1.3. Atlanstic 1

Participant: Florian Richoux.

Title: Atlanstic project about deep learning for games.

Duration: 2016.

Topic: deep learning for games.

9.1.4. Atlanstic 2

Participant: Charles Prud Homme.

Title: CoMe4ACloud.

Duration: 2016.

Topic: CoMe4ACloud is an Atlanstic2020 funded project whose objective is to provide an end-to-end solution for autonomic Cloud services. To that end, we rely on techniques of Constraint Programming so as a decision-making tool and Model-driven Engineering to ease the automatic generation of the so-called autonomic managers as well as their communication with the managed system (see Constraints and Model Engineering for Autonomic Clouds). The project is led by ASCOLA research team and involves also AtlanModels and TASC.

9.2. National Initiatives

9.2.1. 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 responsible for the constraint part. To interact with policy makers it uses some qualitative network model (see Figure 10) embedded with constraint programming models that also capture dependancy between potential actions as well as costs.

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

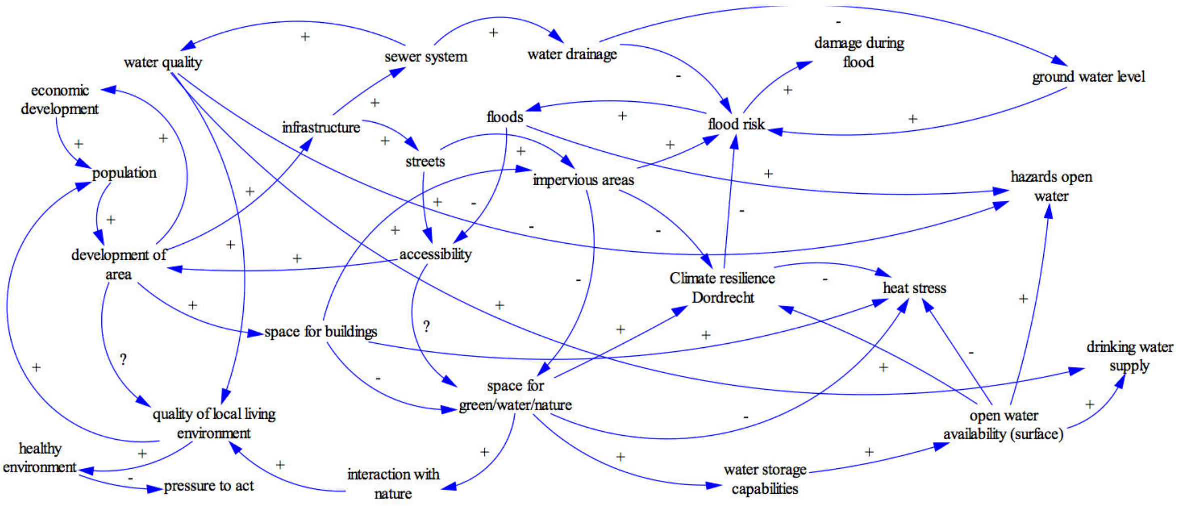

Figure 10. Illustration of some qualitative network capturing causality in the context of flooding prevention

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. In 2016 we got the following the following new result *using rewriting for synthesising filtering algorithm for the Allen constraint*: For all 8192 combinations of Allen's 13 relations between one task with origin oi and fixed length li and another task with origin oj and fixed length lj, we give a formula evaluating to a set of integers which are infeasible for a task origin for the given combination. Such forbidden regions are useful e.g. in a range-consistency maintaining propagator for an Allen constraint in finite domain constraint programming. No visit to Melbourne was done this year because of VISA problem. Consequently we also did remotly (i.e. from Nantes) the following result: the availability of the time-series constraints of the time-series constraint catalog available in the MiniZinc modelling language (and consequently made them accessible to solvers like Choco or Cplex).

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- A visit regarding time-series constraints of Andreina Francisco RodriguezHelmut Simonis, Pierre Flener and Justin Pearson in Nantes in May.
- A visit regarding time-series constraints of Helmut Simonis, in July in May.

9.5.2. Visits to International Teams

- Two visits of E. Arafailova regarding time-series constraints in Cork (March 2016) and in Uppsala (April 2016)
- Three visits of N. Beldiceanu regarding time-series constraint in Cork (June 2016) and in Uppsala (February 2016, August 2016)

AOSTE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. HOPE

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

The ANR HOPE project focused on hierarchical aspects for the high-level modeling and early estimation of power management techniques, with potential synthesis in the end if feasible. Partners were Intel, Synopsys, Magillem, UNS UMR LEAT, and ourselves.

We defined a multi-view, Model-Based design environment named MuVarch, accounting for power-level and performance of embedded hardware architectures, together with representation of abstract applications defining typical use cases fro these platforms.

Started in November 2013, the project reached its completion in February 2016, while Ameni Khecharem PhD defense took place in April 2016 [16].

8.1.1.2. GeMoC

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

This project was admistratively handled by CNRS for our joint team, on the UMR I3S side. It ended September 2016. Partners were Inria (DiverSE EPC), ENSTA-Bretagne, IRIT, Obeo, Thales TRT and Supelec. The project focused on the executable modeling of heterogeneous systems using Models of Computation and Communication described using meta-languages. Specifically, the operational semantics of languages were equipped with precise timely constraints specified in CCSL. There were many outputs from the project but, from AOSTE perspective, we essentially developped MoCCML, an extension of CCSL with constraint automata (already integrated to TimeSquare) and BCool, a language dedicated to coordination apttern specification, which is described as part of Matias Vara-Larsen PhD thesis[19]. All the development realized in this project will end up as the first official eclipse research consortium.

8.1.1.3. 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.

8.1.1.4. 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.

8.1.2. Investissements d'Avenir

8.1.2.1. 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.

8.1.2.2. CLARITY

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

This project is funded by the LEOC Call (*Logiciel Embarqué et Objets Connectés*) of the national support programme *Investissements d'Avenir*. It was started in September 2014 , and a kick-of meeting was held on October 9th. Partners are: Thales (several divisions), Airbus, Areva, Altran, All4Tec, Artal, the Eclipse Fondation, Scilab Enterprises, CESAMES, U. Rennes, and Inria. The purpose of 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 6.2 .

8.1.2.3. 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.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, Except FP7 & H2020

8.2.1.1. ASSUME

Participants: Dumitru Potop-Butucaru, Keryan Didier, Liliana Cucu.

This project is funded by the ITEA3 program. It has started on September 1st 2015. Project coordinator is Daimler. ASSUME has funded the (now completed) post-doc of Raul Gorcitz, and funds the PhD thesis of Keryan Didier.

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. Currently 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. ASSUME will provide a seamless engineering methodology, which addresses this roadblock on the constructive and analytic side.

In this project, most our effort goes to work package "Synthesis of Predictable Concurrent Systems", which we lead. Main scientific results of our work in this project have beenn presented in sections 6.11 and 6.12 . In addition, we closely interacted with our industrial partners to determine their needs, and developed importer tools for their internal formalisms, including Scade v4 and internal formalisms used at Airbus (all importers were developed jointly with EPI PARKAS). This work also resulted in proposals to Airbus on the specification of certain non-functional properties (e.g. the atomic groups of operations that cannot be split during allocation and scheduling). By applying our prototype tools, we have also determined that the use case has significant potential parallelism and will achieve significant speedups through execution on the chosen target architecture (the many-core Kalray MPPA256).

8.3. International Initiatives

8.3.1. 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/

Cyber-Physical Systems (CPS) and the connected Internet of Things (IoT) are inherently heterogeneous systems, with ("cyber") computer digital parts interacting with their physical sensible environment, under user requirements for functional and temporal correctness. Thus, design of such systems as a whole requires a diversity of models, and the behavior orchestration between such models must be carefully defined and analyzed.

FM4CPS will address 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.

Beyond their own expertise in this field, the partners will build on the results of previous cooperations in the context of the Liama projects Hades and Tempo, and the associated team DAESD. The current proposal widely broadens the domain of collaboration, and with the inclusion, for the first time, of Jiao Tong University. We expect this is the first step towards the extension of LIAMA in Shanghai with the strengthening of the involvement of E.C.N.U., and the contribution of new top notch universities such as Jiaotong.

8.3.2. Inria International Partners

8.3.2.1. Declared Inria International Partners

We have signed an agreement with the University of Verona, which covers joint activities (see section 6.7 , together with the housing of interns.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Nieto Luis Agustin

Date: Sep 2015 - Feb 2016

Institution: Universidad de Buenos Aires (Argentina)

CONVECS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. ARC6 Programme

Participants: Lina Marsso, Radu Mateescu, Wendelin Serwe.

ARC6 is an academic research community funded by the Auvergne Rhône-Alpes region, whose objective is to foster the scientific collaborations between different academic institutions of the region working in the domain of information and communication technologies. ARC6 organizes various scientific animations (conferences, working groups, summer schools, etc.) and issues a yearly call for PhD and post-doctorate research project proposals.

Lina Marsso is supported by an ARC6 grant (from October 2016 to October 2019) on formal methods for testing networks of programmable logic controllers, under the supervision of Radu Mateescu and Wendelin Serwe (CONVECS), Ioannis Parissis and Christophe Deleuze (LCIS, Valence).

8.2. National Initiatives

8.2.1. FSN (Fonds national pour la Société Numérique)

8.2.1.1. Connexion

Participants: Hubert Garavel [correspondent], Frédéric Lang.

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, and was extended for 6 months until September 2016. 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.

8.2.2. Competitivity Clusters

8.2.2.1. Bluesky for I-Automation

Participants: Hugues Evrard, 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.cluster-connexion.fr

Bluesky started in September 2012 for three years and was extended for nine months until June 2016. The main contributions of CONVECS to Bluesky (see § 6.1.6) 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.

8.2.3. Other National Collaborations

We had sustained scientific relations with the following researchers:

- Pierre Boullier (Inria, team ALPAGE),
- Pierre-Etienne Moreau (LORIA, team PAREO),
- Fabrice Kordon and Lom Messan Hillah (LIP6, Paris),
- Noël De Palma and Fabienne Boyer (LIG, Grenoble),
- Xavier Etchevers (Orange Labs, Meylan),
- Christophe Deleuze and Ioannis Parissis (LCIS, Valence),
- Pascal Poizat (LIP6, Paris),
- Lina Ye (LRI, Paris).

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

8.3.1.1. SENSATION

Participants: Hubert Garavel [correspondent], Radu Mateescu, 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 contributed 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.

8.3.2. 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.

8.4. 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

At Saarland University (Germany), H. Garavel is a guest scientist of the DEPEND research group headed by Holger Hermanns, who received an ERC Advanced Grant ("POWVER") in 2016.

In 2016, we had scientific relations with several universities and companies abroad, including:

- SRI International, California, USA (Steven Eker),
- Technical University of Eindhoven, The Netherlands (Jan Friso Groote),
- University of Málaga, Spain (Francisco Durán and Carlos Canal),
- Aalto University, Finland (Hernan Ponce de Leon),
- Technical University of Graz, Austria (Franz Wotawa),
- University of Zaragoza, Spain (José Ignacio Requeno),
- University of Utah, USA (Chris Myers and Zhen Zhang),
- DiffBlue, Oxford, UK (Matthias Güdemann).

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Hernan Ponce de Leon (Aalto University, Finland) visited us from February 15 to February 19, 2016.

HYCOMES Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- Ayman Aljarbouh's PhD is partially funded by an ARED grant of the Brittany Regional Council. His doctoral work took place in the context of the Modrio (completed in 2016) and Sys2Soft (completed in 2015) projects on hybrid systems modeling. 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 and Aurélien Lamercerie are participating to the S3PM and SUNSET projects 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 [31]. 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 [9], [5].

8.2. European Initiatives

8.2.1. 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)

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.

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

MUTANT Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

Mutant was the PI of the ANR INEDIT project, ended in october 2015. 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*.

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

7.2. European Initiatives

7.2.1. Collaborations in European Programs, Except FP7 & H2020

Program: PHC Amadeus (France-Austria)

Project acronym: LETITBE

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

Duration: 01/2015 - 01/2017

Coordinator: Florent Jacquemard, Christoph Kirsch

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

Abstract: The objective of the LETITBE 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.

This year, Pierre Donat-Bouillud has spent 5 months in the University of Salzburg and one month in the University of California Berkeley, in the context of the LETITBE project, before starting his PhD in Mutant. Several other student exchanges and scientists visits between Salzburg and Paris have been funded this year by the LETITBE projetc

7.3. International Initiatives

7.3.1. Inria International Partners

7.3.1.1. Informal International Partners

- We are collaborating with Slawek Staworko (LINKS and Algomus, Lille – on leave at U. Edinburgh in 2016), and the Algomus group at Lille, in the context of our projects on rhythm transcription described at Sections 5.2 and 6.2 . This collaboration led this year to the following publications: [23], [22].
- 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) [19], [27].
- 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 5.4) and publications [13], [32], [33].
- MuTant team collaborated with researchers at National Institute of Informatics of Tokyo on real-time Symbolic Alignment of music data [56].

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

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)

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

Programm: 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.

8.2.2. Collaborations in European Programs, Except FP7 & H2020

Program: ITEA 3

Project acronym: ASSUME

Project title: Affordable Safe & Secure Mobility Evolution

Duration: Sep 2015–Aug 2018

Coordinator: Udo Gleich

Other partners: AbsInt Angewandte Informatik GmbH, Airbus, Arcelik, Articus Systems AB, BTC Embedded Systems AG, Berner & Mattner Systemtechnik GmbH, Daimler AG, Eindhoven University of Technology, Ericsson, ANSYS, FindOut Technologies AB,

Ford Otosan, Forschungszentrum Informatik (FZI), Havelsan, KTH (Royal Institute of Technology), Kalray SA, Karlsruhe Institute of Technology (KIT), Kiel University, Koc University, KoçSistem, Model Engineering Solutions GmbH, Mälardalen University, NXP Semiconductors, OFFIS, Recore Systems BV, Robert Bosch GmbH, Safran Aircraft Engines SAS, Safran Electronics & Defense, Scania, TNO, Thales, UNIT Information Technologies R&D Ltd., University Pierre et Marie Curie, University of Technology in Munich, University of Twente, VDL Bus & Coach bv, Verum Software Tools BV, École normale supérieure.

Abstract: 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. Currently 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. ASSUME will provide a seamless engineering methodology, which addresses this roadblock on the constructive and analytic side.

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. 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: 2016

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

The objective of the associate team is to foster collaborations on fundamental and applied research. It also supports training sessions, exchange of undergraduate and master students, and highlighting opportunities in the partners' research, education and economic environments.

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, where computation is specified in terms of computational statements within nested loops and control structures. 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 the system analysis, modeling and design of embedded reactive control applications. They also underline the construction of domain-specific languages and compiler intermediate representations. The execution semantics of data-flow languages impose a different set of challenges for compilation and optimization. We are studying techniques enabling the extraction of a polyhedral representation from data-flow programs, to transform them with the goal of generating memory-efficient and high-performance code for modern architectures.

The research conducted in PolyFlow covers both fundamental and applied aspects. The partners also emphasize the development of solid research tools. The associate team will facilitate their dissemination as free software and their exploitation through industrial collaborations.

8.3.2. Inria International Partners

8.3.2.1. Informal International Partners

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.

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

Prof. Ramakrishna Updadrasta, IIT Hyderabad, India, collaboration visits including internships.

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.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Prasanth Chatarasi, PhD student from Rice University.

Keyur Joshi, undergraduate student from IIT Hyderabad.

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

Guillaume Baudart spent three months working at the IBM Thomas J. Watson Research Centre.

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

- 2 *Arts & Science* projects of Bordeaux eventually granted in 2016 by the Initiative of Excellence (Idex) of Bordeaux,

9.2. International Initiatives

9.2.1. Inria International Partners

9.2.1.1. Informal International Partners

In 2016, PoSET members had active collaboration with

- Shlomo Dubnov, UCSD, USA,
- Mark Lawson, Herriot-Watt University, Edimbourg, UK,
- Camillo Rueda, Universidad Javaneria, Cali, Colombia,

9.3. International Research Visitors

9.3.1. Visits of International Scientists

Shlomo Dubnov, Professor at UCSD (USA), was member of the PoSET project for nine months, thanks to an Bordeaux Idex fellowship in 2016.

SPADES Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. CASERM (PERSYVAL-Lab project)

Participants: Pascal Fradet, Alain Girault, Gregor Goessler, Xiaojie Guo, Xavier Nicollin, Stephan Plassart, Sophie Quinton, Jean-Bernard Stefani.

Despite recent advances, there exist currently no integrated formal methods and tools for the design and analysis of reconfigurable multi-view embedded systems. This is the goal of the CASERM project.

The CASERM project represents a significant effort towards a COQ-based design method for reconfigurable multi-view embedded systems, in order to formalize the structure and behavior of systems and to prove their main properties. The use of a proof assistant to support such a framework is motivated by the fact that the targeted systems are both extremely complex and critical. The challenges addressed are threefold:

1. to model software architectures for embedded systems taking into account their dynamicity and multiple constraints (functional as well as non functional);
2. to propose novel scheduling techniques for dynamically reconfiguring embedded systems; and
3. to advance the state of the art in automated proving for such systems.

The objectives of CASERM that address these challenges are organized in three tasks. They consist respectively in designing an architecture description framework based on a process calculus, in proposing online optimization methods for dynamic reconfiguration systems (this is the topic of Stephan Plassart's PhD), and in developing a formal framework for real-time analysis in the COQ proof assistant (this is the topic of Xiaojie Guo's PhD). A fourth task focuses on common case studies for the evaluation of the obtained results.

The CASERM consortium gathers researchers from the G-SCOP, LIG and VERIMAG laboratories who are reknown specialists in these fields. The project started in November 2016 and will last three years.

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 is involved 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 and in the TypicalCPA project which aims at computing deadline miss models for distributed systems.

We also a recent collaboration with the MPI-SWS in Kaiserslautern (Germany) on formal proofs for real-time systems.

8.3. International Initiatives

8.3.1. Inria Associate Teams Not Involved in an Inria International Labs

8.3.1.1. 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

- Athena 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 synthesized from different physical locations.

9.1.2. 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...

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 modeling 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 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 [0][0], 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. We published a joint paper at the 52nd. Digital Automation Conference in San Francisco [11].

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

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 modeling and virtual prototyping in cyber-physical systems.

In the context of project ITF ARD159 (System-Level Virtual Prototyping of Embedded Systems), ASTRI has used Polychrony and AADL to collaboratively develop a platform for conducting the design of an hardware-in-the-loop simulation of an UR5 robot arm, from its physical model described using Matlab/Simulink and powered using an Opal-RT/RT-Lab workstation, structured around an AADL system model, and using Polychrony to orchestrate real-time simulation down to FPGA analog outputs.

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 stabilization and synchronization 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 modeling 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 of International Scientists

Rajesh Gupta (UC San Diego) visited project TEA in July 2016 in the context of IIP TIX.

[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

Brian Larson (FDA) visited project TEA in January and July 2016.

9.3.1.1. Internships

Daian Yue that was selected in the joint program between ENS Rennes and ECNU and joined project TEA for a six month internship in 2016.

9.3.2. Visits to International Teams

Vania Joloboff was invited for two short stays at University of East China Normal University in Shanghai and UC San Diego.

Jean-Pierre Talpin visited ASTRI in May and December, in the context of IIP VESA.

Jean-Pierre Talpin visited UC San Diego in October, in the context of IIP TIX.

Jean-Pierre Talpin visited IIT Kanpur in February and November for the preparation and Chair of MEMOCODE'16.

ANTIQUE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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.

8.1.2. REPAS

The project REPAS, Reliable and Privacy-Aware Software Systems via Bisimulation Metrics (coordination Catuscia Palamidessi, Inria Saclay), aims at investigating quantitative notions and tools for proving program correctness and protecting privacy, focusing on bisimulation metrics, the natural extension of bisimulation on quantitative systems. A key application is to develop mechanisms to protect the privacy of users when their location traces are collected. Partners: Inria (Comete, Focus), ENS Cachan, ENS Lyon, University of Bologna.

8.1.3. VerAsCo

Title: Formally-verified static analyzers and compilers

Type: ANR Ingénierie Numérique Sécurité 2011

Instrument: ANR grant

Duration: September 2011 - June 2016

Coordinator: Inria (France)

Others partners: Airbus France (France), IRISA (France), Inria Saclay (France)

See also: http://www.systematic-paris-region.org/fr/projets/verasco

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

The project VERASCOadvocates a mathematically-grounded solution to the issues of formal verifying compilers and verification tools. We set out to develop a generic static analyzer based on abstract interpretation for the C language, along with a number of advanced abstract domains and domain combination operators, and prove the soundness of this analyzer using the Coq proof assistant. Likewise, we will continue our work on the CompCert C formally-verified compiler, the first realistic C compiler that has been mechanically proved to be free of any miscompilation will be continued. Finally, the tool qualification issues that must be addressed before formally-verified tools can be used in the aircraft industry, will be investigated.

8.1.4. AstréeA

Title: Static Analysis of Embedded Asynchronous Real-Time Software

Type: ANR Ingénierie Numérique Sécurité 2011

Instrument: ANR grant

Duration: January 2012 - November 2016

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.

8.1.5. VeriFault

This was a PEPS project for one year, coordinated by Cezara Drăgoi, on the topic of fault-tolerant distributed algorithms. These algorithms are notoriously difficult to implement correctly, due to asynchronous communication and the occurrence of faults, such as the network dropping messages or computers crashing. Although fault-tolerant algorithms are at the core of critical applications, there are no automated verification techniques that can deal with their complexity. Due to the complexity distributed systems have reached, we believe it is no longer realistic nor efficient to assume that high level specifications can be proved when development and verification are two disconnected steps in the software production process. Therefore we propose to introduce a domain specific language that has a high-level control structure which focuses on the algorithmic aspects rather than on low-level network and timer code, and makes programs amendable to automated verification.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

ASSUME, ITEA 3 project (Affordable Safe & Secure Mobility Evolution). Affordable Safe & Secure Mobility Evolution

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. Currently 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. ASSUME will provide a seamless engineering methodology, which addresses this roadblock on the constructive and analytic side.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Prof. Kwangkeun Yi Visiteur from Seoul National University, was an invited visitor until Oct 2016.

8.3.1.1. Internships

- Ken Chanseau Saint-Germain, ENS Paris, until Aug 2016
- Marc Chevalier, ENS Lyon, since Sept 2016
- Anton Kulaga, Jul and Aug 2016
- Yoon Seok Ko, Inria, until Jun 2016
- David Romero Suarez, Inria, from Feb 2016 until May 2016]
- Gaelle Candel, Chimie ParisTech

CELTIQUE Project-Team

5. Partnerships and Cooperations

5.1. Regional Initiatives

5.1.1. 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.

5.2. National Initiatives

5.2.1. The ANR VERASCO project

Participants: Sandrine Blazy, Delphine Demange, David Pichardie.

Static program analysis, Certified static analysis

The VERASCO project (2012–06/2016) 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.

5.2.2. The ANR AnaStaSec project

Participants: Frédéric Besson, Sandrine Blazy, Thomas Jensen, Alexandre Dang, Julien Lepiller.

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.

5.2.3. The ANR Binsec project

Participants: Frédéric Besson, Sandrine Blazy, Pierre Wilke, Julien Lepiller.

Binary code, Static program analysis

The Binsec project (2013–2017) is funded 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.

5.2.4. 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 (Tamis and Celtique), Inria Saclay (MAXPLUS) and VISEO/Object Direct.

5.2.5. 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.

5.2.6. 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.

5.3. European Initiatives

5.3.1. Collaborations in European Programs, Except FP7 & H2020

Program:CA COST Action CA15123

Project acronym: EUTYPES

Project title: European research network on types for programming and verification

Duration: 03/2016 to 03/2020

Coordinator: Herman Geuvers (Radboud University Nijmegen, The Netherlands)

Other partners: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Macedonia, Germany, Hungary, Israel, Italy, Lithuania, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Spain, Sweden, 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.

5.4. International Initiatives

5.4.1. Inria Associate Teams Not Involved in an Inria International Labs

5.4.1.1. JCERT

Title: Verified Compilation of Concurrent Managed Languages

International Partner (Institution - Laboratory - Researcher):

Purdue University (United States) - School of Electrical and Computer Engineering (ECE) - Jan Vitek

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#.

5.4.2. Inria International Partners

5.4.2.1. WEBCERT

Title: Verified Trustworthy web Applications

International Partner (Institution - Laboratory - Researcher):

Imperial College (United Kingdom) - Department of Computing - Philippa Gardner

Duration: 2015 - 2019

Start year: 2015

See also: JSCert web page

The goal of the WebCert partnership is to extend the development of the JSCert formal semantics of JavaScript in the following domains: further mechanized specification, human-readable formal specification, program logic, verification tools, and the formalization of Defensive JavaScript.

5.4.2.2. Informal International Partners

Alan Schmitt is part of a Polonium Hubert Curien Partnership (PHC) with the University of Wrocław. This partnership is led by Sergueï Lenglet, from Loria, Nancy (currently visiting member of the Celtique project).

5.5. International Research Visitors

5.5.1. Visits of International Scientists

5.5.1.1. Internships

Thomas Wood

Date: Oct 2016 - Dec 2016

Institution: Imperial College (United Kingdom)

Ahmad Salim Al-Sibahi

Date: Sep 2016 - Jan 2017

Institution: IT University of Copenhagen (Denmark)

DEDUCTEAM Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR Locali

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

7.1.2. ANR BWare

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

7.1.3. ANR Tarmac

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

7.2. European Initiatives

7.2.1. Collaborations in European Programs, Except FP7 & H2020

Program: CA COST Action CA15123

Project acronym: EUTYPES

Project title: European research network on types for programming and verification

Duration: 21/03/16 - 20/03/20

Coordinator: Herman Geuvers

7.3. International Initiatives

7.3.1. Participation in Other International Programs

Login

Title: Logic and Information

International Partner (Institution - Laboratory - Researcher):

Universidad de Buenos Aires (Argentina) - Ricardo Oscar Rodrigues

Duration: 2015 - 2016

This project aims to propose an improvement on a long-term already existing collaboration between Inria, the brazilians and the argentin named team. We already have a CAPES-COFECUB cooperation (n. 690/10, namely “Teorias lógicas contemporâneas e a filosofia da linguagem: questões epistemológicas e semânticas”) that leaded to many students interchange and technical visits of Professors, including the organisation of some workshops (the last one was the 2nd Workshop on Logic and Semantics, at UERJ, Ilha Grande-RJ, Brazil. Prof. Gilles Dowek is also a Co-Advisor with Prof. Edward Hermann Haeusler of a brazilian Ph.D. Candidate in this project (and a former one also in this project, these two candidates finalised recently a sandwich doctorate - similar to stage doctorale - at Inria). Prof. Gilles Dowek also collaborates with other members of this team and is supervising a post-doc project of another member. Since 2011 members of the team presents.

FoQCoSS

Title: Foundations of Quantum Computation: Syntax and Semantics

International Partners (Institution - Laboratory - Researcher):

Universidad Nacional de Quilmes (Argentina) - Alejandro Diaz-Caro

CNRS (France) - Simon Perdrix

Duration: 2016 - 2017

The design of quantum programming languages involves the study of many characteristics of languages which can be seen as special cases of classical systems: parallelism, probabilistic systems, non-deterministic systems, type isomorphisms, etc. This project proposes to study some of these characteristics, which are involved in quantum programming languages, but also have a more immediate utility in the study of nowadays systems. In addition, from a more foundational point of view, we are interested in the implications of computer science principles for quantum physics. For example, the consequences of the Church-Turing thesis for Bell-like experiments: if some of the parties in a Bell-like experiment use a computer to decide which measurements to make, then the computational resources of an eavesdropper have to be limited in order to have a proper observation of non-locality. The final aim is to open a new direction in the search for a framework unifying computer science and quantum physics.

7.4. International Research Visitors

7.4.1. Internships

- Clément Chouteau, from May 2016 to July 2016
- David Pham (Univ. Évry) from June 2016 to July 2016

7.4.2. Visits to International Teams

7.4.2.1. Research Stays Abroad

F. Gilbert spent one month in the formal methods team at NASA Langley Research Center, to work with Cesar Munoz on the use of automated theorem provers to verify PVS proofs.

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.

9.1.3. 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, Michael 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.

MARELLE Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. 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.

6.2. International Initiatives

6.2.1. Inria International Partners

6.2.1.1. Informal International Partners

We work with the team of Adam Chlipala at MIT, in particular the engineer Paul Steckler, with whom we have regular meetings concerning the optimization of parts of the Coq system with respect to use cases provided by the MIT team, and the design of user-interface tools. This engineer had a visit of 6 weeks in France in April, three weeks in the pi.r2 team (mostly hosted by Matthieu Sozeau) and three weeks in the Marelle team, mostly hosted by Enrico Tassi and Maxime Dénès. The collaboration continues since that visit with a weekly phone conference.

6.3. International Research Visitors

6.3.1. Visits of International Scientists

We had visits by Gilles Barthe (IMDEA, Madrid, Spain) for 2 weeks, Benedikt Schmidt (IMDEA), for 2 weeks, François-Xavier Standaert (Université Catholique de Louvain, Crypto Group, Belgium), for 1 week, Sebastian Faust (Ruhr-University Bochum, Germany) for 1 week, François Dupressoir (IMDEA) for 1 week, Pierre-Yves Strub (IMDEA), for 1 week, and Peter Schwabe (Radboud University, Nijmegen, the Netherlands) for 3 days.

6.3.2. Visits to International Teams

Benjamin Grégoire visited IMDEA (Madrid, Spain) for two one-week trips.

Yves Bertot, Maxime Dénès, and Enrico Tassi visited Princeton University in June for the kick-off meeting of the *Expedition in Computing* entitled “the science of deep specification” funded by the NSF foundation.

Enrico Tassi visited the team of Jesper Bengtson at the IT-University of Copenhagen, Denmark.

Anders Mörtberg visited the team of Thierry Coquand at Chalmers and University of Göteborg in Sweden.

MEXICO Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

We will be participating in the ANR Project ALGORECELL that starts in 2017.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

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

8.3. International Initiatives

8.3.1. Inria Associate Teams Not Involved in an Inria International Labs

8.3.1.1. LifeForm

Title: Life Sciences need formal Methods !

International Partner (Institution - Laboratory - Researcher):

Newcastle University (United Kingdom) - School of Computing Science - Victor Khomenko

Start year: 2016

See also: http://projects.lsv.ens-cachan.fr/LifeForm/

This project extends an existing cooperation between the MEXICO team and Newcastle University on partial-order based formal methods for concurrent systems. We enlarge the partnership to bioinformatics and synthetic biology. The proposal addresses addresses challenges concerning formal specification, verification, monitoring and control of synthetic biological systems, with use cases conducted in the Center for Synthetic Biology and the Bioeconomy (CSBB) in Newcastle. A main challenge is to create a solid modelling framework based on Petri-net type models that allow for causality analysis and rapid state space exploration for verification, monitoring and control purposes; a potential extension to be investigated concerns the study of attractors and cell reprogramming in Systems Biology.

8.3.2. Participation in Other International Programs

UMI with CMI, India, starting in 2017; currently LIA INFORMEL, see below.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Visits by Victor Khomenko and Maciej Koutny within the LifeForm associated team

8.4.2. Internships

- **Juraj Kolc˘ák** from Masaryk University, Brno, Czech Republic, on *Efficient Analysis of Boolean Networks under Parameter Uncertainty*, Spring/summer of 2016 (Master's thesis research); director: Stefan Haar
- **Clara Scherbaum** from Aachen University, Germany, on *Computing Cut Sets for Petri Nets*, Spring 2016, LSV (ENS Cachan),
- **Hugues Mandon**: Algorithms for cellular reprogramming.

8.4.3. Visits to International Teams

8.4.3.1. Research Stays Abroad

Paul Gastin is visiting IIT Bombay and Chennay Mathematical Institute, India, from October 10, 2016 to March 10, 2017.

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.

8.1.2. Collaborations in European Programs, Except FP7 & H2020

8.1.2.1. FISP: ANR blanc International

Participants: Kaustuv Chaudhuri, François Lamarche, Sonia Marin, Dale Miller, Lutz Straßburger.

Title: The Fine Structure of Formal Proof Systems and their Computational Interpretations

Duration: 01/01/2016 – 31/12/2018

Partners:

University Paris VII, PPS (PI: Michel Parigot)

Inria Saclay–IdF, EPI Parsifal (PI: Lutz Straßburger)

University of Innsbruck, Computational Logic Group (PI: Georg Moser)

Vienna University of Technology, Theory and Logic Group (PI: Matthias Baaz)

Total funding by the ANR: 316 805 EUR

The FISP project is part of a long-term, ambitious project whose objective is to apply the powerful and promising techniques from structural proof theory to central problems in computer science for which they have not been used before, especially the understanding of the computational content of proofs, the extraction of programs from proofs and the logical control of refined computational operations. So far, the work done in the area of computational interpretations of logical systems is mainly based on the seminal work of Gentzen, who in the mid-thirties introduced the sequent calculus and natural deduction, along with the cut-elimination procedure. But that approach shows its limits when it comes to computational interpretations of classical logic or the modelling of parallel computing. The aim of our project, based on the complementary skills of the teams, is to overcome these limits. For instance, deep inference provides new properties, namely full symmetry and atomicity, which were not available until recently and opened new possibilities at the computing level, in the era of parallel and distributed computing.

8.1.2.2. COCA HOLA: ANR JCJC Project

Participant: Beniamino Accattoli.

Title: COst model for Complexity Analyses of Higher-Order programming LAnguages.

Collaborators: Ugo Dal Lago (University of Bologna & Inria), Delia Kesner (Paris Diderot University), Damiano Mazza (CNRS & Paris 13 University), Claudio Sacerdoti Coen (University of Bologna).

Duration: 01/10/2016 – 31/09/2019

Total funding by the ANR: 155 280 EUR

The COCA HOLA project aims at developing complexity analyses of higher-order computations, i.e. that approach to computation where the inputs and outputs of a program are not simply numbers, strings, or compound data-types, but programs themselves. The focus is not on analysing fixed programs, but whole programming languages. The aim is the identification of adequate units of measurement for time and space, i.e. what are called reasonable cost models. The problem is non-trivial because the evaluation of higher-order languages is defined abstractly, via high-level operations, leaving the implementation unspecified. Concretely, the project will analyse different implementation schemes, measuring precisely their computational complexity with respect to the number of high-level operations, and eventually develop more efficient new ones. The goal is to obtain a complexity-aware theory of implementations of higher-order languages with both theoretical and practical downfalls.

The projects stems from recent advances on the theory of time cost models for the lambda-calculus, the computational model behind the higher-order approach, obtained by the principal investigator and his collaborators (who are included in the project).

COCA HOLA will span over three years and is organised around three work packages, essentially:

1. extending the current results to encompass realistic languages;
2. explore the gap between positive and negative results in the literature;
3. use ideas from linear logic to explore space cost models, about which almost nothing is known.

8.2. International Initiatives

8.2.1. Participation in Other International Programs

8.2.1.1. PHC Amadeus: Analytic Calculi for Modal Logics

Participants: Kaustuv Chaudhuri, Sonia Marin, Giselle Reis, Lutz Straßburger.

Title: Analytic Calculi for Modal Logics

Duration: 01/01/2016 – 31/12/2017

Austrian Partner: TU Wien, Institute for Computer Science (Department III)

Modal logics are obtained from propositional logics by adding modalities $\Box$ and $\Diamond$, meaning necessity and possibility. Originally studied by philosophers in order to reason about knowledge and belief, modal logics have nowadays many applications in computer science. Well known examples are epistemic logics, which allow to formally reason about the knowledge of independently acting and interacting agents, temporal logics, which allow to reason about temporal properties of processes, and authentication logics, which are used to formally reason about authentication protocols.

The purpose of this project is to develop a proof theory for variants of modal logic that have applications in modern computer science but that have been neglected by traditional proof theory so far.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Professor Chuck Liang (from Hofstra University, NY, USA) visited the team from 5 June to 25 June 2016 in order to continue his collaborations with team members on basic questions of proof theory. In particular, he worked with Miller on identifying possible means to allow classical and intuitionistic logic to be mixed in a common proof system. Miller is exploring how the resulting ideas might be able to reorganize the notion of kernel logic used within the ProofCert project.

8.3.1.1. Internships

Ameni Chtourou was an intern funded by ProofCert during May, June, and July 2016. She was advised by Accattoli and worked with using the Abella theorem prover to formalize connections various connections between λ-term evaluation and abstract machine models.

8.3.2. Visits to International Teams

8.3.2.1. Research Stays Abroad

Stéphane Graham-Lengrand spent 8 months, from January 2016 to August 2016, at SRI International, Computer Science Lab. This visit developed a collaboration with N. Shankar, MP Bonacina, D. Jovanovic, and Martin Schaeff on new algorithms and new architectures for automated and interactive theorem proving, as well as on new programme verification techniques.

PI.R2 Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

Alexis Saurin (coordinator) and Yann Régis-Gianas are members of the four-year RAPIDO ANR project, started 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 IRIF (PPS team), David Baelde from LSV, ENS-Cachan, and Pierre Clairambault, Damien Pous and Colin Riba from LIP, ENS-Lyon.

Pierre-Louis Curien (coordinator), Yves Guiraud (local coordinator), Philippe Malbos and Samuel Mimram have been members of the three-year Focal project of the IDEX Sorbonne Paris Cité (July 2013 to June 2016). 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 mathematicians form LAGA (Univ. Paris 13).

Pierre-Louis Curien (coordinator), Yves Guiraud (local coordinator), Philippe Malbos and Samuel Mimram 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 linear algebra, combinatorial group theory and theoretical computer science. This project is joint with mathematicians and computer scientists from LAGA (Univ. Paris 13), LIX (École Polytechnique), ICJ (Univ. Lyon 1 and Univ. Saint-Étienne), I2M (Univ. Aix-Marseille) and IMT (Univ. Toulouse 3).

Pierre-Louis Curien, Yves Guiraud, Hugo Herbelin, Philippe Malbos, Samuel Mimram and Alexis Saurin are members of the GDR Informatique Mathématique, in the Géocal (Geometry of computation) and LAC (Logic, algebra and computation) working groups.

Pierre-Louis Curien, Yves Guiraud (local coordinator), Philippe Malbos, Samuel Mimram and Matthieu Sozeau are members of the GDR 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 and theoretical computer science.

Hugo Herbelin was the coordinator of the PPS site for the ANR Récré (January 2012 to 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 was funded by the CoqHoTT ERC.

6.2. European Initiatives

6.2.1. FP7 & H2020 Projects

Hugo Herbelin is a deputy representative of France in the COST action EUTYPES.

6.3. International Initiatives

6.3.1. Inria Associate Teams Not Involved in an Inria International Labs

Pierre-Louis Curien participates 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).

6.3.2. Inria International Partners

6.3.2.1. 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, University of Cambridge, and Universidad Nacional de Córdoba.

6.3.3. 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 (Deducteam).

6.4. International Research Visitors

6.4.1. Visits of International Scientists

Paolo Giarrusso (Univ. of Marburg) visited Yann Régis-Gianas in February 2016.

Lourdes del Carmen Gonzalez Huesca (Univ. of Mexico) visited Yann Régis-Gianas in December 2016.

6.4.2. Visits to International Teams

6.4.2.1. Research Stays Abroad

Pierre-Louis Curien visited the Category Theory group at Macquarie University in June-July 2016 (collaborative work on the combinatorial structure of type dependency).

As a part of his joint PhD, Étienne Miquey worked most of the year in Montevideo within the Logic group of the Universidad de la República of Uruguay.

SUMO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

ANR STOCH-MC: Model-Checking of Stochastic Systems using approximated algorithms, 2014-2018, http://perso.crans.org/~genest/stoch.htmlweb 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.

ANR HeadWorks: Human-Centric Data-oriented WORKflows , 2016-2020
Led by Université Rennes 1.
Partners: Inria Project Team VALDA (LSV and ENS-ULM), Univestité Rennes 1 (DRUID), Inria SUMO, Inria Lille (LINKs), MNHN, Foule Factory.
Headwork was accepted in 2016. Participants : Loïc Hélouët, Éric Badouel.

Partners: IRISA (DRUID), ENS ULM (VALDA), Inria SUMO, Inria Lille (LINKs), MNHN, Foule Factory.

The objective of this project is to develop techniques to facilite development, deployment, and monitring of crowd-based participative applications. This requires handling complex workflows with multiple participants, incertainty in data collections, incentives, skills of contributors, ... To overcome these challenges, Headwork will define rich workflows with multiple participants, data and knowledge models to capture various kind of crowd applications with complex data acquisition tasks and human specificities. We will also address methods for deploying, verifying, optimizing, but also monitoring and adapting crowd- based workflow executions at run time.

9.1.2. IPL HAC SPECIS

The Inria Project Lab HAC SPECIS (High-performance Application and Computers, Studying PErformance and Correctness In Simulation, 2016-2020: http://hacspecis.gforge.inria.fr/) is a transversal project internal to Inria. The goal of the HAC SPECIS project is to answer the methodological needs raised by the recent evolution of HPC architectures by allowing application and runtime developers to study such systems both from the correctness and performance point of view. Inside this project, we collaborate with Martin Quinson (Myriads team) on the dynamic formal verification of high performance runtimes and applications. The PhD of The Anh Pham is granted by this project.

Partners: Inria teams AVALON (Lyon), POLARIS (Grenoble), HIEPACS, STORM (Bordeaux), MEXICO (Paris), MYRIADS, SUMO (Rennes), VERIDIS (Nancy).

Participants: Thierry Jéron, The Anh Pham.

9.1.3. National informal collaborations

The team collaborates with the following researchers:

- Yliès Falcone (CORSE LIG/Inria team in Grenoble) and Antoine Rollet (Labri Bordeaux) on the enforcement of timed properties,
- Arnaud Sangnier (IRIF) on the parameterized verification of probabilistic systems,
- Béatrice Bérard (LIP6) and Serge Haddad (LSV) on problems of opacity and diagnosis.
- Thomas Chatain, on problems related to concurrency and time,
- 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/),
- Patricia Bouyer (LSV, ENS Cachan) on the analysis of probabilistic timed systems and quantitative aspects of verification,
- François Laroussinie (IRIF, UP7-Diderot) on logics for multi-agent systems.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

Nicolas Markey is a member of Project ERC EQualIS whose principal investigator is Patricia Bouyer from LSV.

9.3. International Initiatives

9.3.1. Inria Associate Teams Not Involved in an Inria International Labs

9.3.1.1. QuantProb

Title: Quantitative analysis of non-standard properties in probabilistic models

International Partner (Institution - Laboratory - Researcher):

Technical University of Dresde (Germany) - Saxe - Christel Baier

Start year: 2016

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

Quantitative information flow and fault diagnosis share two important characteristics: quantities (in the description of the system as well as in the properties of interest), and users partial knowledge. Yet, in spite of their similar nature, different formalisms have been proposed. Beyond these two motivating examples, defining a unified framework can be addressed by formal methods. Formal methods have proved to be effective to verify, diagnose, optimize and control qualitative properties of dynamic systems. However, they fall short of modelling and mastering quantitative features such as costs, energy, time, probabilities, and robustness, in a partial observation setting. This project proposal aims at developing theoretical foundations of formal methods for the quantitative analysis of partially observable systems.

9.3.2. Inria International Partners

9.3.2.1. 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 and with Thomas Brihaye (University of Mons) on the analysis of probabilistic timed systems.

The team has well-established collaborations with several institutes in India. CMI (Chennai Mathematical Institute, M. Mukund and N.K. Kumar), IIT Bombay (S. Akshay).

The team is building a new collaboration with Ecole Polytechnique Montreal (J. Mullins).

9.4. International Research Visitors

9.4.1. Visits of International Scientists

L. Ricker visited the SUMO team for 2 months in May-June 2016.

9.4.1.1. Internships

Robert Nsaibirni from the University of Yaoundé I joined the team from Sept. 2016 in the context of an Eiffel grant.

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

Nathalie Bertrand spent a month at the Simons Institute for the theory of computing, UC Berkeley, California. She participated to the program Logical Structure in Computation (https://simons.berkeley.edu/programs/logic2016).

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. https://digicosme.lri.fr/GT+ELFIC

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).

9.1.2. ELEFFAN

Participant: Sylvie Boldo [contact].

ELEFFAN is a Digicosme project funding the PhD of F. Faissole. S. Boldo is the principal investigator. It began in 2016 for three years. https://project.inria.fr/eleffan/

The ELEFFAN project aims at formally proving rounding error bounds of numerical schemes.

Partners: ENSTA Paristech (A. Chapoutot)

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. https://vocal.lri.fr/

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. http://ajacs.inria.fr/

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], 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. http://soprano-project.fr/

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], 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 [109]. This therefore should be a driving factor to reduce the risks of the project, which can then focus on the design of several extensions of the verification tools to deal with a larger amount of proof obligations.

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

9.2.8. ANR Verasco

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

The Verasco 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).

9.2.9. FUI LCHIP

Participant: Sylvain Conchon [contact].

LCHIP (Low Cost High Integrity Platform) is aimed at easing the development of safety critical applications (up to SIL4) by providing: (i) a complete IDE able to automatically generate and prove bounded complexity software (ii) a low cost, safe execution platform. The full support of DSLs and third party code generators will enable a seamless deployment into existing development cycles. LCHIP gathers scientific results obtained during the last 20 years in formal methods, proof, refinement, code generation, etc. as well as a unique return of experience on safety critical systems design. http://www.clearsy.com/en/2016/10/4260/

Partners: 2 technology providers (ClearSy, OcamlPro), in charge of building the architecture of the platform ; 3 labs (IFSTTAR, LIP6, LRI), to improve LCHIP IDE features ; 2 large companies (SNCF, RATP), representing public ordering parties, to check compliance with standard and industrial railway use-case.

The project lead by ClearSy has started in April 2016 and lasts 3 years. It is funded by BpiFrance as well as French regions.

9.2.10. ANR PARDI

Participant: Sylvain Conchon [contact].

Verification of parameterized distributed systems, 2016-2021.

Partners: Université Paris VI - Université Paris XI - Inria NANCY

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 in European Programs, Except FP7 & H2020

Program: COST (European Cooperation in Science and Technology).

Project acronym: EUTypes https://eutypes.cs.ru.nl/

Project title: The European research network on types for programming and verification

Duration: 2015-2019

Coordinator: Herman Geuvers, Radboud University Nijmegen, The Netherlands

Other partners: 36 members countries, see http://www.cost.eu/COST_Actions/ca/CA15123?parties

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.

9.3.3. 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

- Ran Chen is a PhD student from Institute of Software (Chinese Academy of Sciences, Beijing, China) visiting the team for 10 months under the supervision of C. Marché and J.-J. Lévy (PiR2 team, Inria Paris). She is working on the formal verification of graphs algorithms, and also in the context of the CoLiS project on verification of some aspects of the Unix file system and shell scripts. [34]
- Cláudio Belo Lourenço is a PhD student from Universidade do Minho, Portugal. He studies deductive verification of imperative programs and the behaviour of different kinds of verification condition generators [101]. The goal of his visit is to use Why3 as a platform for prototyping and experimental evaluation of these generators.

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

- F. Faissole has spent two months visiting B. Spitters at Aarhus University (Denmark) They proposed an extension of ALEA library to continuous datatypes.[32].
- M. Roux has spent three months with D. Jovanovic and B. Dutertre at SRI (California, USA). They worked on extending Sally, the new model checker of SRI based on SAL, to add the verification of parameterized cache coherence protocols. The software can be found on https://github.com/SRI-CSL/sally.
- S. Conchon has been invited a month at SRI by D. Jovanovic. During this visit, he has collaborated with CSL researchers to compare the design and implementation choices between the model checkers Sally and Cubicle.

VERIDIS Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR-DFG Project SMArT

Participants: Haniel Barbosa, Pascal Fontaine, 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 project gathers members of VeriDis in Nancy and Saarbrücken, 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. The results feed back into the implementations of Redlog (section 6.2) and veriT (section 6.5), which also serve as experimentation platforms for theories, techniques and methods designed within this project.

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

9.1.2. ANR Project IMPEX

Participants: Souad Kherroubi, Dominique Méry.

The ANR Project IMPEX, within the INS program, 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 [49], 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 [11] is to offer rigorous mechanisms for handling domain knowledge in design models.

9.1.3. Inria IPL HAC SPECIS

Participants: Marie Duflot-Kremer, Stephan Merz.

The goal of the HAC SPECIS (High-performance Application and Computers: Studying PErformance and Correctness In Simulation) project is to answer methodological needs of HPC application and runtime developers and to allow studying real HPC systems with respect to both correctness and performance. To this end, this Inria Project Lab assembles experts from the HPC, formal verification, and performance evaluation communities.

HAC SPECIS started in 2016. VeriDis contributes through its expertise in formal verification techniques. In particular, our goal is to extend the functionalities of exhaustive and statistical model checking within the SimGrid platform.

9.1.4. 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 (cf. section 6.1), 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 (Toccata group) and Inria Rennes (Celtique group), among others. Simon Cruanes was hired in October 2015 and has started the development of Nunchaku, whereas Blanchette has developed an Isabelle frontend. Three releases have taken place so far, and the tool is an integral part of the Isabelle2016-1 official release. Work has started on Coq and TLAPS frontends. The tool is described in a conference publication [33] and was presented at a workshop [28].

9.1.5. Inria ADT PLM (2014-2016)

Participant: Matthieu Nicolas.

Joint work with Gérald Oster (project-team Coast, Inria Nancy – Grand Est) and Martin Quinson (project-team Myriads, Inria Rennes – Bretagne Atlantique)

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 finalized the web version of our framework, and submitted several project applications to pursue this work in the future. Unfortunately, none of these applications have been accepted so far. Martin Quinson invited Peter Hubwieser, professor of the Technical University of Munich (TUM) and specialist of the didactics of Computer Science, for two weeks in November. Developing the PLM and exploiting the data already gathered were central elements of this work meeting. A joint publication is currently prepared, targeting the ItiCSE'17 conference.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

Program: H2020-FETOPEN-2015-CSA

Project acronym: SC^2

Project title: Satisfiability Checking and Symbolic Computation

Duration: July 2016 – September 2018

Coordinator: James H. Davenport (U. Bath, U.K.)

Other partners: RWTH Aachen (Germany), Fondazione Bruno Kessler (Italy), Università degli Studi di Genova (Italy), Maplesoft Europe Ltd (Germany), Coventry University (U.K.), University of Oxford (U.K.), Universität Kassel (Germany), Max Planck Institut für Informatik (Germany), Universität Linz (Austria)

Abstract: Whereas symbolic computation is concerned with efficient algorithms for determining exact solutions to complex mathematical problems, more recent developments in the area of satisfiability checking tackle similar problems with different algorithmic and technological solutions. Both communities have made remarkable progress in the last decades and address practical problems of rapidly increasing size and complexity. For example, satisfiability checking is an essential backend for assuring the security and the safety of computer systems. Techniques and tools of symbolic computation are used by different scientific communities for solving large mathematical problems that are out of reach of pencil and paper developments. Currently the two communities are largely disjoint and unaware of the achievements of each other, despite strong reasons for them to discuss and collaborate, as they share many central interests. Bridges between the communities in the form of common platforms and roadmaps are necessary to initiate an exchange, and to support and to direct their interaction. This Coordination and Support Action within the FET-Open framework will initiate a wide range of activities to bring the two communities together, identify common challenges, offer global events and bilateral visits, propose standards, and so on. Combining the knowledge, experience and the technologies in these communities will lead to cross-fertilization and mutual improvements, enabling the development of radically improved software tools.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. KANASA

Title: Kanazawa-Nancy for Satistifiability and Arithmetics

International Partner: Japan Advanced Institute for Science and Technology (Dept. Intelligent Robotics, Mizuhito Ogawa)

Starting year: 2016

During the last decade, there has been tremendous progress on symbolic verification techniques, spurred in particular by the development of SMT (satisfiability modulo theories) techniques and tools. Our first direction of research will be to investigate the theoretical background and the practical techniques to integrate Interval Constraint Propagation within a generic SMT framework, including other decision procedures and quantifier handling techniques. On the purely arithmetic side, we also want to study how to unite the reasoning power of all arithmetic techniques developed in the team, including simplex-based SMT-like reasoners, Virtual Substitution, and Cylindrical Algebraic Decomposition. In particular, this includes developing theory combination frameworks for linear and non-linear arithmetic. There is a strong incentive for these kind of combinations since even non-linear SMT problems contain a large proportion of linear constraints. The partnership is supported by a Memorandum of Understanding between JAIST and LORIA.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Ilina Stoilkovska

Date: 1 September – 31 October

Institution: TU Wien (Austria)

Host: Stephan Merz

Ilina is a PhD student at TU Wien, Austria, and works on tailored abstractions for the parameterized verification of fault-tolerant distributed algorithms. During her stay in Nancy, she worked on a formal soundness proof of her abstractions in the TLA$^+$ Proof System.

Tung Vu Xuan

Date: 1 May 2016 – 30 April 2017

Institution: JAIST

Host: Pascal Fontaine

Tung Vu Xuan is a PhD student at JAIST, Japan. He is visiting VeriDis in the context of the KANASA project. He works mainly on Interval Constraint Propagation (ICP), a heuristic but powerful method for satisfiability checking of non-linear arithmetic (NLA) constraints. During his stay, we investigate techniques to combine ICP with decision procedures for NLA within an SMT context.

9.4.2. Internships

Anders Olav Candasamy

Date: 1 March – 31 July

Institution: Université de Lorraine (Erasmus Mundus DESEM)

Host: Dominique Méry

Anders Candasamy analyzed a hemodialysis case study using Event-B. Besides developing the formal model, he also reflected on the modeling process and proposed several methodological improvements.

Matthieu Lequesne

Date: 1 March – 31 July

Institution: École Polytechnique

Host: Stephan Merz

Matthieu Lequesne worked on translating formulas in a core sublanguage of TLA$^+$ to the input format of Nunchaku (section 6.1), with the aim of producing (counter)models for TLA$^+$ proof obligations.

Weichung Shaw

Date: 1 March – 31 August

Institution: Université de Lorraine (Erasmus Mundus DESEM)

Host: Stephan Merz

Weichung Shaw worked on formalizing a correctness proof of the Raft consensus algorithm [50] in TLA$^+$. He proved several fundamental lemmas and documented several methodological issues with the use of TLAPS.

CARTE Team

7. Partnerships and Cooperations

7.1. National Initiatives

We participate in a PEPS project “Jeux quantiques sans probabilite´s”. The partners are Mehdi Mhalla (CR CNRS, LIG, coordinator), Pablo Arrighi (Prof. Aix-Marseille), Paul Dorbec (MdC, U. Bordeaux), Frédéric Magniez (DR CNRS, IRIF), Simon Perdrix (CR CNRS, CARTE).

7.1.1. 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.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Mathieu Hoyrup participates in the Marie-Curie RISE project *Computing with Infinite Data* coordinated by Dieter Spreen (Univ. Siegen) that has been accepted and will start in April 2017.

7.3. International Initiatives

7.3.1. 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 need to study topics such as parallelism, probabilistic systems, isomorphisms, etc., which constitute subjects of study by themselves. 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.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

- Walid Gomaa, associate professor at Alexandria E-Just University, was invited during two months (March and May) in the team in the PHC Imhotep.

7.4.1.1. Internships

Arinta Auza (ENS Cachan / Indonesie)

7.4.2. Visits to International Teams

7.4.2.1. Research Stays Abroad

Nazim Fatès was invited for a short stay at the Technische Universtät Dresden, in the Centre for Information Services and High Performance Computing (ZIH), in the team of Andreas Deutsch, head of Department for Innovative Methods of Computing. He gave a talk at the monthly ZIH colloquium.

Simon Perdrix spent one month at the Simons Institute for Theoretical Computer Science at Berkeley, University of California, as an invited researcher during the semester of Logic and Computation (mid-November to Mid-December 2016)

COMETE Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. Projects funded by Digiteo-DigiCosme

9.1.1.1. OPTIMEC

Project title: Optimal Mechanisms for Privacy Protection

Duration: September 2016 - August 2019

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's: Serge Haddadm ENS Cachan.

Abstract: In this project we plan to investigate classes of utility and privacy measures, and to devise methods to obtain optimal mechanisms with respect to the trade-off between utility and privacy. In order to represent the probabilistic knowledge of the adversary and of the user, and the fact that mechanisms themselves can be randomized, we will consider a probabilistic setting. We will focus, in particular, on measures that are expressible as linear functions of the probabilities.

9.1.1.2. D-SPACES

Project title: D-spaces : Distributed Spaces in Concurrent Epistemic Systems

Duration: Nov 2013 - Oct 2016

Coordinator: Frank Valencia, CNRS-LIX and Inria Saclay, EPI Comète

Other PI's: Stefan Haar ENS Cachan.

Abstract: In this project we developed an innovative and expressive computational model for these systems that coherently combines techniques for the analysis of concurrent systems such as process calculi with epistemic and spatial formalisms.

9.2. National Initiatives

9.2.1. Large-scale initiatives

Project acronym: CAPPRIS

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

Duration: September 2013 - December 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.

9.3. International Initiatives

9.3.1. Inria-MSR joint lab

9.3.1.1. 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.

9.3.2. Inria Associate Teams

9.3.2.1. LOGIS

Title: Logical and Formal Methods for Information Security

Inria principal investigator: Konstantinos Chatzikokolakis

International Partners:

Mitsuhiro Okada, Keio University (Japan)

Yusuke Kawamoto, AIST (Japan)

Tachio Terauchi, JAIST (Japan)

Masami Hagiya, University of Tokyo (Japan)

Start year: 2016

URL: http://www.lix.polytechnique.fr/~kostas/projects/logis/

Abstract: The project aims at integrating the logical / formal approaches to verify security protocols with (A) complexity theory and (B) information theory. The first direction aims at establishing the foundations of logical verification for security in the computational sense, with the ultimate goal of automatically finding attacks that probabilistic polynomial-time adversaries can carry out on protocols. The second direction aims at developing frameworks and techniques for evaluating and reducing information leakage caused by adaptive attackers.

9.3.3. Inria International Partners

9.3.3.1. Informal International Partners

Geoffrey Smith, Florida International University (United States)

Carroll Morgan, NICTA (Australia)

Annabelle McIver, Maquarie University (Australia)

Moreno Falaschi, Professor, University of Siena, Italy

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

Camilo Rueda, Professor, Universidad Javeriana Cali, Colombia

9.3.4. Participation in Other International Programs

9.3.4.1. REPAS

Program: ANR Blanc

Project title: Reliable and Privacy-Aware Software Systems via Bisimulation Metrics

Duration: October 2016 - September 2021

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's and partner institutions: Ugo del Lago, Inria Sophia Antipolis (EPI Focus) and University of Bologna (Italy). Vincent Danos, ENS Paris. Filippo Bonchi, ENS Lyon.

Abstract: In this project, we aim at investigating quantitative notions and tools for proving program correctness and protecting privacy. In particular, we will focus on bisimulation metrics, which are the natural extension of bisimulation on quantitative systems. As a key application, we will develop a mechanism to protect the privacy of users when their location traces are collected.

9.3.4.2. 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, Frank Valencia, CNRS-LIX and Inria Saclay (France). 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.

9.3.4.3. 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.

9.3.4.4. 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.

9.3.4.5. CLASSIC

Program: Colciencias - Conv. 712.

Project title: Concurrency, Logic and Algebra for Social and Spatial Interactive Computation.

Duration: Oct 2016 - Oct 2019

URL: http://goo.gl/Gv6Lij

Coordinator: Camilo Rueda PUJ Cali (Colombia).

Other PI's and partner institutions: Carlos Olarte, Universidade Federal do Rio Grande do Norte (Brazil). Frank Valencia, CNRS-LIX and Inria Saclay (France).

Abstract:This project will advance the state of the art of domains such as mathematical logic, order theory and concurrency for reasoning about spatial and epistemic behaviour in multi-agent systems..

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil, Dec 2016

Annabelle McIver, Associate Professor, Macquarie University, Australia, Dec 2016

Carroll Morgan, Professor, University of New South Wales and NICTA, Australia, Dec 2016

Geoffrey Smith, Professor, Florida International University, USA, Dec 2016

Camilo Rueda, Professor, PUJ Cali, Colombia, May 2016 and Nov 2016.

Camilo Rocha, Professor, PUJ Cali, Colombia, Oct 2016.

9.4.2. Visits to International Teams

Catuscia Palamidessi visited the Computer Security team of Roberto Focardi at the University of Venice, Italy, from 4 April to 30 April, 2016.

DICE Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. IXXI

The Dice team is hosted in the Rhoˆne-Alpes Institute for Complex Systems, IXXI, located in Ecole Normale Supe´rieure 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. ARC 6 "Innovative Services for Social Networks"

DICE is involved in a regional project of the Rhoˆne-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.

PESTO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. CNRS

- CNRS PEPS JCJC INS2I 2016 project VESPA *Verifying Equivalence Security in Protocols: Tools and Algorithms*, duration: 1 year, leader: Jannik Dreier, participant: Vincent Cheval.

  Privacy-related notions such as unlinkability and anonymity are usually expressed as equivalence properties, which are notoriously difficult to prove. Due to the complexity of the protocols and the properties, tool support is a must, yet currently rather limited. Notably, there is currently no tool that can verify unlinkability of the electronic passport for an unbounded number of sessions, or anonymity in certain classic electronic cash protocols. The goal of this project is to enable the proofs for these and similar protocols using two complementary approaches: (1) by significantly advancing the state of the art of the algorithms used inside the tools to improve handling of branching and cryptographic primitives, and (2) by providing new reduction results that simplify the tools' inputs.
- CNRS PEPS INS2I 2016 project ASSI *Analyse de Sécurité de Systèmes Industriels*, duration: 1 year, leader: Pascal Lafourcade (Université Clermont-Ferrand), participant PESTO: Jannik Dreier, other participants: Marie-Laure Potet, Maxime Puys (University Grenoble-Alpes).

  The goal of the project is to develop an approach to verify protocols used in industrial control (SCADA) systems using tools such as *TAMARIN* or ProVerif. These protocols have specific security requirements such as flow integrity, going beyond the classical authentication and secrecy properties. The project also aims at analyzing different intruder models matching the particularities of industrial systems, and to develop specific modeling and verification techniques.

9.1.2. ANR

- ANR SEQUOIA *Security properties, process equivalences and automated verification*, duration: 4 years, since 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.

9.1.3. 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, an objective is 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 Pesto (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. The long-term aim of the project is to develop 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, the project is structured in three main tasks. First, we 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 consider the cryptographic part of the primitives that are used in such protocols (encryption, signatures, ...), obtaining higher security guarantees. Third, we propose 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.

  Steve Kremer is the leader of the project.

9.3. International Initiatives

9.3.1. Inria International Partners

- Collaboration with David Basin, Ralf Sasse and Lara Schmid (ETH Zurich), Cas Cremers (University of Oxford), and Sasa Radomirovic (University of Dundee) on the improvement of the *TAMARIN* prover and the elaboration of a user manual.
- 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 Michael Backes and Robert Künnemann (CISPA, Germany) on automated verification of security protocols.
- 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, partly funded as Inria invited researcher
- David Galindo (University of Bimingham), April 2016
- Bogdan Warinschi (University of Bristol), November 2016

[0] http://prosecure.loria.fr

[0] https://members.loria.fr/SKremer/files/spooc/index.html

PRIVATICS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. FUI

8.1.1.1. 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.

8.1.3. Inria Project Labs

8.1.3.1. CAPPRIS

Title: CAPPRIS

Type: Inria Project Lab

Duration: January 2011 - 2016.

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.

8.1.4. Inria CNIL project

8.1.4.1. MOBILITICS

Title: MOBILITICS

Type: joint project.

Duration: January 2012 - Ongoing.

Coordinator: CNIL.

Others partners: CNIL.

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

8.2. European Initiatives

8.2.1. Collaborations in European Programs, ANR Chistera

8.2.1.1. 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.

8.2.1.2. UPRISE-IoT

Title: User-centric PRIvacy & Security in IoT

Programm: CHISTERA

Duration: December 2016 - december 2019

Coordinator: SUPSI (Suisse)

Inria contact: Claude Castelluccia

The call states that “Traditional protection techniques are insufficient to guarantee users’ security and privacy within the future unlimited interconnection”: UPRISE-IoT will firstly identify the threats and model the behaviours in IoT world, and further will build new privacy mechanisms centred around the user. Further, as identified by the call “all aspects of security and privacy of the user data must be under the control of their original owner by means of as simple and efficient technical solutions as possible”, UPRISE-IoT will rise the awareness of data privacy to the users. Finally, it will deeply develop transparency mechanisms to “guarantee both technically and regulatory the neutrality of the future internet.” as requested by the call. The U-HIDE solution developed inn UPRISE-IoT will “empower them to understand and make their own decisions regarding their data, which is essential in gaining informed consent and in ensuring the take-up of IoT technologies”, using a methodology that includes “co-design with users to address the key, fundamental, but inter-related and interdisciplinary aspects of privacy, security and trust.”

8.3. Regional Initiatives

8.3.1. ACDC

Title: ACDC

Type: AGIR 2016 Pole MSTIC.

Duration: September 2016 - 2017.

Coordinator: Inria.

Others partners: UGA.

Abstract: The objective of this project is to evaluate the security and privacy impacts of drone. The project targets 2 milestones: the evaluation of the possiblity to tamper with the drone control/command systems and the capacity of drone to collect private information (for instance text recognition).

8.3.2. 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).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Lucas Melis

Gergely Acs

PROSECCO Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. AnaStaSec

Title: Static Analysis for Security Properties (ANR générique 2014.)

Other partners: Inria/Antique, Inria/Celtique, Airbus Operations SAS, AMOSSYS, CEA-LIST, TrustInSoft

Duration: January 2015 - December 2018.

Coordinator: Jérôme Féret, Inria Antique (France)

Participant: Bruno Blanchet

Abstract: The project aims at using automated static analysis techniques for verifying security and confidentiality properties of critical avionics software.

8.1.1.2. 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.

8.1.1.3. SafeTLS

Title: SafeTLS: La se´curisation de l’Internet du futur avec TLS 1.

Other partners: Université Rennes 1, IRMAR, Inria Sophia Antipolis, SGDSN/ANSSI

Duration: October 2016 - September 2020

Coordinator: Pierre-Alain Fouque, Univesité de Rennes 1 (France)

Abstract: Our project, SafeTLS, addresses the security of both TLS 1.3 and of TLS 1.2 as they are (expected to be) used, in three important ways: (1) A better understanding: We will provide a better understanding of how TLS 1.2 and 1.3 are used in real-world applications; (2) Empowering clients: By developing a tool that will show clients the quality of their TLS connection and inform them of potential security and privacy risks; (3) Analyzing implementations: We will analyze the soundness of current TLS 1.2 implementations and use automated verification to provide a backbone of a secure TLS 1.3 implementation.

8.1.1.4. QuickChick

Title: QuickChick: Property-based Testing for Coq

Coordinator: Catalin Hritcu

Abstract: The goal of the project was to develop a property-based testing framework for Coq proofs. Catalin Hritcu was awarded an ANR Jeune Chercheur/Jeune Chercheuse grant to pursue this project, but he declined it in favour of his ERC Starting Grant SECOMP (described below.)

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. ERC Consolidator Grant: CIRCUS

Title: CIRCUS: An end-to-end verification architecture for building Certified Implementations of Robust, Cryptographically Secure web applications

Duration: April 2016 - March 2021

Coordinator: Karthikeyan Bhargavn, Inria

Abstract: The security of modern web applications depends on a variety of critical components including cryptographic libraries, Transport Layer Security (TLS), browser security mechanisms, and single sign-on protocols. Although these components are widely used, their security guarantees remain poorly understood, leading to subtle bugs and frequent attacks. Rather than fixing one attack at a time, we advocate the use of formal security verification to identify and eliminate entire classes of vulnerabilities in one go.

CIRCUS proposes to take on this challenge, by verifying the end-to-end security of web applications running in mainstream software. The key idea is to identify the core security components of web browsers and servers and replace them by rigorously verified components that offer the same functionality but with robust security guarantees.

8.2.1.2. ERC Starting Grant: SECOMP

Title: SECOMP: Efficient Formally Secure Compilers to a Tagged Architecture

Duration: Jan 2017 - December 2021

Coordinator: Catalin Hritcu, Inria

Abstract: This new ERC-funded project called SECOMP1 is aimed at leveraging emerging hardware capabilities for fine-grained protection to build the first, efficient secure compilers for realistic programming languages, both low-level (the C language) and high-level (F*, a dependently-typed ML variant). These compilers will provide a secure semantics for all programs and will ensure that high-level abstractions cannot be violated even when interacting with untrusted low-level code. To achieve this level of security without sacrificing efficiency, our secure compilers will target a tagged architecture, which associates a metadata tag to each word and efficiently propagates and checks tags according to software-defined rules. We will use property-based testing and formal verification to provide high confidence that our compilers are indeed secure.

8.2.1.3. NEXTLEAP

Title: NEXTLEAP: NEXT generation Legal Encryption And Privacy

Programm: H2020

Duration: January 2016 - December 2018

Coordinator: Harry Halpin, Inria

Other partners: IMDEA, University College London, CNRS, IRI, and Merlinux

Abstract: NEXTLEAP aims to create, validate, and deploy protocols that can serve as pillars for a secure, trust-worthy, and privacy-respecting Internet. For this purpose NEXTLEAP will develop an interdisciplinary study of decentralisation that provides the basis on which these protocols cann be designed, working with sociologists to understand user needs. The modular specification of decentralized protocols, implemented as verified open-source software modules, will be done for both privacy-preserving secure federated identity as well as decentralized secure messaging services that hide metadata (e.g., who, when, how often, etc.).

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. 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

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Carmela Troncoso from IMDEA visited the group from 17-18th October and gave a seminar “Traffic Analysis - When Encryption is not Enough to Protect Privacy”

8.4.1.1. Internships

- Alejandro Aguirre: Apr 2016 until Aug 2016
- Abhishek Bichhawat: Sep 2016 until Dec 2016
- Diane Gallois-Wong: Mar 2016 until Aug 2016
- Ritobroto Maitra: May 2016 until Aug 2016
- Guido Martinez: Jan 2016 until Jun 2016
- Jianyang Pan: May 2016 until Aug 2016
- Marina Polubelova: Sep 2016 until Nov 2016
- Natalia Kulatova: May 2016 until Aug 2016
- Vinay Yogendra: May 2016 until Jul 2016

8.4.2. Visits to International Teams

- Bruno Blanchet, March 14 to June 10, 2016, Google, Mountain View.
- Catalin Hritcu, October to November 2016, Microsoft Research, Redmond, USA.

TAMIS Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

ARED grant for Nisrine Jafri.

Postdocs grants for Fabrizio Biondi, Jeffrey Paul Burdges, Florian Dold, Ronan Lashermes.

9.2. National Initiatives

9.2.1. ANR

- ANR MALTHY, Méthodes ALgèbriques pour la vérification de modèles Temporisés et HYbrides, Thao Dang, 4 years, Inria and VISEO and CEA and VERIMAG
- ANR COGITO, Runtime Code Generation to Secure Devices,, 3 years, Inria and CEA and ENSMSE and XLIM.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. ACANTO

Participants: Axel Legay, Thomas Given-Wilson, Sean Sedwards, Olivier Zendra.

Start: 2015. End: 2018.

The population of the advanced countries is ageing. This simple and widely recognised fact has important implications for health, society and economics. The most evident is in the number of people who report activity limitations, which grows significantly with age as clearly shown in the following chart. Activity limitations have an adverse effect on a person's productivity, on the quality of her social relations and, ultimately, on her quality of life. Policy makers confronted with a problem of challenging complexity: how to develop an effective strategy to fight the physical and cognitive decline of older adults in the face of ever shrinking financial resources for health care and social services.

In this context, technology can be of considerable help to care–givers to extend the range and the efficacy of their actions. The ACANTO project (http://www.ict-acanto.eu) aims to develop a portfolio of technical solution that can serve this purpose. More specifically, our goal is to spur older adults into a sustainable and regular level of physical exercise under the guidance and the supervision of their carers.

The key elements of ACANTO are a robotic friend (the FriWalk) that sup-ports the user in the execution of daily activities that require physical exercise and an intelligent system that recommends activites that a senior user perceives as compelling and rewarding.

The FriWalk takes the form of a standard walking assistant, but it is in fact an intelligent robot that is able to localise itself, to sense the surrounding environment, to plan a course of action that suits the user needs and to guide the user along safe routes. The FriWalk is also a personal trainer that can support the user in the execution of a training programme, monitor the motion of the user in search of muscular or gait problems and report them into the user profile (that can be inspected by doctors and physicians).

The second key idea of ACANTO is that physical exercise is actually "concealed" within compelling activities (such as shopping, taking walks in museums and exhibitions etc.). Such activities have a social dimension (they are proposed to group of users) and are chosen based on the interest and on the past experiences of the user. At the heart of the recommendation system there is a social network which is created and developed by primarily using information collected by the FriWalk using "physical" observations on her behaviour and on her emotional state. For this reason, we call this social network "cyberphysical".

This project aims at developping an autonomous system to drive groups of citizens with respect to point of interest. Those citizens are supposed to communicate, and one of the objective of Tamis is to build a robust and secure system to guarantee this communication. Axel Legay and Olivier Zendra are the permanent researchers of Tamis involved in this project. The project supports two postdocs in Tamis.

9.3.1.2. DIVIDEND

Participant: Laurent Morin.

Start: 2014. End: 2017.

The DIVIDEND project (http://www.chistera.eu/projects/dividend) attacks the data centre energy efficiency bottleneck through vertical integration, specialisation, and cross-layer optimization. Our vision is to present heterogeneous data centres, combining CPUs, GPUs, and task-specific accelerators, as a unified entity to the application developer and let the runtime optimize the utilization of the system resources during task execution. DIVIDEND embraces heterogeneity to dramatically lower the energy per task through extensive hardware specialisation while maintaining the ease of programmability of a homogeneous architecture. To lower communication latency and energy, DIVIDEND refers a lean point-to-point messaging fabric over complex connection-oriented network protocols. DIVIDEND addresses the programmability challenge by adapting and extending the industry-led heterogeneous systems architecture programming language and runtime initiative to account for energy awareness and data movement. DIVIDEND provides for a cross-layer energy optimization framework via a set of APIs for energy accounting and feedback between hardware, compilation, runtime, and application layers. The DIVIDEND project will usher in a new class of vertically integrated data centres and will take a first stab at resolving the energy crisis by improving the power usage effectiveness of data centres.

Laurent Morin from Tamis is involved in this project

9.3.1.3. EMC^2

Participants: Axel Legay, Olivier Zendra.

Start: 2014. End: 2017.

EMC^2 (Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments https://www.artemis-emc2.eu) is an ARTEMIS Joint Undertaking project in the Innovation Pilot Programme ‘Computing platforms for embedded systems’ (AIPP5). Embedded systems are the key innovation driver to improve almost all mechatronic products with cheaper and even new functionalities. They support today’s information society as inter-system communication enabler. A major industrial challenge arises from the need to face cost efficient integration of different applications with different levels of safety and security on a single computing platform in an open context. EMC^2 finds solutions for dynamic adaptability in open systems, provides 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. The objective of EMC^2 is to establish Multi-Core technology in all relevant Embedded Systems domains. EMC^2 is a project of 99 partners of embedded industry and research from 19 European countries with an effort of about 800 person years and a total budget of about 100 million Euro.

EMC2 (2014–2017) is at the border between formal methods and security. We in Tamis are mainly using the fundings to develop the Plasma toolset that is used by our statistical model checking and symbolic model checking tools. The permanent members of Tamis who are involved are Axel Legay and Olivier Zendra. The project was initiated during the lifetime of the ESTASYS.Inria team.

9.3.1.4. ENABLE-S3

Participants: Axel Legay, Jean-Louis Lanet.

Start: 2016. End: 2019.

The objective of ENABLE-S3 (http://www.enable-s3.eu) is to establish cost-efficient cross-domain virtual and semi-virtual V&V platforms and methods for ACPS. Advanced functional, safety and security test methods will be developed in order to significantly reduce the verification and validation time but preserve the validity of the tests for the requested high operation range. ENABLE-S3 aspires to substitute today's physical validation and verification efforts by virtual testing and verification, coverage-oriented test selection methods and standardization. ENABLE-S3 is use-case driven; these use cases represent relevant environments and scenarios. Each of the models, methods and tools integrated into the validation platform will be applied to at least one use case (under the guidance of the V&V methodology), where they will be validated (TRL 5) and their usability demonstrated (TRL6). Representative use cases and according applications provide the base for the requirements of methods and tools, as well as for the evaluation of automated systems and respective safety.

This project is industry driven and has the objective of designing new technologies for autonomous transportation, including to secure them. Tamis tests its results on the case studies of the project. Axel Legay and Jean-Louis Lanet are involved in this project. The project supports one postdoc in Tamis starting in 2017.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Clémentine MAURICE (Graz University of Technology, Institute of Applied Information Processing and Communications, Austria) visited Tamis and also gave a talk on Reverse-engineering CPUs for fun and profit.

9.4.2. Visits to International Teams

- Axel Legay stayed at Namur University, Belgium.
- Axel Legay stayed at University of Limerick, Ireland.
- Axel Legay and Sean Sedwards stayed at Aalborg University, Denmark.
- Axel Legay, Fabrizio Biondi and Thomas Given-Wilson stayed at John Hopkins University, USA.