RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2017

Section Partnerships and Cooperations

Edition: 2018-02-19

ALGORITHMICS, COMPUTER ALGEBRA AND CRYPTOLOGY

ARCHITECTURE, LANGUAGES AND COMPILATION

EMBEDDED AND REAL-TIME SYSTEMS

PROOFS AND VERIFICATION

SECURITY AND CONFIDENTIALITY

ARIC Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

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

9.2. National Initiatives

9.2.1. 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.

9.2.2. ANR FastRelax Project

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

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

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

9.2.3. ANR MetaLibm Project

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

MetaLibm is a four-year project (started in October 2013 and recently extended till March 2018) focused on the design and implementation of code generators for mathematical functions and filters. The web page of the project is http://www.metalibm.org/ANRMetaLibm/. It is headed by Florent de Dinechin (INSA Lyon and Socrate team) and, besides Socrate and AriC, also involves teams from LIRMM (Perpignan), LIP6 (Paris), CERN (Geneva), and Kalray (Grenoble). The main goals of the project are to automate the development of mathematical libraries (libm), to extend it beyond standard functions, and to make it unified with similar approaches developed in or useful for signal processing (filter design). Within AriC, we are especially interested in studying the properties of fixed-point arithmetic and floating-point arithmetic that can help develop such a framework.

9.2.4. ANR ALAMBIC Project

Participants: Benoît Libert, Fabien Laguillaumie, Ida Tucker.

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.

9.2.5. RISQ Project

Participants: Benoît Libert, Fabien Laguillaumie, Damien Stehlé, Chitchanok Chuengsatiansup.

RISQ (Regroupement de l'Industrie française pour la Sécurité Post – Quantique) is a BPI-DGE four-year project (started in January 2017) focused on the transfer of post-quantum cryptography from academia to industrial poducts. The web page of the project is http://risq.fr. It is headed by Secure-IC and, besides AriC, also involves teams from ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Airbus, C& S (Communication et Systèmes), CEA (CEA-List), CryptoExperts, Gemalto, Orange, Thales Communications & Security, Paris Center for Quantum Computing, the EMSEC team of IRISA, and the Cascade and Polsys Inria teams. The outcome of this project will include an exhaustive encryption and transaction signature product line, as well as an adaptation of the TLS protocol. Hardware and software cryptographic solutions meeting these constraints in terms of security and embedded integration will also be included. Furthermore, documents guiding industrials on the integration of these post-quantum technologies into complex systems (defense, cloud, identity and payment markets) will be produced, as well as reports on the activities of standardization committees.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. 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.

9.3.1.2. PROMETHEUS Project

Participants: Benoît Libert, Fabien Laguillaumie, Damien Stehlé.

PROMETHEUS (Privacy-Preserving Systems from Advanced Cryptographic Mechanisms Using Lattices) is a 4-year European H2020 project (call H2020-DS-2016-2017, Cybersecurity PPP Cryptography, DS-06-2017) that will start in January 2018. It gathers 7 academic partners (ENS de Lyon and Université de Rennes 1; CWI, Pays-Bas; Royal Holloway University of London, United Kingdom; Universitat Politècnica de Catalunya, Spain; Ruhr-Universität Bochum, Germany; Weizmann Institute, Israel), 5 industrial partners (Orange, IBM, Thales, TNO, Scytl). The goal of this project is to develop a toolbox of privacy-preserving cryptographic algorithms and protocols (like group signatures, anonymous credentials, or digital cash systems) that resist quantum adversaries. Solutions will be mainly considered in the context of Euclidean lattices and they will be analyzed from a theoretical point of view (i.e., from a provable security aspect) and a practical angle (which covers the security of cryptographic implementations and side-channel leakages). The project is hosted by ENS de Lyon and Benoît Libert is the administrative coordinator while Orange is the scientific leader.

9.4. International Initiatives

9.4.1. Participation in International Programs

Vincent Lefèvre participated in the standardization of interval arithmetic (simplified version of the standard, IEEE 1788.1). He actively participates in the revision of the IEEE 754 standard for 2018.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- Lloyd Nicholas Trefethen, from Oxford University (UK), is an expert in numerical analysis and notably the systematic use of Chebyshev approximation. He is spending the academic year 2017-2018 with AriC.
- Warwick Tucker, from Uppsala University (Sweden), is an expert of certified computation for dynamical systems. He is spending the academic year 2017-2018 with AriC.
- Huaxiong Wang, from Nanyang Technological University (Singapore), is an expert in cryptographic protocols and multi-party computation. He visited us in March and April 2017.
- Jung Hee Cheon, from Seoul National University (South Korea), is an expert in algorithmic number theory and the mathematical foundations of cryptography. He is visiting us since October 2017, until January 2018.

9.5.2. Internships

Benjamin Graillot

Date: May 2017–July 2017

Institution: ENS de Cachan

Supervisor: Bruno Salvy

9.5.3. Visits to International Teams

9.5.3.1. Research Stays Abroad

Benoît Libert spent one month in the cryptography team of Nanyang Technological University (Singapore), to collaborate with Khoa Nguyen and Huaxiong Wang.

AROMATH Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Our team AROMATH participates to the VADER project for VIRTUAL MODELING of RESPIRATION, UCA Jedi, axis "Modélisation, Physique et Mathématique du vivant". http://benjamin.mauroy.free.fr/VADER.

8.2. European Initiatives

8.2.1. 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.

8.2.2. Collaborations in European Programs, Except FP7 & H2020

Program: Partnership Agreement for the Development Framework

Project acronym: RANWALK

Project title: Random walks for the computation of potential and capacitance of electronic circuits

Duration: December 2017 - May 2020

Coordinator: C. Bakolias (Helic S.A.)

Scientist-in-charge at Inria: I.Z. Emiris (NKUA, Athens, Greece, and ATHENA Research Innovation Center)

Other partners: ATHENA Research Innovation Center, Maroussi (Greece), School of Electrical Engineering, U. Patras (Greece).

Abstract: The Project aims at reducing the fabrication cost of new generation circuits and achieve significant progress in Electronic Design Automation (EDA) of Integrated Circuits with the development of innovative technology, which will radically upgrade Helic's existing products by giving them a unique lead in the global market. A key element of the modeling engine and the general approach is the method of random walks between a set of conductors, based on the solution of the Laplace equation and the calculation of the Green function in cubic-shaped areas. We target the geometric modeling of the physical design of the conductors, as well as the efficient and robust calculation of the above electrostatic parameters, with the ultimate goal of a rapid simulation of the circuit's accuracy. We focus on calculating the maximum cube gap between rectangular elements and, for this, we develop large-scale geometric software.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Vlada Pototskaia, University of Göttingen (Germany), visited from August 28th to September 15th. The collaboration with E. Hubert and B. Mourrain concerned AAK theory and its applications to approximate low rank sums of exponentials.

Ibrahim Nonkané, University of Ouagadougou, visited from September 25th to October 9th to work with L. Busé on the discriminant of complete intersections in a projective space.

Sotirios Choularias, Unversity of Strachlyde (Scotland), visited us from August 5th to November 5th in the context of his secondment in the ITN network ARCADES, to work on boundary element methods and isogeometric analysis.

Yairon Cid Ruiz, University of Barcelona (Spain), visits us since October 1st, to work with L. Busé on the birationality of bi-graded rational maps in small dimensions.

Roser Homs Pons, University of Barcelona (Spain), visited us from October 9th to December 15th, to work with B. Mourrain on effective methods for the construction of Gorenstein algebra of low colength.

Simon Telen, University of Leuven (Belgium), visited us from August 24th to September 24th, to work with B. Mourrain on algebraic solvers and numerical linear algebra.

Meng Wu, University of Hefei (China), visited us from September 4th to September 29th, to work with B. Mourrain on isogeometric analysis and its applications.

Gang Xu, Hangzhou Dianzi University (China) visited us from September 7th to September 15th, to work with B. Mourrain on parameterization of computation domains for isogeometric analysis.

8.3.1.1. Internships

Antoine Deharveng, student at the engineer school of the University of Nice Sophia Antipolis, did his PFE (Projet de fin d'étude) with L. Busé until March 2017. He developed the interpolation of cylinders and cones passing through minimal point sets in the C++ library ASurfExt (https://gitlab.inria.fr/lbuse/ASurfExt/wikis/home).

Andrien Boudin did his internship with L. Busé from June 15th to September 15th. He developed and implemented a new method for the interpolation of torus through a minimal point set in the C++ library ASurfExt (https://gitlab.inria.fr/lbuse/ASurfExt/wikis/home).

Thomas Laporte, student at the engineer school of the University of Nice Sophia Antipolis, did his internship with A. Galligo from June 15th to September 15th. He studied "Hand modeling" and implemented in Axel a method inspired by the paper by P AULY .M, T AGLIASACCHI .A, T KACH .A. Sphere-Meshes for Real-Time Hand Modeling and Tracking. ACM Transactions on Graphics 2016. (Proc. of SIGGRAPH Asia).

Emmanouil Christoforou, Master student from NKUA, works from September 4th to December 31th on software development for the algebraic-geometric modeler Axel.

8.3.1.2. Research Stays Abroad

F. Yildirim was on secondment at Barcelona university (Spain), with Carlos D'Andrea, for 3 months (September 15-December 15).

A. Fuentes Suarez was on secondment at Athens university (Greece), with Ioannis Emiris, for 4 months (September-December).

A. Blidia was on secondment at Evolute, Vienna (Austria), with A. Schiftner (Evolute) and H. Pottmann (TUW), for 3 months (November-January).

E. Hubert received a grant from the London Mathematics Society to visit the University of Kent in Canterburry (UK) from February 21st to March 1st.

CARAMBA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. PEPS CHARIoT

The PEPS CHARIoT (“CHiffrement Authentifié pour Renforcer l’IoT”) project is dedicated to the study of authenticated encryption schemes, especially the CAESAR candidates, and to the performance analysis of those schemes on dedicated embedded architectures such as micro-controllers (MSP430, ARM and AVR). It involves Marine Minier (CARAMBA), Franck Rousseau (IMAG - Grenoble) and Pascal Lafourcade (LIMOS-UCA - Clermont-Ferrand).

9.2. International Research Visitors

9.2.1. Visits of International Scientists

Thorsten Kleinjung from EPFL visited the team from 6 to 10 February to work on the Number Field Sieve algorithm.

7. Partnerships and Cooperations

7.1. National Initiatives with Industry

7.1.1. 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.

7.1.2. RISQ

Program: GDN

Duration: February 2017 – September 2020

Coordinator: Secure-IC

Partners: ANSSI, AIRBUS, C-S, CEA LIST, CryptoExperts, Inria/ENS/CASCADE, GEMALTO, Inria POLSYS, Inria AriC, IRISA, Orange Labs, THALES, UVSQ, PCQC

Local coordinator: Michel Abdalla

The main goal of RISQ is to help the French Industry and Academia become a significant international player in the transition to post-quantum cryptography.

7.2. National Collaborations within Academics

7.2.1. EnBiD

Title: Encryption for Big Data

Program: ANR JCJC

Duration: October 2014 – September 2018

PI: Hoeteck Wee

Partners: Université Paris 2, Université 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.

7.2.2. EfTrEC

Title: Efficient Transferable E-Cash

Program: ANR JCJC

Duration: October 2016 – September 2020

PI: Georg Fuchsbauer

Partners: Université 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.

7.2.3. ALAMBIC

Title: AppLicAtions of MalleaBIlity in Cryptography

Program: ANR PRC

Duration: October 2016 – September 2020

PI: Damien Vergnaud

Partners: ENS Lyon, Université 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 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), Inria/ENS (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.

7.3.6. FENTEC

Title: Functional Encryption Technologies

Program: H2020

Duration: January 2018 – December 2020

Coordinator: ATOS Spain SA

Scientific coordinator: Michel Abdalla

Partners: Inria/ENS (France), Flensburg University (Germany), KU Leuven (Belgium), University of Helsinki (Finland), Nagra (Switzerland), XLAB (Switzerland), University of Edinburgh (United Kingdom), WALLIX (France)

Local coordinator: Michel Abdalla

Functional encryption (FE) has recently been introduced as a new paradigm of encryption systems to overcome all-or-nothing limitations of classical encryption. In an FE system the decryptor deciphers a function over the message plaintext: such functional decryptability makes it feasible to process encrypted data (e.g. on the Internet) and obtain partial view of the message plaintext. This extra flexibility over classical encryption is a powerful enabler for many emerging security technologies (i.e. controlled access, searching and computing on encrypted data, program obfuscation...). FENTEC's mission is to make the functional encryption paradigm ready for wide-range applications, integrating it in ICT technologies as naturally as classical encryption. The primary objective is the efficient and application-oriented development of functional encryption systems. FENTEC's team of cryptographers, software and hardware experts and information technology industry partners will document functional encryption needs of specific applications and subsequently design, develop, implement and demonstrate applied use of functional cryptography. Ultimately, a functional encryption library for both SW and HW-oriented application will be documented and made public so that it may be used by European ICT entities. With it, the FENTEC team will build emerging security technologies that increase the trustworthiness of the European ICT services and products. Concretely, the FENTEC team will showcase the expressiveness and versatility of the functional encryption paradigm in 3 use cases:

- Privacy-preserving digital currency, enforcing flexible auditing models
- Anonymous data analytics enabling computation of statistics over encrypted data, protecting European Fundamental Rights of Data Protection and Privacy
- Key and content distribution with improved performance & efficiency as foundational technology for establishing secure communication among a vast amount of IOT devices.

7.4. International Initiatives with Industry

7.4.1. CryPrivBC

Title: Cryptography for Privacy on the Blockchain

Partners: MSR Redmond (USA), MSR Cambridge (UK), Inria

Duration: October 2017 – October 2021

PI: Georg Fuchsbauer

The goal of this Microsoft-Inria joint project on privacy and decentralization is to use cryptography to improve privacy on the blockchain. We will investigate means of privacy-preserving authentication, such as electronic currencies, and other applications of blockchain and distributed transparency mechanisms.

7.5. International Research Visitors

- Melissa Chase (MSR Redmond)
- Huijia Rachel Lin (UCSB)
- Yuval Ishai (Technion)
- Stefano Tessaro (UCSB)
- Vinod Vaikuntanathan (MIT)

DATASHAPE Project-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 from October 2013 to September 2017.

- 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. GUDHI

Title: Algorithmic Foundations of Geometry Understanding in Higher Dimensions

Programm: FP7

Type: ERC

Duration: February 2014 - January 2019

Coordinator: Inria

Inria contact: 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, Mathematical Sciences Publishers, Canada (June and November 2017)

Arijit Ghosh, Indian Statistical Institute, Kolkata (June and november 2017)

Kim Jisu, CMU, Pittsburgh, USA (November 2017).

Wolfgang Polonik, UC Davis, USA (June 2017).

Konstantin Mischaikow, Rutgers University, USA, (November 2017).

Magnus Botnan, TU Munich, Germany (March 2017).

Sara Kalisnik, MPI, Germany (November 2017).

9.4.1.1. Internships

Divyansh Pareek, IIT Bombay (May-July 2017)

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

Vincent Divol, UC Davis (April-June 2017)

GAMBLE Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

We organized, with colleagues of the mathematics department (Institut Elie Cartan Nancy) a regular working group about geometry and probability.

9.2. National Initiatives

9.2.1. 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.

The project has a total budget of 100kE. It started on March 1st 2014 and will finished in August 2018. It is coordinated by Guillaume Moroz, with a participation of 60%, and Marc Pouget with a participation of 40%.

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

9.3. International Initiatives

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

9.3.1.1. Astonishing

Title: ASsociate Team On Non-ISH euclIdeaN Geometry

International Partners (Institution - Laboratory - Researcher):

University of Groningen (Netherlands) - Johann Bernouilli Institute of Mathematics and Computer Science - Gert Vegter

University of Luxembourg - Mathematics Research Unit - Jean-Marc Schlenker

Université Paris Est Marne-la-Vallée - Laboratoire d'Informatique Gaspard Monge - Éric Colin de Verdière

Start year: 2017

See also: https://members.loria.fr/Monique.Teillaud/collab/Astonishing/

Some research directions in computational geometry have hardly been explored. The spaces in which most algorithms have been designed are the Euclidean spaces R^d. To extend further the scope of applicability of computational geometry, other spaces must be considered, as shown by the concrete needs expressed by our contacts in various fields as well as in the literature. Delaunay triangulations in non-Euclidean spaces are required, e.g., in geometric modeling, neuromathematics, or physics. Topological problems for curves and graphs on surfaces arise in various applications in computer graphics and road map design. Providing robust implementations of these results is a key towards their reusability in more applied fields. We aim at studying various structures and algorithms in other spaces than R^d, 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.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Gert Vegter spent three weeks in GAMBLE in the framework of the Astonishing associate team.

9.4.2. Visits to International Teams

Olivier Devillers spent one month at Computational Geometry Lab of Carleton University http://cglab.ca/about.html.

GRACE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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/.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: TECHNISCHE UNIVERSITEIT EINDHOVEN

Partners:

Academia Sinica (Taiwan)
Bundesdruckerei (Germany)
Danmarks Tekniske Universitet (Denmark)
Katholieke Universiteit Leuven (Belgium)
Nxp Semiconductors Belgium Nv (Belgium)
Ruhr-Universitaet Bochum (Germany)
Stichting Katholieke Universiteit (Netherlands)
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.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

B. Smith has continued our successful informal partnership with the cryptography research group at Radboud University, Nijmegen (NL). 2017 has seen visits from researchers in both directions, and the production of the **qDSA** signature scheme package.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Beth Malmskog (Colorado College) visited the team from November 27 to December 1 2017 and gave a talk on locally recoverable codes based on fibre products of algebraic curves.

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

B. Smith was an invited researcher in the Computer Science department at CINVESTAV (Mexico City, Mexico) for the month of August 2017, hosted by Professor Francisco Rodríguez Henríquez.

J. Lavauzelle visited Incidence Geometry team at Gent University (Belgium) for the month of April 2017, hosted by Professor Leo Storme.

E. Barelli visited the COMPUTE team in the DTU University at Lyngby (Danemark) during one month in february-march 2017, hosted by Professor Peter Beelen.

LFANT Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. 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

Title: OpenDreamKit

Program: H2020

Duration: January 2016 - December 2020

Coordinator: Nicolas Thiéry

Inria contact: Karim Belabas

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

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

7.3. International Initiatives

7.3.1. Inria International Labs

7.3.1.1. FAST

Title: (Harder Better) FAster STronger cryptography

International Partner

Université des Sciences et Techniques de Masuku (Gabon) - Tony Ezome and the PRMAIS project

Start year: 2017

See also: https://www.inria.fr/en/associate-team/fast

The project aims to develop better algorithms for elliptic curve cryptography with prospect of the two challenges ahead: - securing the internet of things - preparing towards quantum computers.

Elliptic curves are currently the fastest public-key cryptosystem (with a key size that can fit on embeded devices) while still through a different mode of operation beeing (possibly) able to resist quantum based computers.

Activities for this year involved the funding of Luca De Feo to speak at the EMA "Mathématiques pour la Cryptographie Post-quantique et Mathématiques pour le Traitement du Signal", organised by Djiby Sow and Abdoul Asiz Ciss organised an EMA at the École Polytechnique de Thiès (Sénégal) from May 10 to May 23, about "Cryptographie à base d'isogénies"; the visit of Abdoulaye Maiga to the LFANT team where he worked with Damien Robert to find absolute invariants of good reduction modulo 2 for abelian surfaces; and the organisation by Damien Robert of a workshop in Bordeaux with most of the team members from September 04 to September 08. The slides or proceedings are available at https://lfant.math.u-bordeaux.fr/index.php?category=seminar&page=2017.

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 Damien Stehlé (ENS Lyon), Cécile Pierrot (Centrum Wiskunde and Informatica, Amsterdam), Christophe Petit (Oxford), Benjamin Wesolowski (EPFL), Bernhard Schmidt (Nanyang Technological University, Singapore), Mohamadou Sall (Université Cheikh Anta Diop, Dakar, Sénégal), Emmanuel Fouotsa (The University of Bamenda, Cameroon), Abdoulaye Maiga (Université Cheikh Anta Diop, Dakar, Sénégal), Tony Ezome (Université des Sciences et Techniques de Masuku (USTM), Franceville, Gabon), Abdoul Aziz Ciss (Université Cheikh Anta Diop, Dakar, Sénégal), José Manuel Rodriguez Caballero (Labri), Jean Kieffer (ENS Paris), Christian Klein (Institut de Mathématiques de Bourgogne), Frank Vallentin (Mathematisches Institut, Universität zu Köln).

7.4.2. Visits to International Teams

Jared Asuncion went to the Autumn school: Topics in arithmetic and algebraic geometry last 9 - 13 October 2017 at the University of Mainz in Mainz, Germany.

Jared Asuncion went to see his cosupervisor, Marco String last 6 - 10 November 2017 at the Universiteit Leiden in Leiden, The Netherlands. It is planned to stay in Leiden for a period of six months while working on his PhD.

Jared Asuncion went to the 21st Workshop on Elliptic Curve Cryptography last 13 - 15 November 2017 at the Radboud University in Nijmegen, The Netherlands.

A. Page visited C. Maire in Cornell University (Ithaca, US) from November 27th to December 4th and gave a research talk there on December 1st. He then visited Michael Lipnowski in the Institute for Advanced Studies (Princeton, US) from December 4th to December 14th.

A. Enge visited Bernhard Schmidt in Nanyang Technological University, Singapore for three weeks.

Fredrik Johansson participated in the OSCAR: Antic workshop at TU Kaiserslautern, Germany and gave an invited talk on "Fundamental algorithms in Arb".

Fredrik Johansson participated in the workshop on Elliptic Integrals, Elliptic Functions and Modular Forms in Quantum Field Theory at DESY, Zeuthen, Germany, and gave an invited talk on "Numerics of classical elliptic functions, elliptic integrals and modular forms".

POLSYS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- **French Ministry of Armies**

  POLSYS has a collaboration with the French Ministry of Armies.

- **Grant GAMMA** (funded by PGMO).

  GLOBAL ALGEBRAIC SHOOTING METHOD IN OPTIMAL CONTROL AND APPLICATIONS

  Optimal control consists in steering a system from an initial configuration to a final one, while minimizing some given cost criterion. One of the current main challenges is to develop innovative methods for computing global solutions. This is crucial for applications where validating the global control laws is a crucial but a highly time consuming and expensive phase. GAMMA focuses on the wide range of optimal control problems having an algebraic structure, involving for instance polynomial or semi-algebraic dynamics and costs, or switches between polynomial models. In this case, GAMMA aims at designing methods relying on algebraic computations to the mainstream shooting method in order to yield optimal solutions that purely numerical techniques cannot provide.

8.2. National Initiatives

8.2.1. ANR

- **ANR Jeunes Chercheurs GALOP (Games through the lens of ALgebra and OPptimization)**

  `Duration:` 2018–2022

  GALOP is a Young Researchers (JCJC) project with the purpose of extending the limits of the state-of-the-art algebraic tools in computer science, especially in stochastic games. It brings original and innovative algebraic tools, based on symbolic-numeric computing, that exploit the geometry and the structure and complement the state-of-the-art. We support our theoretical tools with a highly efficient open-source software for solving polynomials. Using our algebraic tools we study the geometry of the central curve of (semi-definite) optimization problems. The algebraic tools and our results from the geometry of optimization pave the way to introduce algorithms and precise bounds for stochastic games.

  `Participants:` E. Tsigaridas [contact], F. Johansson, H. Gimbert, J.-C. Faugère, M. Safey El Din.

8.2.2. Programme d'investissements d'avenir (PIA)

- **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).

  The RISQ project is certainly the biggest industrial project ever organized in quantum-safe cryptography. RISQ is one of few projects accepted in the call Grands Défis du Numérique which is managed by BPI France, and will be funded thanks to the so-called Plan d'Investissements d'Avenir.

  The RISQ project is a natural continuation of POLSYS commitment to the industrial transfert of quantum-safe cryptography. RISQ is a large scale version of the HFEBoost project; which demonstrated the potential of quantum-safe cryptography.

  POLSYS actively participated to shape the RISQ project. POLSYS is now a member of the strategic board of RISQ, and is leading the task of designing and analyzing quantum-safe algorithms. In particular, a first milestone of this task was to prepare submissions to NIST's quantum-safe standardisation process.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

8.3.1.1. A3

Type: PEOPLE

Instrument: Career Integration Grant

Duration: May 2013 - Apr. 2017

Coordinator: Jean-Charles Faugère

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

Inria contact: Elias Tsigaridas

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

8.3.2. Collaborations in European Programs, Except FP7 & H2020

Program: COST

Project acronym: CryptoAction

Project title: Cryptography for Secure Digital Interaction

Duration: Apr. 2014 - Apr. 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: Dec. 2014 - Dec. 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.

8.4. International Initiatives

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

8.4.1.1. 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.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- May – July 2017, Delaram Kahrobaei, Professor, CUNY, NYC, USA

8.5.1.1. Internships

- May – July 2017, Kelsey Horan, PhD student, CUNY, NYC, USA.
- Apr. – Nov. 2017, Eliane Koussa, Université de Versailles
- Apr. – Aug. 2017, Pascal Fong, Université de Versailles

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- **ANR BRUTUS** ($10/14 \to 09/18$)
  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** ($10/16 \to 09/21$)
  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.
- **ANR CBCRYPT** ($10/17 \to 09/21$)
  Code-based cryptography
  ANR Program: AAP Générique 2017
  Partners: Inria SECRET (coordinator), XLIM, Univ. Rouen, Univ. Bordeaux.
  197 kEuros
  The goal of CBCRYPT is to propose code-based candidates to the NIST call aiming at standardizing public-key primitives which resist to quantum attacks. These proposals are based either on code-based schemes relying on the usual Hamming metric or on the rank metric. The project does not deal solely with the NIST call. We also develop some other code-based solutions: these are either primitives that are not mature enough to be proposed in the first NIST call or whose functionalities are not covered by the NIST call, such as identity-based encryption, broadcast encryption, attribute based encryption or functional encryption. A third goal of this project is of a more fundamental nature: namely to lay firm foundations for code-based cryptography by developing thorough and rigorous security proofs together with a set of algorithmic tools for assessing the security of code-based cryptography.

- **ANR quBIC** ($10/17 \rightarrow 09/21$)
  Quantum Banknotes and Information-Theoretic Credit Cards
  ANR Program: AAP Générique 2017
  Partners: Univ. Paris-Diderot (coordinator), Inria SECRET, UPMC (LIP6), CNRS (Laboratoire Kastler Brossel)
  87 kEuros
  For a quantum-safe future, classical security systems as well as quantum protocols that guarantee security against all adversaries must be deployed. Here, we will study and implement one of the most promising quantum applications, namely unforgeable quantum money. A money scheme enables a secure transaction between a client, a vendor and a bank via the use of a credit card or via the use of banknotes, with maximal security guarantees. Our objectives are to perform a theoretical analysis of quantum money schemes, in realistic conditions and for encodings in both discrete and continuous variables, and to demonstrate experimentally these protocols using state-of-the-art quantum memories and integrated detection devices.

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

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

NXP Semiconductors Belgium Nv (Belgium)

Ruhr-Universitaet Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

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

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.

9.2.1.3. ERC QUASYModo

Title: QUASYModo *Symmetric Cryptography in the Post-Quantum World*

Program: ERC starting grant

Duration: September 2017 - August 2022

PI: María Naya Plasencia

As years go by, the existence of quantum computers becomes more tangible and the scientific community is already anticipating the enormous consequences of the induced breakthrough in computational power. Cryptology is one of the affected disciplines. Indeed, the current state-of-the-art asymmetric cryptography would become insecure, and we are actively searching for alternatives. Symmetric cryptography, essential for enabling secure communications, seems much less affected at first sight: its biggest known threat is Grover's algorithm, which allows exhaustive key searches in the square root of the normal complexity. Thus, so far, it is believed that doubling key lengths suffices to maintain an equivalent security in the post- quantum world. The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which neither exists nor has ever been studied. This is the big gap I have identified and that I plan to fill with this project. Next, doubling the key length is not a trivial task and needs to be carefully studied. My ultimate aim is to propose efficient solutions secure in the post-quantum world with the help of our previously obtained quantum symmetric cryptanalysis toolbox. This will help prevent the chaos that big quantum computers would generate: being ready in advance will definitely save a great amount of time and money, while protecting our current and future communications. The main challenge of QUASYModo is to redesign symmetric cryptography for the post-quantum world.

9.2.2. Collaborations in European Programs, Except FP7 & H2020

9.2.2.1. COST Action IC1306

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) and a winter school dedicated to Symmetric Cryptography and Blockchain (Torremolinos, Spain, February 19-23, 2018). She also serves on the program committee of the CryptoAction Symposium organized every year.

9.2.2.2. QCDA

Program: QuantERA ERA-NET Cofund in Quantum Technologies

Project acronym: QCDA

Project title: Quantum Code Design and Architecture

Duration: February 2018 - January 2021

Coordinator: Earl Campbell, University of Sheffield, UK

Other partners: University of Sheffield (UK), TU Delft (Netherlands), TU Munich (Germany), University College London (UK)

Abstract: General purpose quantum computers must follow a fault-tolerant design to prevent ubiquitous decoherence processes from corrupting computations. All approaches to fault-tolerance demand extra physical hardware to perform a quantum computation. Kitaev's surface, or toric, code is a popular idea that has captured the hearts and minds of many hardware developers, and has given many people hope that fault-tolerant quantum computation is a realistic prospect. Major industrial hardware developers include Google, IBM, and Intel. They are all currently working toward a fault-tolerant architecture based on the surface code. Unfortunately, however, detailed resource analysis points towards substantial hardware requirements using this approach, possibly millions of qubits for commercial applications. Therefore, improvements to fault-tolerant designs are a pressing near-future issue. This is particularly crucial since sufficient time is required for hardware developers to react and adjust course accordingly.

This consortium will initiate a European co-ordinated approach to designing a new generation of codes and protocols for fault-tolerant quantum computation. The ultimate goal is the development of high-performance architectures for quantum computers that offer significant reductions in hardware requirements; hence accelerating the transition of quantum computing from academia to industry. Key directions developed to achieve these improvements include: the economies of scale offered by large blocks of logical qubits in high-rate codes; and the exploitation of continuous-variable degrees of freedom.

The project further aims to build a European community addressing these architectural issues, so that a productive feedback cycle between theory and experiment can continue beyond the lifetime of the project itself. Practical protocols and recipes resulting from this project are anticipated to become part of the standard arsenal for building scalable quantum information processors.

9.3. International Initiatives

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

9.3.1.1. CHOCOLAT

Title: Chosen-prefix Collision Attack on SHA-1 with ASICs Cluster

International Partner (Institution - Laboratory - Researcher):

NTU (Singapore) - SYLLAB - Peyrin Thomas

Start year: 2017

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

The hash function SHA-1 is one of the most widely used hash functions in the industry, but it has been shown to not be collision-resistant by a team of Chinese researchers led by Prof. Wang in 2005. However, a real pair of colliding messages was only published recently by a team from CWI and Google, because the estimated attack complexity is around 2^{63} SHA-1 computations (this represents about 70000 years of computation on a normal PC).

While this SHA-1 collision clearly demonstrates the weakness of the algorithm, a much more powerful attack would be to find a collision such that the prefix of the colliding messages is chosen by some challenger beforehand. In particular, this would allow creating a rogue certificate authority certificate that would be accepted by browsers. Such an attack has already been deployed for certificates using the MD5 hash function, but MD5 is much weaker than SHA-1 and it has already been removed from most security applications. SHA-1 is still widely used and performing such an attack for certificates using SHA-1 would have a very big impact.

The objective of the project is to design a chosen-prefix collision attack against the SHA-1 hash function, and to implement the attack in practice. We estimate this will require 2^{70} computations.

9.3.2. Inria International Partners

9.3.2.1. 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.

9.3.2.2. Informal International Partners

- Nanyang Technological University (Singapore): cryptanalysis of symmetric primitives.
- Ruhr-Universität Bochum (Germany): design and cryptanalysis of symmetric primitives.

9.3.3. Participation in Other International Programs

Anirudh Krishna, PhD student at Sherbroke University (Canada) spends six months in our team within the MITACS program.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Giannicola Scarpa, Universidad Complutense de Madrid, Spain, April 2017.
- Thomas Peyrin, NTU Singapore, May 2017, July 2017 and January 2018.
- Kaisa Nyberg, University of Helsinki, Finlande, May 2017.
- Adi Shamir, The Weizmann Institute of Science, Rehovot, Israel, May 2017.
- Christof Beierle, Bochum University, Germany, visiting PhD student, April-June 2017.
- Özgül Küçük, Bilgi University, Turkey, July-August 2017 (Bourse SSHN du Gouvernement Français).

9.4.1.1. Internships

- Sristy Agrawal, Kolkata, India, June-Aug. 2017
- Tim Beyne, Univ. Leuven, Belgium, Aug.-Sept. 2017
- Mathilde De La Morinerie, École Polytechnique, April-July 2017
- Matthieu Lequesne, MPRI, March-Aug. 2017
- André Schrottenloher, MPRI and Telecom ParisTech, March-Aug. 2017
- Ferdinand Sibleyras, MPRI, March-Aug. 2017
- Valentin Vasseur, Univ. Grenoble, March-Aug. 2017
- Matthieu Vieira, ENS Lyon, May-July 2017

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

- NTU, Singapore, October 16 - November 3, joint work within the CHOCOLAT Associate Team (G. Leurent).

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. 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, ENS Lyon). Participants: Assia Mahboubi, Th. Sibut-Pinote. Website: http://fastrelax.gforge.inria.fr/.

7.2. International Research Visitors

7.2.1. Visits of International Scientists

- Marni Mishna (Simon Fraser University) visited the team for one week in January.
- Emre Sertöz (Max Planck Institute Leipzig) visited the team for one week in November. He worked with Pierre Lairez on applications to algebraic geometry of two tools developped at Specfun: the computations of periods (Lairez's PhD) and numerical analytic continuation (Mezzarobba's PhD, 2011).
- Karen Yeats (Simon Fraser University) visited the team for a few days in June. She continued a work on bijective combinatorics of words with Frédéric Chyzak. A text is now under writing.

7.2.1.1. Internships

- Pascal Fong did a Master internship from March to August. Under the supervision of Pierre Lairez and Mohab Safey El Din (UPMC), he studied the numerical computation of the length of plane algebraic curves.
- Rémy Garnier did a Master internship from March to July. Under the supervision of Alin Bostan and Frédéric Chyzak, he studied existing algorithms to solve linear differential systems for their rational-function solutions.
- Meissa M'baye did a Master internship from February to June. Under the remote supervision of Assia Mahboubi, he studied the principles of proof assistants and surveyed formalization methodologies for elementary number theory.

7.2.2. Visits to International Teams

- Frédéric Chyzak and Alin Bostan have been invited by the Erwin Schrödinger Institute (Vienna, Austria) for two weeks, to participate to the thematic program "Algorithmic and Enumerative Combinatorics" http://www.mat.univie.ac.at/~kratt/esi4/.
- Pierre Lairez visited Felipe Cucker (City University of Hong Kong) for two weeks. The outcome is a strengthened collaboration on the study of the complexity of numerical algorithms. A publication is in preparation: the second part of [10].
- Georges Gonthier was invited at the Newton Institue, for six weeks, as co-organiser and participant to the Big Proof thematic program.
- Assia Mahboubi visited Sander Dahmen (VU Amsterdam, The Netherlands) for three days. She has started a collaboration with his team, to obtain formal guarantees of computations for number theory.
- Assia Mahboubi has been invited by the Newton Institute (Cambridge, UK) for one month. She participated to the Big Proof thematic program.

CAIRN Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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.

8.1.2. Labex CominLabs - RELIASIC (2014-2018)

Participants: Emmanuel Casseau, Imran Wali.

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, Nantes). 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. We also propose a lightweight design and assessment framework for arithmetic operators with reduced-precision redundancy.

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

Participants: Arnaud Tisserand, 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/.

8.1.4. Labex CominLabs - BBC (2016-2020)

Participants: Olivier Sentieys, Cédric Killian, Joel Ortiz Sosa.

The aim of the BBC (on-chip wireless Broadcast-Based parallel Computing) project is to evaluate the use of wireless links between cores inside chips and to define new paradigms. Using wireless communications enables broadcast capabilities for Wireless Networks on Chip (WiNoC) and new management techniques for memory hierarchy and parallelism. The key objectives concern improvement of power consumption, estimation of achievable data rates, flexibility and reconfigurability, size reduction and memory hierarchy management. For more details see http://www.bbc.cominlabs.ueb.eu In this project, CAIRN will address new low-power MAC (media access control) technique based on CDMA access as well as broadcast-based fast cooperation protocol designed for resource sharing (bandwidth, distributed memory, cache coherency) and parallel programming.

8.1.5. Labex CominLabs - SHERPAM (2014-2018)

Participant: Patrice Quinton.

Heart failure and peripheral artery disease patients require early detection of health problems in order to prevent major risk of morbidity and mortality. Evidence shows that people recover from illness or cope with a chronic condition better if they are in a familiar environment (i.e., at home) and if they are physically active (i.e., practice sports). The goal of the Sherpam project is to design, implement, and validate experimentally a monitoring system allowing biophysical data of mobile subjects to be gathered and exploited in a continuous flow. Transmission technologies available to mobile users have been improved a lot during the last two decades, and such technologies offer interesting prospects for monitoring the health of people anytime and anywhere. The originality of the Sherpam project is to rely simultaneously and in an agile way on several kinds of wireless networks in order to ensure the transmission of biometric data, while coping with network disruptions. Sherpam also develops new signal processing algorithms for activity quantification and recognition which represent now a major social and public health issue (monitoring of elderly patient, personalized quantification activity, etc.). Sherpam involves research teams from several scientific domains and from several laboratories of Brittany (IRISA/CASA, LTSI, M2S, CIC-IT 1414-CHU Rennes and LAUREPS). For more details see http://www.sherpam.cominlabs.ueb.eu

8.1.6. DGA RAPID - FLODAM (2017–2021)

Participants: Olivier Sentieys, Angeliki Kritikakou.

FLODAM is an industrial research project for methodologies and tools dedicated to the hardening of embedded multi-core processor architectures. The goal is to: 1) evaluate the impact of the natural or artificial environments on the resistance of the system components to faults based on models that reflect the reality of the system environment , 2) the exploration of architecture solutions to make the multi-core architectures fault tolerant to transient or permanent faults and 3) test and evaluate the proposed fault tolerant architecture solutions and compare the results under different scenarios provided by the fault models.

8.2. European Initiatives

8.2.1. 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.

8.2.2. 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.

8.3. International Initiatives

8.3.1. Inria Associate Teams

8.3.1.1. IoTA

Title: Ultra-Low Power Computing Platform for IoT leveraging Controlled Approximation

International Partner (Institution - Laboratory - Researcher):

Ecole Polytechnique Fédérale de Lausanne (Switzerland) - Christian Enz

Start year: 2017

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

Energy issues are central to the evolution of the Internet of Things (IoT), and more generally to the ICT industry. Current low-power design techniques cannot support the estimated growth in number of IoT objects and at the same time keep the energy consumption within sustainable bounds, both on the IoT node side and on cloud/edge-cloud side. This project aims to build on the preliminary results on inexact and exact sub/near-threshold circuit design to achieve major energy consumption reductions by enabling adaptive accuracy control of applications. Advanced ultra low-power hardware design methods utilize very low supply voltage, such as in near-threshold and sub-threshold designs. These emerging technologies are very promising avenues to decrease active and stand-by-power in electronic devices. To move another step forward, recently, approximate computing has become a major field of research in the past few years. IoTA proposes to address, in a consistent fashion, the entire design stack, from 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. The main scientific challenge is twofold: (1) to add adaptive accuracy to hardware blocks built in near/sub threshold technology and (2) to provide the tools and methods to program and make efficient use of these hardware blocks for applications in the IoT domain. This entails developing approximate computing units, on one side, and methods and tools, on the other side, to rigorously explore trade-offs between accuracy and energy consumption in IoT systems. The expertise of the members of the two teams is complementary and covers all required technical knowledge necessary to reach our objectives, i.e., ultra low power hardware design (EPFL), approximate operators and functions (Inria, EPFL), formal analysis of precision in algorithms (Inria), and static and dynamic energy management (Inria, EPFL). Finally, the proof of concept will consist of results on (1) an adaptive, inexact or exact, ultra-low power microprocessor in 28 nm process and (2) a real prototype implemented in an FPGA platform combining processors and hardware accelerators. Several software use-cases relevant for the IoT domain will be considered, e.g., embedded vision, IoT sensors data fusion, to practically demonstrate the benefits of our approach.

8.3.2. Inria International Partners

8.3.2.1. 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

8.3.2.2. HARAMCOP

Title: Hardware accelerators modeling using constraint-based programming

International Partner (Institution - Laboratory - Researcher):

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

8.3.2.3. 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.

8.3.2.4. DARE

Title: Design space exploration Approaches for Reliable Embedded systems

International Partner (Institution - Laboratory - Researcher):

IMEC (Belgium) - Francky Catthoor

Methodologies to design low cost and efficient techniques for safety-critical embedded systems, Design Space Exploration (DSE), run-time dynamic control mechanisms.

8.3.2.5. Informal International Partners

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.

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

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

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

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Mattia Cacciotti, Ecole Polytechnique Fédérale de Lausanne (Switzerland), from May 2017 until June 2017.

Emna Hammami, University of Tunis, from April 2017 until June 2017.

Prof. Stanislaw Piestrak, Univ de Lorraine, June 2017.

8.4.2. Visits to International Teams

P. Quinton was invited in Passau University (Passau, Germany) by Prof. Chris Lengauer during one week in June 2017, and gave an invited seminar on the synthesis of parallel architectures.

P. Quinton was invited by Prof. Daniel Massicotte of Université de Trois-Rivières (Québec) in October 2017 to cooperate on the design of FPGA hardware accelerators for electric simulation. His stay was supported by a grant of the RESMIQ (regroupement stratégique en microsystèmes du Québec). He gave an invited seminar on the synthesis of data-flow parallel systems.

8.4.3. 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 was 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

9.1.1. Inria Large Scale Initiative on Multicore

Philippe Clauss, Jens Gustedt, 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. The PhD defense was held December the 18th 2017.

Philippe Clauss, Jens Gustedt and Maxime Mogé are involved in the ADT Inria project ASNAP (*Accélération des Simulations Numériques pour l'Assistance Peropératoire*), in collaboration with the Inria team MIMESIS. The goal is to find opportunities in the SOFA simulation platform for applying automatic parallelization techniques developed by Camus. We are currently investigating two approaches. The first uses memory behavior memoization to generate a parallel code made of independent threads at runtime. The second uses ordered read-write locks (ORWL) to dynamically schedule a pipeline of parallel tasks.

9.1.2. 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, from October 2014, until November 2018. 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. Arthur Charguéraud focuses on the description of a formal semantics for JavaScript, and the development of tools for interactively executing programs step-by-step according to the formal semantics.

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

9.1.3. ANR Vocal

Participant: Arthur Charguéraud [contact].

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/

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

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), team DCS (Verimag), TrustInSoft, and OCamlPro.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

Project acronym: ERC Deepsea

Project title: Parallel dynamic computations

Duration: Jun. 2013 - May 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 Camus), who works part time on this project. Project website: http://deepsea.inria.fr/.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. 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
- Carnegie Mellon University, Pittsburgh, USA
- Indian Institute of Science (IIIS) Bangalore, India
- Barcelona Supercomputing Center, Barcelona, Spain

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 run-time 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. AGIR DEREVES

- Title: DEcentralised Run-Time Verification and Enforcement of distributed and cyber-physical Systems
- DEREVES leader: Yliès Falcone
- CORSE participants: Yliès Falcone, Antoine El-Hokayem, Raphaël Jakse
- DEREVES aims at advancing the theory of decentralized run-time verification and enforcement 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, distributed and cyber-physical systems. The project shall help transferring run-time 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. PIA ELCI

- Title: Software environment for computation-intensive applications
- Coordinator: Corinne Marchand (BULL SAS)
- CORSE participants: François Broquedis, Philippe Virouleau
- INRIA Partners: Avalon, Cardamon, Myriads; Realopt, Roma, Storm, Tadaam
- Other Partners: Algo'Tech, CEA, Cenaero, CERFACS, CORIA, Kitware, Onera, SAFRAN
- Duration: from Sept. 2014 to Sept. 2017
- Abstract: 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 run-time 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/run-time cooperation to improve the execution of scientific task-based programs on NUMA platforms. The PhD of Philippe Virouleau is funded by this project.

8.2.2. IPL ZEP

- Title: Zero-Power computing systems
- Coordinator: Kevin Marquet (INRIA Socrate)
- CORSE participants: Fabrice Rastello
- Other INRIA Partners: Cairn, Pacap
- Duration: from Apr. 2017 to Sept. 2019
- Abstract: The ZEP project addresses the issue of designing tiny computing objects with no battery by combining non-volatile memory (NVRAM), energy harvesting, micro-architecture innovations, compiler optimizations, and static analysis. The main application target is Internet of Things (IoT) where small communicating objects will be composed of this computing part associated to a low-power wake-up radio system. The ZEP project gathers four Inria teams that have a scientific background in architecture, compilation, operating system and low power together with the CEA Lialp and Lisan laboratories of CEA LETI & LIST. The major outcomes of the project will be a prototype harvesting board including NVRAM and the design of a new microprocessor associated with its optimizing compiler and operating system.

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 project 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

CORSE contact: Jean-François Méhaut

CORSE participants: Jean-François Méhaut, Frédéric Desprez and Francieli Zanon Boito

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 modeling. These four pillars will be anchored within a strong transverse 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 modeling 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.

Francieli Zanon Boito started in November 2017 as post-doc for the EoCoe project. She is working with Frédéric Desprez, Thierry Deutsch (CEA INAC) and Jean-François Méhaut. Francieli is investigating the data storage issues for the scientific workflows on the nano-scale characterization center (PFNC@Minatec http://inac.cea.fr/en/Phocea/Vie_des_labos/Ast/ast_technique.php?id_ast=217).

8.3.1.3. HPC4e

Title: HPC for Energy (HPC4E), Brazil and Europe

https://hpc4e.eu

H2020 European program

2 Years Duration (December 2015 - November 2017)

H2020 program: consortium

Coordinator: Barcelona Supercomputing Center

Partners:

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

Inria (France)

Queen Mary University of London (United Kingdom)

Iberdrola Renovables Energia (Spain)

Repsol (Spain)

Total S.A. (France)

COPPE Federal University of Rio de Janeiro (Brazil)

Laboratório Nacional Computação Cientifica (LNCC), Petropolis, (Brazil)

Instituto Technológico de Aeronautica (ITA), Brazil

Universidade Federal do Rio Grande do Sul (UFRGS), Brazil

Universidade Federal de Pernambuco (Brazil)

Petrobras (Brazil)

INRIA contact: Stephane Lanteri

CORSE particpants: Jean-François Méhaut, Frédéric Desprez, François Broquedis, 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 analyze 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, renewably and reduction of CO2 emissions, contribution to diversification of energy supply, rural development, and it does not compete with feed and food feed-stock. However, its use in practical systems is still limited since the complex fuel composition might lead to unpredictable combustion performance and instabilities in industrial fuels. 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 modeling 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.

Emmanuelle Saillard was one year post-doc for the HPC4e project. She used the BOAST framework on the Alya application (BSC) and the Hou10ni application (Inria Magique 3D). Emmanuelle Saillard got an Inria Research position (CR2) in the Storm team at Bordeaux.

Two papers [18], [16] were accepted this year with the Brazilian researchers at UFRGS and also with the Magique3D team.

Jean-François Méhaut got a *Chaire* position at Laboratório Nacional Computação Cientifica (LNCC) in Petrópolis (Brazil). The LNCC is also partner of the HPC4e project. Jean-François Méhaut is working on the optimization of the MHM (Multiscale Hybrid-Mixed Methods) simulator by using the binLPT loop scheduling strategies and also new memory allocators.

8.3.1.4. PRACE-5IP

Title: PRACE-5IP (PRACE Fifht Implementation Phase)

Program H2020

Duration: 01/01/2013 - 30/04/2019

Inria partners: Hiepacs team (Inria Bordeaux Sud-Ouest), Storm team (Inria Bordeaux Sud-Ouest), Nachos team (Inria Sophia Antipolis Méditerranée), CORSE team (Inria Grenoble Rhône Alpes) INRIA contact: Stéphane Lanteri (Nachos, Sophia Antipolis)

CORSE contact: Jean-François Méhaut

CORSE participants: François Broquedis, Jean-François Méhaut

The objectives of PRACE-5IP are to build on and seamlessly continue the successes of PRACE and start new innovative and collaborative activities proposed by the consortium. These include:

- assisting the transition to PRACE2 including analysis of TransNational Access;
- strengthening the internationally recognized PRACE brand;
- continuing and extend advanced training which so far provided more than 18800 person-training days;
- preparing strategies and best practices towards Exascale computing;
- coordinating and enhancing the operation of the multi-tier HPC systems and services;
- supporting users to exploit massively parallel systems and novel architectures.

The INRIA contribution is in the prolongation of involvement (jointly with CINES) in PRACE 4IP – WP7. The participation of Inria's researchers has been enlarged to include project-teams that were all involved in the C2S@Exa Inria Project Lab. The Inria teams will contribute to the WP7 and the following sub-tasks:

- Task 7.1: Applications Enabling Services for PRACE systems
- Task 7.4 Provision of Numerical Libraries for Heterogeneous/Hybrid Architectures

The activities are organized along two complementary lines

- Generic (or transverse) technologies for simulation software
- Specific (or vertical) technologies i.e. simulation software

The CORSE activities for PRACE-5IP will start with the hiring of one year postdoc in 2018. We will work on the DIOGENEs (DisOntinous GalErkin Nanoscale Solvers) software suite developed in the Nachos team. The post-doc will investigate the new vectorization features of processors.

8.3.2. Collaborations in European Programs, Except FP7 & H2020

Program: COST

Project acronym: ArVI

Project title: Run-Time Verification beyond Monitoring

Duration: December 2014 - Dec 2018

Coordinator: Martin Leucker, University of Lubeck

Abstract: Run-Time verification (RV) is a computing analysis paradigm based on observing a system at run-time 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 run-time 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 Associate Teams Not Involved in an Inria International Labs

8.4.1.1. IOComplexity

Title: Automatic characterization of data movement complexity

International Partner (Institution - Laboratory - Researcher):

Ohio State University (United States) - P. Sadayappan

Colorado State University (United States) - Louis-Noël Pouchet

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 stark contrast with all known previous work that are strictly 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.

8.4.1.2. 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 run-time 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. Participation in Other International Programs

- 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)
  - http://energysfe.ufsc.br/
  - 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 at the INRIA Minatec building in September 2016.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Julien Langou (UCDenver) is visiting professor from September 2016 till July 2017
- Henrique Cota de Freitas (PUC Minas) visited the team for a week in April 2017 (Pedro Penna's thesis)
- Philippe Navaux (UFRGS) visited the team for a week in February 2017. (HPC4e project)
- Paolo Rech (UFRGS) visited the team for a week in September 2017 (EnergySFE project).
- Mohamad Jaber (American University of Beirut, Lebanon) visited the team for a week in January 2017.
- Maurice Tchuente (Yaoundé 1) visited the team for a week in June 2017 (related to Thomas Messi Nguele's thesis).
- Márcio Castro (UFSC) visited the team for two weeks in February 2017 (EnergySFE project).
- Laercio Pilla (UFSC) visited the team for a week in December 2017 (EnergySFE project).

8.5.2. Visits to International Teams

- Jean-François Méhaut visited for one week (July 2017) the UFRGS (Porto Alegre) and the GPPD group for the HPC4e project.
- Jean-François Méhaut visited for one week (July 2017) the Federal University of Rio de Janeiro for the HPC4e project.
- Jean-François Méhaut visited for one day (July 2017) the LNCC to prepare the research work for the chaire position and also for the HPC4e project.
- Jean-François Méhaut visited for a week (August 2017) the LaPeSD and ECL laboratories at UFSC (Florianopolis). He was member of the master jurie of Pedro Penna. This visit was funded by the EnergySFE project.

- Jean-François Méhaut visited for one week (August 2017) the PUC Minas to prepare the cotutelle agreement of the Pedro Penna's PhD. This agreement is signed between PUC Minas, LIG, Ecole Doctorale MSTII, Post-Graduation program of PUC Minas and the COMUE Grenoble Alpes.
- Jean-François Méhaut visited for one day (December 2017) the French consulate in Rio de Janeiro and the CNRS Bureau. He presented the first results of the research work at LNCC.

8.5.2.1. Sabbatical programme

- Fabrice Rastello is on sabbatical at Colorado State University (USA) from July 2017 till July 2018

8.5.2.2. Research Stays Abroad

- Jean-François Méhaut holds a *Chaire* position at Laboratório Nacional Computação Cientifica (LNCC) in Petrópolis (Brazil). This *Chaire* position is funded by the LNCC and the French Consulate in Rio de Janeriro.

PACAP Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Britanny region fellowship

Participants: Niloofar Charmchi, André Seznec.

The Britanny Region is partially funding a Ph.D. fellowship for Niloofar Charmchi on the topic "Hardware prefetching and related issues".

8.2. National Initiatives

8.2.1. 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.

8.2.2. Zero Power Computing Systems (ZEP): Inria Project Lab, 2017–2020

Participant: Erven Rohou.

This proposal addresses the issue of designing tiny wireless, batteryless, computing objects, harvesting energy in the environment. The energy level harvested being very low, very frequent energy shortages are expected. In order for the new system to maintain a consistent state, it will be based on a new architecture embedding non-volatile RAM (NVRAM). In order to benefit from the hardware innovations related to energy harvesting and NVRAM, software mechanisms will be designed. On the one hand, a compilation pass will compute a worst-case energy consumption. On the other hand, dedicated runtime mechanisms will allow:

1. to manage efficiently and correctly the NVRAM-based hardware architecture;
2. to use energy intelligently, by using the worst-case energy consumption.

The ZEP project gathers four Inria teams that have a scientific background in architecture, compilation, operating systems together with the CEA Lialp and Lisan laboratories of CEA LETI & LIST. The main application target is Internet of Things (IoT).

8.2.3. 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.

8.2.4. ANR W-SEPT 2012-2017

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.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

8.3.1.1. ANTAREX

Participants: Erven Rohou, Imane Lasri.

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

Program: 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.

8.3.1.2. Eurolab-4-HPC

Participant: André Seznec.

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

Program: H2020

Duration: September 2015 - September 2017

Coordinator: Chalmers Tekniska Hoegskola AB

Partners:

Barcelona Supercomputing Center - Centro Nacional de Supercomputacion (Spain)

Chalmers Tekniska Hoegskola (Sweden)

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)

Universität 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.

8.3.1.3. ARGO

Participants: Isabelle Puaut, Damien Hardy, Imen Fassi.

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 für Technologie (KIT)

Université Rennes I contact: Steven Derrien

Partners:

Karlsruher Institut für Technologie (KIT)

SCILAB enterprises SAS

Recore Systems BV

Université de Rennes I

Technologiko Ekpaideftiko Idryma (TEI) Dytikis Elladas

Absint GmbH

Deutsches Zentrum für 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 and Angeliki Kritikakou from the CAIRN team.

8.3.1.4. 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.

8.4. International Initiatives

8.4.1. 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, Sabancı Üniversitesi (Turkey), and Université Catholique de Louvain (Belgium).

8.4.2. 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.

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

8.4.3.1. 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.

8.5. International Research Visitors

Prof. Ahmed ElMahdy, from the Egypt-Japan University of Science and Technology (E-JUST), Alexandria, Egypt, visited PACAP for two weeks in September, in the context of the project PHC IMHOTEP.

8.5.1. Visits of International Scientists

8.5.1.1. Internships

Stefano Cherubin, PhD student at Politecnico di Milano for one month in Mar 2017, within the context of the ANTAREX H2020 project.

Andrei Rimsa Alvares, PhD at UFMG and Assistant Professor at CEFET-MG, 1 month from January 6 to February 5, 2017, PROSPIEL Associate Team.

AOSTE2 Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. FUI

9.1.1.1. CEOS

Participants: Slim Ben-Amor, Liliana Cucu, Mehdi Mezouak, Yves Sorel, Walid Talaboulma.

This project was started on May 2017. Partners of the project are: ADCIS, ALERION, Aéroports de Lyon, EDF, ENEDIS, RTaW, EDF, Thales Communications and Security, ESIEE engineering school and Lorraine University. The CEOS project delivers a reliable and secure system of inspections of pieces of works using professional mini-drone for Operators of Vital Importance coupled with their Geographical Information System. These inspections are carried out automatically at a lower cost than current solutions employing helicopters or off-road vehicles. Several software applications proposed by the industrial partners, are developed and integrated in the drone, within an innovative mixed-criticality approach using multi-core platforms.

9.1.1.2. WARUNA

Participants: Antoine Bertout, Liliana Cucu, Adriana Gogonel, Tomasz Kloda, Yves Sorel, Walid Talaboulma.

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

9.1.2. PIA

9.1.2.1. CAPACITES

Participants: Liliana Cucu, Cristian Maxim, 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 was 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 PhD of Walid Talaboulma is funded on this contract.

9.1.2.2. DEPARTS

Participants: Liliana Cucu, Adriana Gogonel, Walid Talaboulma.

This project is funded by the BGLE Call (Briques Logicielles pour le Logiciel Embarqué) of the national support programme Investissements d'Avenir. Formally started on October 1st, 2012 with the kick-off meeting held on April, 2013 for administrative reasons. Research will target solutions for probabilistic component-based models, and a Ph.D. thesis should start at latest on September 2015. The goal is to unify in a common framework probabilistic scheduling techniques with compositional assume/guarantee contracts that have different levels of criticality.

9.2. European Initiatives

9.2.1. Collaborations in European Programs, Except FP7 & H2020

9.2.1.1. ASSUME

Participants: Keryan Didier, Fatma Jebali, Dumitru Potop-Butucaru.

Program: ITEA

Project acronym: ASSUME

Project title: Affordable Safe and Secure Mobility Evolution

Duration: September 2015 - August 2018

Coordinator: Daimler

Other partners: among 38 partners Absint, Ansys, Airbus, Kalray, Safran, Thales, ENS, KTH, FZI, etc.

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.

9.2.2. Collaborations with Major European Organizations

University of York: Real-Time System Group (UK)

Uncertainties in real-time systems: the utilization of extreme value theory has received increased efforts from our community and more rigorous principles are needed for its full understanding. Our two research teams have gathered these principles in a joint publication.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

Professor George Lima (University of Baha, Brazil) visited us between May and June. His stay was dedicated the study of the utilization of extreme value theory on the problem of probabilistic estimation of worst case execution time bounds for a program on a processor.

HYCOMES Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

- Ayman Aljarbouh's PhD (see Section 5.1.3) was 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 [28]. 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 [36], [35]. In 2017, Benoît Caillaud and Aurélien Lamercerie have released Demodocos, a software synthesizing surgical process models from instances of surgical procedures.

7.2. National Initiatives

7.2.1. Inria Project Lab (IPL): ModeliScale, Languages and Compilation for Cyber-Physical System Design

The project gathers researchers from three Inria teams, and from three other research labs in Grenoble and Paris area.

Name	*Team*	*Inria Center or Laboratory*
Vincent Acary	Bipop	Inria Grenoble Rhône Alpes
Albert Benveniste Benoît Caillaud Khalil Ghorbal	Hycomes	Inria Rennes Bretagne Atlantique
Marc Pouzet Tim Bourke	Parkas	ENS Inria Paris
Goran Frehse	Tempo	Verimag-univ. Grenoble Alpes
Antoine Girard		L2S-CNRS, Saclay
Eric Goubault Sylvie Putot	Cosynus	LIX, École Polytechnique, Saclay

The main objective of ModeliScale is to advance modeling technologies (languages, compile-time analyses, simulation techniques) for CPS combining physical interactions, communication layers and software components. We believe that mastering CPS comprising thousands to millions of components requires radical changes of paradigms. For instance, modeling techniques must be revised, especially when physics is involved. Modeling languages must be enhanced to cope with larger models. This can only be done by combining new compilation techniques (to master the structural complexity of models) with new mathematical tools (new numerical methods, in particular).

MiodeliScale gathers a broad scope of experts in programming language design and compilation (reactive synchronous programming), numerical solvers (nonsmooth dynamical systems) and hybrid systems modeling and analysis (guaranteed simulation, verification). The research program is carried out in close cooperation with the Modelica community as well as industrial partners, namely, Dassault Systèmes as a Modelica/FMI tool vendor, and EDF and Engie as end users.

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

KAIROS Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. UCA project Smart IoT for Mobility

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

We have started a collaboration with Renault Software Lab and Orange in Sophia Antipolis to apply our system engineering to the field of connected vehicles. The goal is to model formally and with digital models contracts between car manufacturers (like Renault) and service providers that should provide new services for connected vehicles. The contract also involves the communication infrastructure provider (here Orange) that operates the communications. A project funded by Academy RISE of UCA Jedi has started in December 2017 with a Master student starting at the beginning of January 2018. This project is done in collaboration with the LEAT laboratory and the GREDEG Laboratory which provides experts on legal issues for connected objects.

8.2. National Initiatives

8.2.1. FUI CLISTINE

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

This project was officially closed this year, but work had finished by the end of last year. The outcomes were somehow weakened by the fact that the original project leader failed to integrate the results of various partners into the promised innovative architecture of network-on-board.

8.2.2. Investissements d'Avenir: PIA Clarity

Participants: Julien Deantoni, Ales Mishchenko, Robert de Simone, Amine Oueslati, Frédéric Mallet, 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 will end in December 2017. 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. In this project we investigated extensions of Capella to enable simulation and analysis of mode automata in the context of model based system engineering.

8.2.3. PEPS CNRS INS^{3}PECT

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

The project is funded by CNRS-INS2I call PEPS 2017 Connected Objects Algorithms Algorithm, Application and Architecture. It ended in December 2017.
The focus is on System Level engineering for Secured Services for connected Objects. The idea is to have a high level modeling and verification of services that integrate hardware, communication and computing edges, and the software parts. Security is transversal in this value chain and is included as a viewpoint in the design. See https://www.i3s.unice.fr/ins3pect/ for more information.

Academic partners are I3S (Sophia), LIG(Grenoble), LabSTICC (Lorient), LEAT (Sophia). An internal meeting was held in late Spring, while a more open Workshop was held in Sophia in December.

8.3. International Initiatives

8.3.1. Inria International Labs

8.3.1.1. LIAMA project SACCADES

This project was supported by the associated-team FM4CPS 8.3.1.2 , with Vania Joloboff from EPI TEA in Inria Rennes as Prime Investigator. The chinese partner was ECNU Shanghai, whose status inside LIAMA was then to be established.

8.3.1.2. 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

A Memorandum of Understanding (MoU) was signed a couple of years ago between Inria and ECNU Shanghai. The same kind was agreement was also concluded between University Côte d’Azur (UCA) and ECNU, covering mostly our colaboration, both on research and on academic student exchange sides.

We have an ongoing contractual collaborative project on our joint activities on co-modeling, named FIDEL, with the Computer Science department from the University of Verona; it is funded on their side by a specific University programme. The collaboration should be strenghtened on our side with the arrival of Giovanni Liboni, formerly student there, as PhD student working with us on a CIFRE grant by SAFRAN on the same topic.

8.3.3. Participation in Other International Programs

We are active members of the International Joint Lab of Trustworthy Software (IJLTS), of which Eric Madelaine is Steering Committee Member. The lab is funded by the Chinese Ministry of Reseach, and headed by ECNU, Shanghai (together with CWI, ENS Rennes, ENS Lyon, as partners amongst others). This Joint Lab forms the counterpart of the FM4CPS associated team and SACCADES LIAMA project, and in particular funded the Chinese partners in joint actions and visits. All this is reported under the FM4CPS Associated-Team section 8.3.1.2 .

Marie-Agnes Peraldi Frati is involved in the DNITT (Danang International Institute of Technology) Institute in Vietnam which is co-managed by UCA and University of Danang. She visited the institute 10 days in May 2017 in the context of the IGLOO (Specific Domain Language For Experience Global Orchestration) research project. The research topic is on domain specific scenario language for Home care and eHealth.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Visiting Professors

Reinhard von Hanxleden

Date: July 2017 - Sept. 2017

Institution: University of Kiel (Germany)

Min ZHANG

Date: 2017 - 2017

East China Normal University (Shanghai, China)

Jing LIU

Date: December 2017 - January 2018

East China Normal University (Shanghai, China)

8.4.1.2. Visiting PhD students

Donddong AN

Date: Oct. 2016 - March 2018

ECNU Shanghai

Maroua El Hami

Date: Oct. 2017 - July 2018

ENISO, Sousse (Tunisia)

PARKAS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

ANR/CHIST-ERA DIVIDEND project, 2013-2018.

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).

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

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

Inria contact: Albert Cohen

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

8.2.1.3. EMC2

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

Programm: FP7

Duration: April 2014 - March 2017

Coordinator: Infineon Technologies

Inria contact: Albert Cohen

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

8.3. International Initiatives

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

8.3.1.1. POLYFLOW

Title: Polyhedral Compilation for Data-Flow Programming Languages

International Partner (Institution - Laboratory - Researcher):

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

Start year: 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. Participation in Other International Programs

- VerticA (Francesco Zappa Nardelli), 2017-2020, joint project with Northeastern University, USA, financed by the ONR (Office of Naval Research), 1.5M$ (subcontract for 150k$).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Alex Susu from Polytechnica di Bucarest spent a 3 months internship in the Fall.

8.4.2. Visits to International Teams

8.4.2.1. Sabbatical programme

Francesco Zappa Nardelli, from Feb. 1st, 2017 to July. 29th, 2017 has been on sabbatical leave at Northeastern University, Boston, USA, invited by Prof. Jan Vitek.

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 exists 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 and Maxime Lesourd'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. National Initiatives

8.2.1. ANR

An ANR-PRCI project called RT-PROOFS will start in 2018, which involves the SPADES project-team, MPI-SWS, TU Braunschweig, and Onera.

8.3. European Initiatives

8.3.1. 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 have a recent collaboration with the MPI-SWS in Kaiserslautern (Germany) on formal proofs for real-time systems. This collaboration will be concretized by an ANR-PRCI project called RT-PROOFS starting in 2018, which involves MPI-SWS, TU Braunschweig, INRIA, and Onera.

8.4. International Initiatives

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

8.4.1.1. 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.

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

Program: PAI/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. Inria International Labs

9.2.1.1. 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

9.2.2. Inria Associate Teams

9.2.2.1. Composite

Title: Compositional System Integration

International Partner (Institution - Laboratory - Researcher):

- University of California, San Diego (United States) - Microelectronic Embedded Systems Laboratory - Rajesh Gupta

Start year: 2017

See also: http://www.irisa.fr/prive/talpin/composite

Most applications that run somewhere on the internet are not optimized to do so. They execute on general purpose operating systems or on containers (virtual machines) that are built with the most conservative assumptions about their environment. While an application is specific, a large part of the system it runs on is unused, which is both a cost (to store and execute) and a security risk (many entry points).

A unikernel, on the contrary, is a system program object that only contains the necessary the operating system services it needs for execution. A unikernel is build from the composition of a program, developed using high-level programming language, with modules of a library operating system (libOS), to execute directly on an hypervisor. A unikernel can boot in milliseconds to serve a request and shut down, demanding minimal energy and resources, offering stealthiest exposure time and surface to attacks, making them the ideal platforms to deploy on sensor networks, networks of embedded devices, smart grids and clouds.

The goal of COMPOSITE is to develop the mathematical foundations for sound and efficient composition in system programming: analysis, verification and optimization technique for modular and compositional hardware-system-software integration of unikernels. We intend to further this development with the prospect of an end-to-end co-design methodology to synthesize lean and stealth networked embedded devices.

9.2.3. Inria International Partners

9.2.3.1. Convex

Title: Compositional Verification of Cyber-Physical Systems

International Partner:

- Chinese Academy of Science, Institute of Software
- Beihang University
- Nanhang University
- Nankai University

Duration: 2017 - now

Formal modeling and verification methods have successfully improved software safety and security in vast application domains in transportation, production and energy. However, formal methods are labor-intensive and require highly trained software developers. Challenges facing formal methods stem from rapid evolution of hardware platforms, the increasing amount and cost of software infrastructures, and from the interaction between software, hardware and physics in networked cyber-physical systems.

Automation and expressivity of formal verification tools must be improved not only to scale functional verification to very large software stacks, but also verify non-functional properties from models of hardware (time, energy) and physics (domain). Abstraction, compositionality and refinement are essential properties to provide the necessary scalability to tackle the complexity of system design with methods able to scale heterogeneous, concurrent, networked, timed, discrete and continuous models of cyber-physical systems.

Project Convex wants to define a CPS architecture design methodology that takes advantage of existing time and concurrency modeling standards (MARTE, AADL, Ptolemy, Matlab), yet focuses on interfacing heterogeneous and exogenous models using simple, mathematically-defined structures, to achieve the single goal of correctly integrating CPS components.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

Rajesh Gupta visited project-team TEA in August and gave two 68NQTR seminars on “Building Computing Machines That Sense, Adapt and Approximate” and on “Compositional Synthesis for High-level Design of System-Chips”.

Deian Stefan visited project-team TEA in September and gave a 68NQTR seminar on “Practical multi-core information flow control”

Shuvra Bhattacharyya visited project-team TEA in August and December and gave a 68NQTR seminar on “The DSPCAD Framework for Dataflow-based Design and Implementation of Signal Processing Systems“

9.3.2. Visits to International Teams

Jean-Pierre Talpin visited UC San Diego and UC Berkeley in the context of the associate-project Composite in June.

In the context of the IIP Convex, Jean-Pierre Talpin was invited at Beihang and Nanhang Universities in April, visited Beihang and Nankai Universities in July, and Beihang, Nankai and ECNU in November, to give seminars and a introductory course on model checking.

Jean-Pierre Talpin gave an invited talk on “Parametric model-checking the FTSP protocol ” at TU Wien June 30.

Simon Lunel visited CMU and UC San Diego in December to give seminars on “compositional proofs in differential dynamic logic”.

ANTIQUE Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. 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: Jerome 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.

9.1.2. 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.

9.1.3. 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.

9.1.4. TGFSYSBIO

Title: Microznvironment and cancer: regulation of TGF-β signaling

Type: ANR générique 2014

Defi: Société de l'information et de la communication

Instrument: Plan Cancer 2014-2019

Duration: December 2015 - November 2018

Coordinator: INSERM U1085-IRSET

Others partners: Inria Paris (France), Inria Rennes-Bretagne Atlantique (France),

Inria contact: Jerome Feret

Abstract: Most cases of hepatocellular carcinoma (HCC) develop in cirrhosis resulting from chronic liver diseases and the Transforming Growth Factor β (TGF-β) is widely regarded as both the major pro-fibrogenic agent and a critical inducer of tumor progression and invasion. Targeting the deleterious effects of TGF-β without affecting its physiological role is the common goal of therapeutic strategies. However, identification of specific targets remains challenging because of the pleiotropic effects of TGF-β linked to the complex nature of its extracellular activation and signaling networks.

Our project proposes a systemic approach aiming at to identifying the potential targets that regulate the shift from anti- to pro-oncogenic effects of TGF-β. To that purpose, we will combine a rule-based model (Kappa language) to describe extracellular TGF-beta activation and large-scale state-transition based (Cadbiom formalism) model for TGF-β-dependent intracellular signaling pathways. The multi-scale integrated model will be enriched with a large-scale analysis of liver tissues using shotgun proteomics to characterize protein networks from tumor microenvironment whose remodeling is responsible for extracellular activation of TGF-β. The trajectories and upstream regulators of the final model will be analyzed with symbolic model checking techniques and abstract interpretation combined with causality analysis. Candidates will be classified with semantic-based approaches and symbolic bi-clustering technics. All efforts must ultimately converge to experimental validations of hypotheses and we will use our hepatic cellular models (HCC cell lines and hepatic stellate cells) to screen inhibitors on the behaviors of TGF-β signal.

The expected results are the first model of extracellular and intracellular TGF-β system that might permit to analyze the behaviors of TGF-β activity during the course of liver tumor progression and to identify new biomarkers and potential therapeutic targets.

9.2. European Initiatives

9.2.1. 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.

9.2.2. MemCad

Type: IDEAS

Defi: Design Composite Memory Abstract Domains

Instrument: ERC Starting Grant

Objectif: Design Composite Memory Abstract Domains

Duration: October 2011 - September 2016

Coordinator: Inria (France)

Partner: None

Inria contact: Xavier Rival

Abstract: The MemCAD project aims at setting up a library of abstract domains in order to express and infer complex memory properties. It is based on the abstract interpretation frameworks, which allows to combine simple abstract domains into complex, composite abstract domains and static analyzers. While other families of abstract domains (such as numeric abstract domains) can be easily combined (making the design of very powerful static analyses for numeric intensive applications possible), current tools for the analysis of programs manipulating complex abstract domains usually rely on a monolithic design, which makes their design harder, and limits their efficiency. The purpose of the MemCAD project is to overcome this limitation.

Our proposal is based on the observation that the complex memory properties that need to be reasoned about should be decomposed in combinations of simpler properties. Therefore, in static analysis, a complex memory abstract domain could be designed by combining many simpler domains, specific to common memory usage patterns. The benefit of this approach is twofold: first it would make it possible to simplify drastically the design of complex abstract domains required to reason about complex softwares, hereby allowing certification of complex memory intensive softwares by automatic static analysis; second, it would enable to split down and better control the cost of the analyses, thus significantly helping scalability. As part of this project, we propose to build a static analysis framework for reasoning about memory properties, and put it to work on important classes of applications, including large softwares.

9.3. International Initiatives

9.3.1. Participation in Other International Programs

9.3.1.1. EXEcutable Knowledge

Title: EXEcutable Knowledge

Type: DARPA

Instrument: DARPA Program

Program: Big Mechanism

Duration: July 2014 - December 2017

Coordinator: Harvard Medical School (Boston, USA)

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

Inria contact: Jerome Feret

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

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

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

9.3.1.2. Active Context

Title: Active Context

Type: DARPA

Instrument: DARPA Program

Program: Communicating with Computers

Duration: July 2015 - December 2018

Coordinator: Harvard Medical School (Boston, USA)

Partner: University of California, (San Diego, USA), Inria Paris-Rocquencourt, École normale supérieure de Lyon Université Paris-Diderot,

Inria contact: Jerome Feret

Abstract: The traditional approach to the curation of biological information follows a philatelic paradigm, in which epistemic units based on raw or processed data are sorted, compared and catalogued in a slow and all too often insufficiently coordinated process aimed at capturing the meaning of each specimen in isolation. The swelling bounty of data generated by a systematic approach to biology founded on high-throughput technologies appears to have only intensified a sense of disconnected facts, despite their rendering as networks. This is all the more frustrating as the tide of static data (sequences, structures) is giving way to a tide of dynamic data about (protein-protein) interaction that want to be interconnected and understood (think annotated) in terms of process, i.e. a systemic approach.

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

9.4. International Research Visitors

9.4.1. Visits of International Scientists

9.4.1.1. Internships

Xavier Rival supervised the internship of Guillaume Cluzel (L3, École Normale Supérieure de Lyon), on the implementation of array abstract domains.

Xavier Rival supervised the internship of Sixiao Zhu (M1, École Polytechnique), on the integration of a three valued abstraction in MemCAD.

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

Xavier Rival visited KAIST (Korean Advanced Institute for Science and Technology) as an Invited Professor in November/December 2017.

CELTIQUE Project-Team

5. Partnerships and Cooperations

5.1. National Initiatives

5.1.1. 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.

5.1.2. 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.

5.1.3. 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.

5.1.4. 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 November 2018.

5.1.5. The ANR DISCOVER project

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

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 2019.

5.2. European Initiatives

5.2.1. 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: 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.

Sandrine Blazy is Substitute Member of the Managment Committee for France.

5.3. International Initiatives

5.3.1. Inria International Partners

5.3.1.1. Declared Inria International Partners

WEBCERT

Title: Verified Trustworthy web Applications

International Partner (Institution - Laboratory - Researcher):

Imperial College London - Department of Computing - Philippa Gardner

Duration: 2015 - 2019

Start year: 2015

See also: JSCert web page

The WebCert partnership focuses on applying formal methods to the JavaScript language: mechanized specification, development of an executable formal specification, design of a program logic, development of verification tools, and study of secure sub-languages.

CONVECS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. ARC6 Programme

Participants: Lina Marsso, Radu Mateescu [correspondent], 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. PIA (Programme d'Investissements d'Avenir)

8.2.1.1. CAPHCA

Participants: Frédéric Lang, Radu Mateescu [correspondent], Wendelin Serwe.

CAPHCA (*Critical Applications on Predictable High-Performance Computing Architectures*) is a project funded by the PIA. The project, led by IRT Saint-Exupéry (Toulouse), involves a dozen of industrial partners (among which Airbus, CS Systèmes d'Information, Synopsis, and Thalès Avionics), the University Paul Sabatier (Toulouse), and Inria Grenoble – Rhône-Alpes (CONVECS and SPADES project-teams). CAPHCA addresses the dual problem of achieving performance and determinism when using new, high performance, multicore System-on-Chip (SoC) platforms for the deployment of real-time, safety-critical applications. The methodology adopted by CAPHCA consists in building a pragmatic combination of methods, tools, design constraints and patterns deployable at a short-term horizon in the industrial domains targeted in the project.

CAPHCA started in December 2017 for four years. The main contributions of CONVECS to CAPHCA are the detection of concurrency errors in parallel applications by means of formal methods and verification techniques.

8.2.2. Competitivity Clusters

8.2.2.1. SECURIOT-2

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

SECURIOT-2 is a project funded by the FUI (*Fonds Unique Interministériel*) within the *Pôle de Compétitivité* Minalogic. The project, led by Tiempo Secure (Grenoble), involves the SMEs (*Small and Medium Enterprises*) Alpwise, Archos, Sensing Labs, and Trusted Objects, the Institut Fourier and the VERIMAG laboratories of Université Grenoble Alpes, and CONVECS. SECURIOT-2 aims at developing a secure micro-controller unit (SMCU) that will bring to the IoT a high level of security, based on the techniques used for smart cards or electronic passports. The SMCU will also include an original power management scheme adequate with the low power consumption constraints of the IoT.

SECURIOT-2 started in September 2017 for three years. The main contributions of CONVECS to SECURIOT-2 are the formal modeling and verification of the asynchronous hardware implementing the secure elements developed by the project partners.

8.2.3. Other National Collaborations

We had sustained scientific relations with the following researchers:

- Pierre Boullier (Inria, team ALPAGE),
- Anne-Lise Courbis (Ecole des Mines, Alès, France),
- Christophe Deleuze and Ioannis Parissis (LCIS, Valence),
- Xavier Etchevers (Orange Labs, Meylan),
- Laurent Georget (Centrale/Supelec, Rennes, France),
- Claude Girault (LIP6, Paris),
- Fabrice Kordon and Lom Messan Hillah (LIP6, Paris),
- Xavier Leroy (Inria, team GALLIUM),
- Pascal Poizat (LIP6, Paris).

8.3. European Initiatives

8.3.1. Collaborations in European Programs, Except FP7 & H2020

Program: PHC Amadeus

Project acronym: RIDINGS

Project title: Rigourous Development of GALS Systems

Duration: January 2017 – December 2018

Coordinator: Inria Grenoble – Rhône-Alpes / CONVECS

Other partners: TU Graz, Institute of Software Technology (Austria)

Abstract: GALS systems, composed of synchronous components (driven by local clocks) that communicate through a network, are increasingly spreading with the development of the IoT. GALS systems are intrinsically complex due to the interplay of synchronous and asynchronous aspects, which make their development and debugging difficult. Therefore, it is necessary to adopt rigorous design methodologies, based on formal methods assisted by efficient validation tools. The RIDINGS project aims at enhancing the design flow of a GALS system by integrating the automatic generation of conformance tests from the formal model and the temporal properties used for verifying the system. This yields a double benefit for the designer: (i) it makes possible to check that a physical implementation conforms to the verified model; (ii) the development cost of the model and properties is distributed on the verification and testing phases of the design process, therefore increasing the return on investment.

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://fmics.inria.fr

8.4.1. Inria International Partners

8.4.1.1. Informal International Partners

Saarland University (Germany): we collaborate on a regular basis with the DEPEND (*Dependable Systems and Software*) research group headed by Holger Hermanns, who received an ERC Advanced Grant ("POWVER") in 2016.

8.4.2. Other International Collaborations

In 2017, we had scientific relations with several universities and institutes abroad, including:

- University of Málaga, Spain (Francisco Duran),
- University of Boumerdes, Algeria (Sarah Chabane),
- Saarland University, Germany (Alexander Graf-Brill),
- ISTI/CNR, Pisa, Italy (Franco Mazzanti),
- FBK, Torino, Italy (Gianni Zampedri),
- RWTH Aachen, Germany (Christian Dehnert),
- University of Twente, The Netherlands (Enno Ruijters),
- University of York, UK (Jan Staunton),
- University Rio Grande do Norte, Brazil (Wellison Raul Mariz Santos),
- University of Cali, Colombia (Camilo Rocha),
- Utah State University, USA (Nazmus Sakib and Zhen Zhang).

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- Mahsa Shirmohammadi (University of Oxford, UK) visited us on February 23–24, 2017. She gave a talk on February 24, entitled "*Minimal Probabilistic Automata have to make Irrational Choices*".
- Josip Bozic, Birgit Hofer, Hermann Felbinger, and Franz Wotawa (TU Graz, Austria) visited us from May 15 to May 19, 2017, and attended the 1st RIDINGS Workshop held on May 17, 2017 at Inria Grenoble – Rhône-Alpes. J. Bozic gave a talk entitled "*Security Testing Based on Attack Patterns and Planning*". B. Hofer gave a talk entitled "*Fault Localization in Software and Spreadsheets*". H. Felbinger gave a talk entitled "*Test-Suite Reduction Does Not Necessarily Require Executing The Program Under Test*". F. Wotawa gave a talk entitled "*Research Activities at the Institute for Software Technology / TU Graz*".
- Soren Enevoldsen (Aalborg University, Denmark) visited us from September 27 to December 27, 2017. He gave a talk entitled "*Parallel Model Checking and Quantitative Models*" on October 24, 2017.

8.5.2. Visits to International Teams

- H. Garavel is an invited professor at Saarland University (Germany) as a holder of the Gay-Lussac Humboldt Prize.
- G. Salaün visited the University of Málaga (Spain) from May 31 to June 14, 2017.
- L. Marsso and W. Serwe visited TU Graz (Austria) from November 13 to November 17, 2017 in the framework of the PHC RIDINGS project.

DEDUCTEAM Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR PROGRAMme

This is an ANR for junior researcher Liesbeth Demol (CNRS, UMR 8163 STL, University Lille 3) to which G. Dowek participates. The subject is: "What is a program? Historical and Philosophical perspectives". This project aims at developing the first coherent analysis and pluralistic understanding of "program" and its implications to theory and practice.

7.2. International Initiatives

7.2.1. Participation in Other International Programs

7.2.1.1. International Initiatives

FoQCoSS

Title: Foundations of Quantum Computation: Syntax and Semantics

International Partners (Institution - Laboratory - Researcher):

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

CNRS (France) - Simon Perdrix

Universidade Federal de Santa Maria (Brazil) - Juliana Kaizer Vizzotto

Duration: 2016 - 2017

Start year: 2016

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.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

A. Díaz-Caro (Universidad Nacional de Quilmes, Argentina) visited Deducteam 3 weeks.

7.3.2. Visits to International Teams

7.3.2.1. Research Stays Abroad

F. Thiré has visited the Computation and Logic Group at McGill University for three months.

G. Dowek has visited the university of Quilmes in Buenos Aires for two weeks.

G. Dowek has visited the Pontifical University at Rio for three weeks.

GALLIUM Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR projects

9.1.1.1. Vocal

Participants: Armaël Guéneau, Xavier Leroy, François Pottier, Naomi Testard.

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. FUI Projects

9.1.2.1. 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, Adrien Guatto, Michael Rainey.

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. 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

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

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

- TECAP "Analyse de protocoles, Unir les outils existants", starting on October 1st, 20117, for 60 months, with a grant of 89 kEuros. Other partners are Inria teams PESTO (Inria Nancy grand-est), Ecole Polytechnique, ENS Cachan, IRISA Rennes, and CNRS. The corresponding researcher for this contract is Benjamin Grégoire.
- SafeTLS "La sécurisation de l'Internet du futur avec TLS 1.3" started on October 1st, 2016, for 60 months, with a grant of 147kEuros. Other partners are Université de Rennes 1, and secrétariat Général de la Défense et de la Sécurité Nationale. The corresponding researcher for this contract is Benjamin Grégoire.
- 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.

7.2. European Initiatives

7.2.1. Collaborations with Major European Organizations

We have sustained collaborations with the team of Thierry Coquand at Chalmers and the University of Göteborg in Sweden and with the team of Gilles Barthe at IMDEA in Spain.

7.3. International Initiatives

7.3.1. Informal International Partners

In September, we organized a meeting on formal proofs for cryptography, with the following attendants: Manuel Barbosa (Portugal), Gilles Barthe (Spain), Vincent Laporte (Spain), Jose Carlos Bacelar Almeida (Portugal), Pierre-Yves Strub (France), Ko Stoffelen (the Netherlands), Benoit Viguier (the Netherlands), Chitchanok Chuengsatiansup (France).

We have frequent visits by Gilles Barthe, François Dupressoir (IMDEA, Madrid) and visits of Benjamin Grégoire at IMDEA Madrid.

Benjamin Grégoire visited University of Minho in May to work on the Jasmin compiler with Manuel Barbosa.

In our activity to setup the Coq consortium, we have frequent interaction with A. Appel (U. Princeton), B. Pierce (U. Penn), Zhong Shao (Yale University), A. Chlipala (MIT), and G. Morrissett (Cornell University).

We received Reynald Affeldt from AIST for a 10-days visit in November.

MEXICO Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

- Thomas Chatain, Stefan Haar , Serge Haddad and Stefan Schwoon are participating in the ANR Project ALGORECELL.
- Matthias Függer participates in the ANR project FREDDA.

-

8.2. International Initiatives

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

8.2.1.1. 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. International Research Visitors

8.3.1. Visits of International Scientists

Joost-Pieter Katoen, Aachen, spent two weeks with MEXICO.

8.3.1.1. Internships

Aalok Thakkar, 2nd year student from CMI (India), did a two-month research internship on ’Semantics of Mutation Dynamics’ under the supervision of Stefan Haar, from May 2nd to July 21st, 2017.

8.3.2. Visits to International Teams

PARSIFAL Project-Team

7. Partnerships and Cooperations

7.1. European Initiatives

7.1.1. 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 – 31/10/2019

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 an ambitious, long-term 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.

7.1.2. 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.

7.2. International Initiatives

7.2.1. Participation in Other International Programs

7.2.1.1. 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.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

7.3.1.1. Internships

Riccardo Treglia was an intern funded by COCA HOLA during March, April, and May 2017. He was advised by Accattoli and worked on the complexity analysis of abstract machines for the λ-calculus.

7.3.2. Visits to International Teams

7.3.2.1. Research Stays Abroad

Stéphane Graham-Lengrand spent 8 months, from January 2017 to August 2017, at SRI International, Computer Science Lab. This visit developed a collaboration with N. Shankar, MP Bonacina, and D. Jovanovic, on new algorithms and new architectures for automated and interactive theorem proving, as well as on new programme verification techniques.

PI.R2 Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

Alexis Saurin (coordinator) and Yann Régis-Gianas are members of the four-year RAPIDO ANR project, 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 fixpoints 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 are members of the four-year Cathre ANR project (January 2014 to December 2017). This project investigates the general theory of higher-dimensional rewriting, the development of a general-purpose library for higher-dimensional rewriting, and applications in the fields of combinatorial 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). The project Cathre provided the funding for the PhD of Maxime Lucas.

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.

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 (Gallinette team, Inria Nantes & École des Mines de Nantes), funded by an ERC Starting Grant. The post-doctoral grant of Eric Finster is funded by the CoqHoTT ERC and Amin Timany's 2-month visit was funded on the ERC as well.

7.2. European Initiatives

7.2.1. Collaborations in European Programs, Except FP7 & H2020

Hugo Herbelin is a deputy representative of France in the COST action EUTYPES. The full name of the project (whose scientific leader is Herman Geuvers, from the University of Nijmegen) is “European research network on types for programming and verification”.

Presentation of EUTYPES: 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.

7.3. International Initiatives

7.3.1. Inria International Labs

7.3.1.1. Other IIL projects

Matthieu Sozeau is part of an international collaboration network CSEC “Certified Software Engineering in Coq” funded by Inria Chile, Conicyt and the CoqHoTT ERC, which will officially start in early 2018. The participants include Eric Tanter (primary investigator) and Nicolas Tabareau.

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

7.3.2.1. Associate team

Pierre-Louis Curien and Claudia Faggian are members of the CRECOGI associate team, coordinated on one side by Ugo dal Lago (research-team FoCUS , Inria Sophia and Bologna), and on the other side by Ichiro Hasuoi (NII, Tokyo). The full name of the project is Concurrent, Resourceful and Effectful Computation, by Geometry of Interaction.

Presentation of CRECOGI: Game semantics and geometry of interaction (GoI) are two closely related frameworks whose strengh is to have the characters of both a denotational and an operational semantics. They offer a high-level, mathematical (denotational) interpretation, but are interactive in nature. The formalisation in terms of movements of tokens through which programs communicate with each other can actually be seen as a low-level program. The current limit of GoI is that the vast majority of the literature and of the software tools designed around it have a pure, sequential functional language as their source language. This project aims at investigating the application of GoI to concurrent, resourceful, and effectful computation, thus paving a way to the deployment of GoI-based correct-by-construction compilers in real-world software developments in fields like (massively parallel) high-performance computing, embedded and cyberphysical systems, and big data. The presence of both the Japanese GoI community (whose skills are centered around effects and coalgebras) and the French GoI community (more focused on linear logic and complexity analysis) bring essential, complementary, ingredients.

7.3.2.2. Joint Inria-CAS project

Pierre-Louis Curien is principal investigator on the French side for a joint Inria-CAS project (a new programme of Inria with the Chinese Academy of Sciences). The project’s title is “Verification, Interaction, and Proofs”. The principal investigator on the Chinese side is Ying Jiang, from the Institute of Software (ISCAS) in Beijing. The participants of the project on the French side are Pierre-Louis Curien and Jean-Jacques Lévy, as well as other members of IRIF (Thomas Ehrhard, Jean Krivine, Giovanni Bernardi, Ahmed Bouajjani, Mihaela Sighireanu, Constantin Enea, Gustavo Petri), and Gilles Dowek (Deducteam team of Inria Saclay). On the Chinese side, the participants are Ying Jiang, as well as other members of the ISCAS (Angsheng Li, Xinxin Liu, Yi Lü, Peng Wu, Yan Rongjie, Zhilin Wu, and Wenhui Zhang), and Yuxi Fu (from Shanghai Jiaotong University). The project funds the postdoc of Kailiang Ji at University Paris 7, starting in December 2017.

Presentation of VIP: The line between “verification” and “proofs” is comparable to the one separating satisfiability and provability: in a formal system, a formula can be trusted either if it is satisfied in the intended model (for all of its instances), or if it can be proved formally by using the axioms and inference rules of some logical system. These two directions of work are called model-checking and proof-checking, respectively. One of the aims of the present project is to bring specialists of the two domains together and to tackle problems where model-checking and proof-checking can be combined (the “V” and the “P” of the acronym). Applications in the realm of distributed computation, or concurrency theory (the “I” of the acronym) are particularly targeted.

7.3.3. Inria International Partners

7.3.3.1. Informal International Partners

The project-team has collaborations with University of Aarhus (Denmark), KU Leuven, 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.

7.3.4. 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). This project ended in July 2017.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

John Baez (University of California River Side) visited the team for a week in November 2017.

Marcelo Fiore (University of Cambridge) visited the team for two weeks in February 2017.

Jovana Obradović (now a postdoc at Charles University, Prague) visited the team from December 1 to December 10 2017.

Amin Timany (KU Leuven, Belgium) visited the team for two months in March-April 2017 and collaborated with Matthieu Sozeau on the design and implementation of cumulative inductive types in Coq.

7.4.2. Visits to International Teams

7.4.2.1. Research Stays Abroad

Pierre-Louis Curien visited East China Normal University for a month in June 2017 (collaborations with Yuxin Deng and Min Zhang). Pierre-Louis Curien and Jovana Obradović visited the Institute of Mathematics of the Serbian Academy of Sciences in Belgrade in July 2017 (collaboration with Zoran Petrić).

Jean-Jacques Lévy visited the Institute of Software of Chinese Academy of Sciences (ISCAS) in December 2017 (project VIP and on-going work with Ran Chen) during 2 weeks. He gave talks at ISCAS hosted by Ying Jiang, and during a third week at ECNU Shanghai hosted by Min Zhang, USTC Suzhou (University of Science and Technology of China) hosted by Xinyu Feng, Nankai University in Tianjin hosted by Chunfu Jia.

SUMO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR STOCH-MC: Model-Checking of Stochastic Systems using approximated algorithms (2014-2018)

- web site at http://perso.crans.org/~genest/stoch.html.
- Led by Blaise Genest (SUMO);
- Participants: Nathalie Bertrand, Blaise Genest, Éric Fabre, Matthieu Pichené;
- Partners: Inria Project Team CONTRAINTES (Rocquencourt), LaBRI (Bordeaux), and IRIF (Paris).

The aim of STOCH-MC is to perform model-checking of large stochastic systems, using controlled approximations. Two formalisms will be considered: Dynamic Bayesian Networks, which represent compactly large Markov Chains; and Markov Decision Processes, allowing non deterministic choices on top of probabilities.

9.1.2. ANR HeadWork: Human-Centric Data-oriented WORKflows (2016-2020)

- web site at http://headwork.gforge.inria.fr/
- Led by David Gross-Amblard (Université Rennes 1);
- Participants : Loïc Hélouët, Éric Badouel;
- Partners: Inria Project-Teams Valda (Paris), DRUID (Rennes) SUMO (Rennes), LINKs (Lille), MNHN, Foule Factory.

The objective of this project is to develop techniques to facilite development, deployment, and monitoring 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.

9.1.3. IPL HAC-SPECIS: High-performance Application and Computers, Studying PErformance and Correctness In Simulation (2016-2020)

- web site at http://hacspecis.gforge.inria.fr/
- Led by Arnaud Legrand (Inria Rhône-Alpes)
- Participants: Thierry Jéron, The Anh Pham.
- Partners: Inria project-teams Avalon (Lyon), POLARIS (Grenoble), HiePACS, STORM (Bordeaux), MExICo (Saclay), MYRIADS, SUMO (Rennes), VeriDis (Nancy).

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.

This year we have been mainly intrested in dynamic partial-order-reduction methods that allow to reduce the explored state space, and a first prototype implementation of an existing method that combines DPOR with true-concurrency models.

9.1.4. CNRS INS2I JCJC SensAs (2017)

- Led by Ocan Sankur (SUMO).
- Participants: Ocan Sankur
- Partners: Benjamin Monmege, Pierre-Alain Reynier (Université Aix-Marseille).

Model-checking allows one to analyse the reliability of critical systems. There is currently an ongoing effort to extend formal verification and synthesis techniques to check non-functional properties such as performance, energy consumption or robustness, that are particularly important for real-time systems. SensAS is a project whose objective is to develop techniques to analyse the sensitivity of such systems with formal tools. In this context, a nominal behaviour, described with a deterministic timed automaton, is submitted to nondeterministic or stochastic perturbations. We seek then to quantify the variability of perturbed behaviours, giving formal guarantees on the computed result.

9.1.5. National informal collaborations

The team collaborates with the following researchers:

- Arnaud Sangnier (IRIF, UP7-Diderot) on the parameterized verification of probabilistic systems;
- François Laroussinie (IRIF, UP7-Diderot) on logics for multi-agent systems;
- Béatrice Bérard (LIP6) on problems of opacity and diagnosis, and on problems related to logics and partial orders for security;
- Serge Haddad (Inria team MExICo, LSV, ENS Paris-Saclay) on opacity and diagnosis;
- Patricia Bouyer (LSV, ENS Paris-Saclay) on the analysis of probabilistic timed systems and quantitative aspects of verification;
- Stefan Haar and Thomas Chatain (Inria team MExICo, LSV, ENS Paris-Saclay) on topics related to concurrency and time, and to modeling and verification of metro networks, multimodal systems and passenger flows;
- Éric Rutten and Gwenaël Delaval (Inria team Ctrl-A, LIG, Université Grenoble-Alpes) on the control of reconfigurable systems as well as making the link between Reax and Heptagon/BZR (http://bzr.inria.fr/);
- Didier Lime, Olivier H. Roux (LS2N Nantes) on topics related to stochastic and timed nets;
- Loïg Jezequel (LS2N Nantes) on topics related to stochastic and timed nets, and on distributed optimal planning;
- Ylìès Falcone (CORSE LIG/Inria Grenoble) and Antoine Rollet (LaBRI Bordeaux) on the enforcement of timed properties;

9.2. International Initiatives

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

9.2.1.1. QuantProb

- Title: Quantitative analysis of non-standard properties in probabilistic models
- International Partner (Institution - Laboratory - Researcher):

  Technical University of Dresde (Germany) - Faculty of Computer Science - 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.

9.2.2. Inria International Partners

9.2.2.1. Informal International Partners

The team collaborates with the following researchers:

- Jean-François Raskin, Gilles Geeraerts (Université Libre de Bruxelles, Belgium) on multiplayer game theory and synthesis;
- Thomas Brihaye (UMons, Belgium) on the verification of stochastic timed systems;
- Mickael Randour (UMons, Belgium) on quantitative games for synthesis;
- Kim G. Larsen (Aalborg University, Denmark) on quantitative timed games, and on topics related to urban train systems modeling;
- Josef Widder, Igor Konnov and Marijana Laźic (TU Wien, Austria) on the automated verification of randomized distributed algorithms.
- John Mullin (Polytechnique Montréal, Canada), on topics related to security and opacity;
- S. Akshay (IIT Bombay, India) on topics related to timed concurrent models;
- Andrea D'ariano (University Roma Tre, Italy), on topics related to train regulation;
- Stavros Tripakis, Srinivas Pinisetty (Aalto University, Finland) on runtime verification and enforcement.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

- Laurie Ricker visited the SUMO team for 2 months in May-June 2017.

9.3.1.1. Internships

- M2 Internship of Aina Toky Rasoamanana, Feb-July 2017, Nathalie Bertrand and Nicolas Markey
- L3 Internship of Balasubramanian A.R., May-July 2017, Nathalie Bertrand and Nicolas Markey

9.3.2. Visits to International Teams

9.3.2.1. Research Stays Abroad

- Éric Badouel made in September 2017 a one-month visit to Luca Bernardinello and Lucia Pomello from Milan University, and Carlo Ferigato from EJCR at Ispra. A work has been initiated on computer tools for the coordination of debates (from open citizen debates to parliamentary debates) and for managing the related documents (minutes, syntheses, ...) in an open data perspective.
- Engel Lefaucheux spent 6 weeks (May-June 2017) in Cagliari, working with Alessandro Giua and Carla Seatzu on the diagnosis of stochastic Petri nets.

TOCCATA Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. 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 60 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 60 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 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).

9.2.4. 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.

9.2.5. 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.

9.2.6. ANR PARDI

Participant: Sylvain Conchon [contact].

Verification of PARameterized DIstributed systems. A parameterized system specification is a specification for a whole class of systems, parameterized by the number of entities and the properties of the interaction, such as the communication model (synchronous/asynchronous, order of delivery of message, application ordering) or the fault model (crash failure, message loss). To assist and automate verification without parameter instantiation, PARDI uses two complementary approaches. First, a fully automatic model checker modulo theories is considered. Then, to go beyond the intrinsic limits of parameterized model checking, the project advocates a collaborative approach between proof assistant and model checker. http://pardi.enseeiht.fr/

The proof lead by Toulouse INP/IRIT started in 2016 and lasts for 4 years. Partners: Université Pierre et Marie Curie (LIP6), Université Paris-Sud (LRI), Inria Nancy (team VERIDIS)

9.3. European Initiatives

9.3.1. 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.

9.4. 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 worked on the formal verification of graphs algorithms [25], [17], and also in the context of the CoLiS project on verification of some aspects of the Unix file system and shell scripts [74] [11]

VERIDIS Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR-DFG Project SMArT

Participants: Haniel Barbosa, Pascal Fontaine, Stephan Merz, Thomas Sturm.

The SMArT (Satisfiability Modulo Arithmetic Theories) project was funded by ANR-DFG Programmes blancs 2013, a bilateral (French-German) program of Agence Nationale de la Recherche and Deutsche Forschungsgemeinschaft DFG. It started in April 2014 and finished in September 2017. The project gathered members of VeriDis in Nancy and Saarbrücken, and the Systerel company.

The objective of the SMArT project was 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 and veriT, 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 was 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 focus on the analysis of the designed system, exploiting the semantic power of the underlying modeling language. The semantics of this modeling languages are well understood by its users (in particular the system designers), 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 [61], i.e. explicit semantics. At present, 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 [50] is to offer rigorous mechanisms for handling domain knowledge in design models.

9.1.3. ANR Project Formedicis

Participant: Dominique Méry.

The ANR Project Formedicis, within the INS program, started in January 2017 for 4 years. It is coordinated by Bruno d'Augsbourg, the partners are ONERA, IRIT/ENSEIHT, ENAC, and LORIA.

During the last 30 years, the aerospace domain has successfully devised rigorous methods and tools for the development of safe functionally-correct software. During this process, interactive software has received a relatively lower amount of attention. However, Human-System Interactions (HSI) are important for critical systems and especially in aeronautics: new generations of aircraft cockpits make use of sophisticated electronic devices that may be driven by more and more complex software applications. The criticality of these applications require a high degree of assurance for their intended behavior. The report by the French *Bureau d'Enquêtes et d'Analyses* about the crash of the Rio-Paris flight AF 447 in 2009 pointed out a design issue in the behavior of the Flight Director interface as one of the original causes of the crash.

We believe that part of these issues are due to the lack of a well-defined domain specific “hub” language to represent interactive software design in a way that allows system designers to iterate on their designs before injecting them in a development process, and system developers to verify their software against the chosen design. Formedicis aims at designing such a formal hub language L, in which designers can express their requirements concerning the interactive behavior that must be embedded inside the interactive applications. The project will also develop a framework for validating, verifying, and implementing critical interactive applications designed and denoted in L.

More information on the project is available at http://www.agence-nationale-recherche.fr/Project-ANR-16-CE25-0007.

9.1.4. ANR Project PARDI

Participants: Marie Duflot-Kremer, Stephan Merz.

PARDI (Verification of parameterized distributed systems) is funded by ANR. The project started in January 2017 for a duration of 48 months. The project partners other than VeriDis are Toulouse INP (coordinator), Université Paris Sud, and Université Paris Marie Curie.

Distributed systems and algorithms are parameterized by the number of participating processes, the communication model, the fault model, and more generally the properties of interaction among the processes. The project aims at providing methodological and tool support for verifying parameterized systems, using combinations of model checking and theorem proving. VeriDis contributes its expertise on TLA$^+$ and its verification tools, and the integration with the Cubicle model checker is a specific goal of the project.

More information on the project is available at http://pardi.enseeiht.fr/.

9.1.5. 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.

9.1.6. 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, supported the development of a counterexample generator for higher-order logic. This new tool, called Nunchaku, is intended for integration with various proof assistants. The project was coordinated by Jasmin Blanchette and also involved Inria Saclay – Île de France (Toccata group) and Inria Rennes – Bretagne

Atlantique (Celtique group), among others. Simon Cruanes worked on Nunchaku from October 2015 to September 2017, whereas Blanchette has developed an Isabelle frontend. Four releases have taken place so far, and the tool is an integral part of the Isabelle2017 official release. Work has started on Coq and TLAPS frontends, and we will soon work on a Lean frontend as well. The tool is described in [62] and was presented at a workshop last year [57]. A noteworthy development this year is the creation of a backend called SMBC, based on new ideas by Cruanes about how to combine SAT solving and narrowing [29].

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. ERC Matryoshka

Program: European Union's Horizon 2020 research and innovation program

Project acronym: Matryoshka

Duration: April 2017 – March 2022

Coordinator: Jasmin Blanchette (VU Amsterdam)

Proof assistants are increasingly used to verify hardware and software and to formalize mathematics. However, despite the success stories, they remain very laborious to use. The situation has improved with the integration of first-order automatic theorem provers—superposition provers and SMT (satisfiability modulo theories) solvers—through middleware such as Sledgehammer for Isabelle/HOL and HOLyHammer for HOL Light and HOL4; but this research has now reached the point of diminishing returns. Only so much can be done when viewing automatic provers as black boxes.

To make interactive verification more cost-effective, we propose to deliver very high levels of automation to users of proof assistants by fusing and extending two lines of research: automatic and interactive theorem proving. This is our grand challenge. Our starting point is that first-order (FO) automatic provers are the best tools available for performing most of the logical work. Our approach will be to enrich superposition and SMT with higher-order (HO) reasoning in a careful manner, in order to preserve their desirable properties. We will design proof rules and strategies, guided by representative benchmarks from interactive verification.

With higher-order superposition and higher-order SMT in place, we will develop highly automatic provers building on modern superposition provers and SMT solvers, following a novel stratified architecture. To reach end users, these new provers will be integrated in proof assistants and will be available as backends to more specialized verification tools. The users of proof assistants and similar tools stand to experience substantial productivity gains: From 2010 to 2016, the success rate of automatic provers on interactive proof obligations from a representative benchmark suite called Judgment Day has risen from 47% to 77%; with this project, we aim at 90%–95% proof automation.

The Matryoshka ERC grant of Jasmin Blanchette includes Pascal Fontaine and Uwe Waldmann as senior researchers.

9.2.1.2. FET-Open CSA SC^2

Program: European Union's Horizon 2020 research and innovation program

Project acronym: SC^2

Project title: Symbolic Computation and Satisfiability Checking

Duration: July 2016 – August 2018

Coordinator: James Davenport (U. of Bath, UK)

Other partners: see http://www.sc-square.org/CSA/welcome.html

The use of advanced methods for solving practical and industrially relevant problems by computers has a long history. Whereas Symbolic Computation is concerned with the algorithmic determination of exact solutions to complex mathematical problems, more recent developments in the area of Satisfiability Checking tackle similar problems but with different algorithmic and technological solutions.

Though both communities have made remarkable progress in the last decades, they still need to be strengthened to tackle practical problems of rapidly increasing size and complexity. Their separate tools (computer algebra systems and SMT solvers) are urgently needed to examine prevailing problems with a direct effect to our society. For example, Satisfiability Checking is an essential backend for assuring the security and the safety of computer systems. In various scientific areas, Symbolic Computation enables dealing with large mathematical problems 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. However, researchers from these two communities rarely interact, and also their tools lack common, mutual interfaces for unifiying their strengths. 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. These are the main objectives of this CSA. We 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.

We believe that these activities will foster cross-fertilisation of both fields and bring mutual improvements. Combining the knowledge, experience and the technologies in these communities will enable the development of radically improved software tools.

This project is locally coordinated by Pascal Fontaine.

9.3. International Initiatives

9.3.1. Inria International Partners

Title: Kanazawa-Nancy for Satistifiability and Arithmetics (KANASA)

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.

One PhD student from JAIST spent one year in the VeriDiS team, until May 2017. The partnership evolves towards applying SMT to find malware in obfuscated code.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

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 was 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 investigated techniques to combine ICP with decision procedures for NLA within an SMT context, and adapted the subtropical method from computer algebra to the context of SMT. This work is relevant for the SMArT and SC^2 projects.

Andrew J. Reynolds

Date: 16 July 2017 – 17 September 2017

Institution: The University of Iowa

Host: Pascal Fontaine

Andrew J. Reynolds is a Research Scientist at the University of Iowa and one of main developers of the award-winning Satisfiability Modulo Theories (SMT) solver CVC4. His current research interests include implementing techniques in SMT solvers for unbounded strings and regular expressions, first-order quantified formulas and synthesis conjectures. He was an Inria invited researcher for two months in Nancy. We continued working on quantifier handling for SMT, along the lines of [20], and studied enumerative instantiation. This work contributes to the Matryoshka, SMArT and SC^2 projects.

9.4.2. Internships

Poonam Kumari

Date: 1 March – 31 July

Institution: Université de Lorraine (Erasmus Mundus DESEM)

Host: Stephan Merz

Poonam Kumari worked on a translation from a restricted subset of TLA$^+$ specifications into the input language of the Cubicle model checker for array-based parameterized systems.

CARTE Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- Simon Perdrix is PI of the PRCE ANR SoftQPro "Solutions logicielles pour l'optimisation des programmes et ressources quantiques". (2017- 2021) [Atos-Bull, LORIA, CEA, LRI].
- The team is partner of the ANR VanQuTe "Validation des technologies quantiques émergentes" (PRCI with Singapore) [LIP6, LORIA, SUTD, NUS, NTU] (2018-2022)
- The team is a 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.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

Mathieu Hoyrup participates in the Marie-Curie RISE project Computing with Infinite Data coordinated by Dieter Spreen (Univ. Siegen) that has started in April 2017. We organized a workshop CCC'17 in Nancy in June 2017, that was also the first meeting of the project.

9.2.2. Collaborations in European Programs, Except FP7 & H2020

The team is partner of the ITEA3 Quantex project [LORIA, LRI, CEA/Leti, Atos-Bull, Siemens, TUDelft, KPN, EKUT] (2018-2020)

9.3. International Initiatives

Simon Perdrix is member of the STIC AmSud FoQCOSS with Argentina. He visited Quilmes University during 2 weeks in July 2017.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Ross Duncan (Assistant Prof. at Strathclyde U., Glasgow), spent one month (June 2017) in our team as an invited professor at Université de Lorraine.

9.4.2. Internships

Jordina Francès de Mas, Quentin Ladeveze were interns in our team ; they worked on cellular automata and produced two technical reports (see [34] and [38]).

CIDRE Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

- **Region Bretagne ARED Grant :** the PhD of Mourad Leslous on malicious codes in Android applications is supported by a grant from the Région Bretagne.
- **Labex COMINLABS contract (2014-2017): ”Kharon-Security“ - http://kharon.gforge.inria.fr**

  Google Play offers more than 800’000 applications (apps), and this number increases every day. Google play users have performed more than 25 billion app downloads. These applications vary from games to music, video, books, tools, etc. Unfortunately, each of these application is an attack vector on Android. The number of malicious applications (pieces of malware) discovered during the first six months of 2013 exceeds the number of pieces of malware discovered during the 2010 to 2012 period, more than 700 thousand malicious and risky applications were found in the wild. In this context, we propose the Kharon-Security project to stem the progression of Android pieces of malware. We propose to combine static and dynamic monitoring to compute a behavioral signature of Android malware. Behavioral signatures are helpful to understand how malware infect the devices and how they spread information in the Android operating system. Static analysis is essential to understand which particular event or callback triggers malware payload.

  In the project we have already developed GroddDroid a tool dedicated to automatic identification and execution of suspicious code. We have also built a dataset of Android malware. In this dataset, all malware are entirely manually reverse and documented. We have also developed an analysis platform. This platform is been deployed at the High Research Laboratory.
- **Labex COMINLABS contract (2015-2018): ”HardBlare-Security“ - http://www.hardblare.cominlabs.ueb.eu/**

  The general context of the HardBlare project is to address Dynamic Information Flow Tracking (DIFT) that generally consists in attaching marks to denote the type of information that is saved or generated within the system. These marks are then propagated when the system evolves and information flow control is performed in order to guarantee a safe execution and storage within the system. Existing solutions imply a large overhead induced by the monitoring process. Some attempts rely on a hardware-software approach where DIFT operations are delegated to a coprocessor. Nevertheless, such approaches are based on modified processors. Beyond the fact hardware-assisted DIFT is hardly adopted, existing works do not take care of coprocessor security and multicore/multiprocessor embedded systems.

  We plan to implement DIFT mechanisms on boards including a non-modified ARM processor and a FPGA such as those based on the Xilinx Zynq family. The HardBlare project is a multidisciplinary project between CentraleSupélec IETR SCEE research team, CentraleSupélec Inria CIDRE research team and UBS Lab-STICC laboratory. Mounir Nasr Allah is doing his PhD in the context of this project. The main objective of this PhD is to study how hybrid analysis could improve hardware assisted DIFT using static analysis performed at compile-time. Another objective is to manage labels for persistent memory (i.e., files) using a modified OS kernel.
- **Labex COMINLABS contract (2016-2019): “BigClin” - http://www.bigclin.cominlabs.ueb.eu/**

  Health Big Data (HBD) is more than just a very large amount of data or a large number of data sources. The data collected or produced during the clinical care process can be exploited at different levels and across different domains, especially concerning questions related to clinical and translational research. To leverage these big, heterogeneous, sensitive and multi-domain clinical data, new infrastructures are arising in most of the academic hospitals, which are intended to integrate, reuse and share data for research.

Yet, a well-known challenge for secondary use of HBD is that much of detailed patient information is embedded in narrative text, mostly stored as unstructured data. The lack of efficient Natural Language Processing (NLP) resources dedicated to clinical narratives, especially for French, leads to the development of ad-hoc NLP tools with limited targeted purposes. Moreover, the scalability and real-time issues are rarely taken into account for these possibly costly NLP tools, which make them inappropriate in real-world scenarios. Some other today's challenges when reusing Health data are still not resolved: data quality assessment for research purposes, scalability issues when integrating heterogeneous HBD or patient data privacy and data protection. These barriers are completely interwoven with unstructured data reuse and thus constitute an overall issue which must be addressed globally.

In this project, we plan to develop distributed methods to ensure both the scalability and the online processing of these NLP/IR and data mining techniques; In a second step, we will evaluate the added value of these methods in several real clinical data and on real use-cases, including epidemilology and pharmaco-vigilance, clinical practice assessment and health care quality research, clinical trials.

9.2. National Initiatives

9.2.1. ANR

- **ANR INFRA Project: SOCIOPLUG (2013-2017) - http://socioplug.univ-nantes.fr/index.php/SocioPlug_Project**

  SocioPlug is a collaborative ANR project involving Inria (ASAP and CIDRE teams), the Nantes University, and LIRIS (INSA Lyon and Université Claude Bernard Lyon). The project emerges from the observation that the features offered by the Web 2.0 or by social media do not come for free. Rather they bring the implicit cost of privacy. Users are more of less consciously selling personal data for services. SocioPlug aims to provide an alternative for this model by proposing a novel architecture for large-scale, user centric applications. Instead of concentrating information of cloud platforms owned by a few economic players, we envision services made possible by cheap low-end plug computers available in every home or workplace. This will make it possible to provide a high amount of transparency to users, who will be able to decide their own optimal balance between data sharing and privacy.

- **ANR Project: PAMELA (2016-2020) - https://project.inria.fr/pamela/**

  PAMELA is a collaborative ANR project involving Rennes 1 university (ASAP and CIDRE teams in Rennes), Inria Lille (MAGNET team), LIP6 (MLIA team) and two start-ups, Mediego and Snips. It aims at developing machine learning theories and algorithms in order to learn local and personalized models from data distributed over networked infrastructures. The project seeks to provide first answers to modern information systems built by interconnecting many personal devices holding private user data in the search of personalized suggestions and recommendations. More precisely, we will focus on learning in a collaborative way with the help of neighbors in a network. We aim to lay the first blocks of a scientific foundation for these new types of systems, in effect moving from graphs of data to graphs of data and learned models. CIDRE's contribution in this project involves the design of adversary models and privacy metrics suitable to the privacy-related issues of this distributed learning paradigm.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

Emmanuelle Anceaume is actively working with Leonardo Querzoni from the University La Sapienza, Italy, on data streams algorithms and engines. Their cooperation gave rise to one publication in Algotel 2017 [25].

Valérie Viet Triem Tong has shortly visited Prof Alexander Pretchner at TU Munchen in june 2017. She has participated to a workshop about Android Malware analysis.

9.4. International Research Visitors

9.4.1. Research Stays Abroad

In the context of the project with HP Inc Labs, Ronny Chevalier and Guillaume Hiet collaborate with the security team of HP Labs in Bristol. They are working more specifically with David Plaquin and Maugan Villatel, who are co-authors of the article published at ASCAC. Ronny Chevalier has spent 3 monts to HP Labs at Bristol.

Mounir Nasr Allah is currently visiting ARM R&D labs at Cambridge for 6 months in the context of the HardBlare project. This visit has been funded by the EIT Digital Doctoral School Program. He is working with Alastair Reid on the use of formal methods to prove that some hardware security mechanisms of ARM embedded processors effectively enforce information flow policies.

Mourad Leslous did an international mobility of three months at the Technical University of Munich, in the team of Professor Alexander Pretschner. This mobility was part of the program of EIT Digital Doctoral School, a European institute that promotes entrepreneurship and innovation among PhD students. During this mobility, he worked on control flow and data flow dependencies in order to detect the malicious code inside Android applications.

COMETE Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. OPTIMEC

Project title: Optimal Mechanisms for Privacy Protection

Funded by: DigiCosme

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.

7.2. National Initiatives

7.2.1. 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.

7.3. International Initiatives

7.3.1. Inria Associate Teams

7.3.1.1. 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.

7.3.2. Inria International Partners

7.3.2.1. Informal International Partners

Giovanni Cherubin, Royal Holloway, University of London, UK

Geoffrey Smith, Florida International University, USA

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 de Cali, Colombia

Carlos Olarte, Universidade Federal do Rio Grande do Norte, Brazil

Camilo Rocha, Associate Professor, Universidad Javeriana de Cali, Colombia

7.3.3. Participation in Other International Programs

7.3.3.1. CLASSIC

Program: Colciencias - Conv. 712.

Project acronym: CLASSIC.

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, Universidad Javeriana de 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.

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..

7.3.3.2. EPIC

Program: STIC-Amsud.

Project acronym: EPIC.

Project title: EPistemic Interactive Concurrency/

Duration: Oct 2016 - Oct 2019.

URL: https://sites.google.com/site/sticamsudepic/

Coordinator: Frank Valencia, CNRS-LIX and Inria Saclay.

Other PI's and partner institutions: Carlos Olarte, Universidade Federal do Rio Grande do Norte, Brazil. Camilo Rueda, Universidad Javeriana de Cali, Colombia.

Abstract: The aim of the project is to coherently combine and advance the state of the art of domains such as concurrency theory, information theory and rewriting systems for reasoning about social networks.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

David de Frutos Escrig. Professor, Universidad Complutense Madrid, Spain. Jan-Feb 2017

Giovanni Cherubin, PhD student, Royal Holloway, University of London, UK. May 2017 and Oct 2017

Yusuke Kawamoto, Assistant Professor, National Institute of Advanced Industrial Science and Technology (AIST), Japan. July 2017 and Nov 2017

Carlos Olarte, Assistant Professor, Universidade Federal do Rio Grande do Norte, Brazil. July 2017

Camilo Rocha, Associate Professor, Universidad Javeriana de Cali, Colombia. Oct 2017

Camilo Rueda, Professor, Universidad Javeriana de Cali, Colombia. Nov 2017

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil. Dec 2017

7.4.2. Internships

Anna Pazii. Univ. of Kiev, Ukraine. From July 2016 until Jan 2017.

Hector Delgado, Universidad Javeriana de Cali, Colombia. From May 2017 until July 2017.

Marco Romanelli. Univ. of Siena, Italy. From June 2017 until Sept 2017.

Georgi Dikov. Tech. Univ. of Munich, Germany. From Sept 2017 until Nov 2017.

Joaquin Felici. Univ. of Cordoba, Argentina. From Sept 2017 until Jan 2018.

Santiago Quintero, Universidad Javeriana de Cali, Colombia. From Nov until Dec 2017.

DATASPHERE Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

L'équipe est hébergée dans l'IXXI, l'Institut Rhônalpin des Systèmes Complexes au sein de l'ENS de Lyon, et très impliquée dans les partenariats interdisciplinaires.

8.2. National Initiatives

- Chaire Castex, Ecole Militaire, Paris
- AMNECYS (Alpine Multidisciplinary NEtwork on CYber-security Studies), University of Grenoble-Alpes

8.3. International Initiatives

8.3.1. Informal International Partners

- RIHN, Research Institute on Humanity and Nature, Kyoto
- Information School, UC Berkeley
- ICT, Institute of Computing Technologies, Chinese Academy of Sciences, Beijing
- CSIRO, Sydney
- Center for CyberSecurity, University Macquarie, Sydney
- Center for Internet Human Rights (CIHR), Berlin

PESTO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. CNRS

- CNRS PEPS INS2I 2016-2018 project ASSI *Analyse de Sécurité de Systèmes Industriels*, duration: 2 years, leader: Pascal Lafourcade (Univ Clermont-Ferrand), participant Pesto: Jannik Dreier, other participants: Marie-Laure Potet, Maxime Puys (Univ 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, other partners: ENS Cachan, Univ Luxembourg. Most protocol analysis tools are restricted to analyzing reachability properties while many security properties need to be expressed in terms of some process equivalences. 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.
- ANR TECAP *Protocol Analysis — Combining Existing Tools*, duration: 4 years, starting in 2018, leader: Vincent Cheval, other partners: ENS Cachan, Inria Paris, Inria Sophia Antipolis, IRISA, LIX. Despite the large number of automated verification tools, several cryptographic protocols (e.g. stateful protocols) still represent a real challenge for these tools and reveal their limitations. To cope with these limits, each tool focuses on different classes of protocols depending on the primitives, the security properties, etc. Moreover, the tools cannot interact with each other as they evolve in their own model with specific assumptions. The aim of this project is to get the best of all these tools, meaning, to improve the theory and implementations of each individual tool towards the strengths of the others and, to build bridges that allow the cooperations of the methods/tools. We will focus in this project on the tools CryptoVerif, EasyCrypt, Scary, ProVerif, *TAMARIN*, *Akiss* and APTE. In order to validate the results obtained in this project, we will apply our results to several case studies such as the Authentication and Key Agreement protocol from the telecommunication networks, the Scytl and Helios voting protocols, and the low entropy authentication protocols 3D-Secure. These protocols have been chosen to cover many challenges that the current tools are facing.

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 based on 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

- 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 (Univ Oxford), and Sasa Radomirovic (Univ Dundee) on the improvement of the *TAMARIN* prover
- Collaboration with Bogdan Warinschi (Univ Bristol) on defining game-based privacy for e-voting protocols and isolated execution environments
- Collaboration with Myrto Arapinis (Univ 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 (Polytechnique Montreal) on model-checking of collaborative systems
- Collaboration with John Mullins's group (Polytechnique Montreal) on information hiding

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- David Galindo (Univ Birmingham), June 2017
- Bogdan Warinschi (Univ Bristol), November 2017

[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

Title: ADAGE (Anonymous Mobile Traffic Data Generation).

Type: FUI.

Duration: July 2016 - September 2018.

Coordinator: Orange.

Others partners: Inria, CNRS LAAS.

Abstract: The project ADAGE aims at developping solutions for the anonymization of mobility traces produced by mobile operators.

8.1.2. ANR

8.1.2.1. BIOPRIV

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

Type: ANR.

Duration: April 2013 - March 2017.

Coordinator: Morpho (France).

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

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

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

8.1.2.2. SIDES 3.0

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

Type: ANR.

Duration: August 2017 - August 2020.

Coordinator: Uness (France).

Others partners: Inria, UGA, ENS, Theia, Viseo.

Abstract: Since 2013, faculties of medicine have used a shared national platform that enables them to carry out all of their validating exams on tablets with automatic correction. This web platform entitled SIDES allowed the preparation of the medical students to the Computerized National Classing Events (ECN) which were successfully launched in June 2016 (8000 candidates simultaneously throughout France). SIDES 3.0 proposes to upgrade the existing platform. Privatics goals in this project is to ensure that privacy is respected and correctly assessed .

8.1.2.3. DAPCODS/IOTics

Title: DAPCODS/IOTics.

Type: ANR 2016.

Duration: May 2017 - Dec. 2020.

Coordinator: Inria PRIVATICS.

Others partners: Inria DIANA, EURECOM, Univ. Paris Sud, CNIL.

Abstract:

Thanks to the exponential growth of Internet, citizens have become more and more exposed to personal information leakage in their digital lives. This trend began with web tracking when surfing the Internet with our computers. The advent of smartphones, our personal assistants always connected and equipped with many sensors, further reinforced this tendency. And today the craze for "quantified self" wearable devices, for smart home appliances or for other connected devices enable the collection of potentially highly sensitive personal information in domains that were so far out of reach. However, little is known about the actual practices in terms of security, confidentiality, or data exchanges. The enduser is therefore prisoner of a highly asymmetric system. This has important consequences in terms of regulation, sovereignty, and leads to the hegemony of the GAFAs (Google, Amazon, Facebook and Apple). Security, transparency and user control are three key properties that should be followed by all the stakeholders of the smartphone and connected devices ecosystem. Recent scandals show that the reality is sometimes at the opposite.

The DAPCODS project gathers four renowned research teams, experts in security, privacy and digital economy. They are seconded by CNIL, the French data protection agency. The project aims at contributing along several axes:

- by analyzing the inner working of a significant set of connected devices in terms of personal information leaks. This will be made possible by analyzing their data flows (and associated smartphone application if applicable) from outside (smartphone and/or Wifi network) or inside, through ondevice static and dynamic analyses. New analysis methods and tools will be needed, some of them leveraging on previous works when applicable;
- by studying the device manufacturers' privacy policies along several criteria (e.g., accessibility, precision, focus, privacy risks). In a second step, their claims will be compared to the actual device behavior, as observed during the test campaigns. This will enable an accurate and unique ranking of connected devices;
- by understanding the underlying ecosystem, from the economical viewpoint. Data collected will make it possible to define the blurred boundaries of personal information market, a key aspect to set up an efficient regulation;
- and finally, by proposing a public website that will rank those connected devices and will inform citizens. We will then test the impact of this information on the potential change of behavior of stakeholders.

By giving transparent information of hidden behaviors, by highlighting good and bad practices, this project will contribute to reduce the information asymmetry of the system, to give back some control to the endusers, and hopefully to encourage certain stakeholders to change practices.

8.1.3. Inria Innovation Laboratory

Title: LEELCO (Low End-to-End Latency COmmunications).

Duration: 3 years (2015 - 2018).

Coordinator: Inria PRIVATICS.

Others partners: Expway.

Abstract:

This Inria Innovation Lab aims at strengthening Expway (http://www.expway.com/) commercial offer with technologies suited to real-time data transmissions, typically audio/video flows. In this context, the end-to-end latency must be reduced to a minimum in order to enable a high quality interaction between users, while keeping the ability to recover from packet losses that are unavoidable with wireless communications in harsh environments. In this collaboration we focus on new types of Forward Erasure Correction (FEC) codes based on a sliding encoding windows, and on the associated communication protocols, in particular an extension to FECFRAME (RFC6363) to such FEC codes. The outcomes of this work are proposed to both IETF and 3GPP standardisation organisations, in particular in the context of 3GPP mission critical communication services activity. The idea of this 3GPP activity is to leverage on the 3GPP Evolved Multimedia Broadcast Multicast Services (eMBMS) and on the existing Long Term Evolution (LTE) infrastructure for critical communications and such services as group voice transmissions, live high-definition video streams and large data transmissions. In this context, the advanced FEC codes studied in LEELCO offer a significant improvement both from the reduced latency and increased loss recovery viewpoints compared to the Raptor codes included in the existing standard (https://hal.inria.fr/hal-01571609v1/en/).

8.1.4. Inria CNIL project

Privatics is in charged of the Cnil-Inria collaboration. This collaboration was at the origin of the Mobilitics project and it is now at the source of many discussions and collaborations on data anoymisation, risk analysis, consent or IoT Privacy. Privatics and Cnil are both actively involved on the IoTics project, that is the follow-up of the Mobilitics projects. The goal of the Mobilitics project was to study information leakage in mobile phones. The goal of IoTics is to extend this work to IoT and connected devices.

Privatics is also in charged of the organization of the Cnil-Inria prize that is awarded every year to an outstanding publication in the field of data privacy.

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).

8.3.3. Data Institute

- Title: Data Institute UGA
- Duration: 2017 - .
- Coordinator: TIMC-IMAG.
- Others partners: AGEIS, BIG, CESICE, GIN, GIPSA-lab, IAB, IGE, IPAG, LAPP, LARHRA, LIDILEM, LIG, LISTIC, LITT&ArTS, LJK, LUHCIE, LECA, OSUG, PACTE, TIMC-IMAG, Inria

- Abstract: Privatics is leading the WP5 (Data Governance, Data Protection and Privacy). This action (WP5) aims to analyze, in a multi-disciplinary perspective, why and how specific forms of data governance emerge as well as the consequences on the interaction between the state, the market and society. The focus will be on the challenges raised by the collection and use of data for privacy, on the data subjects' rights and on the obligations of data controllers and processors. A Privacy Impact/Risk assessments methodology and software will be proposed. A case study will focus on medical and health data and make recommendations on how they should be collected and processed

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)

Participants: Karthikeyan Bhargavan, Bruno Blanchet, Nadim Kobeissi

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 sécurisation 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)

Participants: Karthikeyan Bhargavan

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.

8.2. 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
Programme: 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 can 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 Labs

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), Mozilla, University of Rennes
- **Web Security**: Microsoft Research (Cambridge, Redmond), Imperial College (London), University of Stuttgart
- **Micro-Policies**: University of Pennsylvania, Portland State University

8.3.2. Participation in Other International Programs

8.3.2.1. International Initiatives

Title: Advanced New Hardware Optimized for Policy Enforcement, A New HOPE

Program: DARPA SSITH

Duration: January 2016 - December 2018

Coordinator: Charles Stark, Draper Laboratory

Participants: Catalin Hritcu

Abstract: A New HOPE builds on results from the Inherently Secure Processor (ISP) project that has been internally funded at Draper. Recent architectural improvements decouple the tagged architecture from the processor pipeline to improve performance and flexibility for new processors. HOPE securely maintains metadata for each word in application memory and checks every instruction against a set of installed security policies. The HOPE security architecture exposes tunable parameters that support Performance, Power, Area, Software compatibility and Security (PPASS) search space exploration. Flexible software-defined security policies cover all 7 SSITH CWE vulnerability classes, and policies can be tuned to meet PPASS requirements; for example, one can trade granularity of security checks against performance using different policy configurations. HOPE will design and formalize a new high-level domain-specific language (DSL) for defining security policies, based on previous research and on extensive experience with previous policy languages. HOPE will formally verify that installed security policies satisfy system-wide security requirements. A secure boot process enables policies to be securely updated on deployed HOPE systems. Security policies can adapt based on previously detected attacks. Over the multi-year, multi-million dollar Draper ISP project, the tagged security architecture approach has evolved from early prototypes based on results from the DARPA CRASH program towards easier integration with external designs, and is better able to scale from micro to server class implementations. A New HOPE team is led by Draper and includes faculty from University of Pennsylvania (Penn), Portland State University (PSU), Inria, and MIT, as well as industry collaborators from DornerWorks and Dover Microsystems. In addition to Draper's in-house expertise in hardware design, cyber-security (defensive and offensive, hardware and software) and formal methods, the HOPE team includes experts from all domains relevant to SSITH, including (a) computer architecture: DeHon (Penn), Shrobe (MIT); (b) formal methods including programming languages and security: Pierce (Penn), Tolmach (PSU), Hritcu (Inria); and (c) operating system integration (DornerWorks). Dover Microsystems is a spin-out from Draper that will commercialize concepts from the Draper ISP project.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Claudia Diaz from KUL visited the group from 1-2 March and gave a seminar “Designing Mixnets”
- Peter Schwabe visited Inria Paris on 11 April; he gave a seminar: From NewHope to Kyber.
- Joseph Bonneau (Stanford University) visited Inria on 20 April 2017, he gave a seminar: Public randomness, blockchains and proofs-of-delay
- Stefan Ciobaca (Alexandru Ioan Cuza University of Iai, Romania) visited Inria Paris on 15 May 2017; he gave a seminar: The RMT Tool for Rewriting Modulo Theories.
- Ana Nora Evans (University of Virginia) joined Inria as a Visiting Scientist Apr–Aug 2017; she gave a seminar: Using Verified Software Fault Isolation for a Formally Secure Compiler.
- David Evans (University of Virginia) joined Inria as a Visiting Scientist Apr–Aug 2017; he gave a seminar: Can Machine Learning Work in the Presence of Adversaries?

- Jean Yang (CMU) visited Inria Paris on 6 June 2017; she gave a seminar: Policy-Agnostic Programming for Database-Backed Applications.
- Amal Ahmed (Northeastern University) joined Inria as a Visiting Professor from September 2017; she gave a seminar: Prosecco Seminars: Compositional Compiler Verification for a Multi-Language World.
- Aaron Weiss (Northeastern University) joined Inria as a Visiting Scientist from September 2017.
- Amin Timany (KU Leuven) visited Inria Paris 6-8 December 2017; he gave a seminar: A Logical Relation for Monadic Encapsulation of State: Proving contextual equivalences in the presence of runST.
- Eric Rescorla visited Prosecco to discuss the design of TLS 1.3.

8.4.1.1. Internships

- Benjamin Lipp: Dec 2017 until May 2018, supervised by B. Blanchet, K. Bhargavan, and H. Halpin
- Iness Ben Guirat: Masters student 2017, supervised by H. Halpin
- Carmine Abate (University of Trento): Dec 2017 until May 2018
- William Bowman (Northeastern University): Oct 2017 until Dec 2017
- Keith Cannon (American University Paris): Mar 2017 until Sep 2017
- Théo Laurent (ENS Paris): Mar 2017 until Aug 2017
- Clément Pit-Claudel (MIT): Jul 2017 until Oct 2017

8.4.2. Visits to International Teams

- Catalin Hritcu, October 8-13, 2017, Aarhus University, Denmark.
- Catalin Hritcu, October 16-17, 2017, MPI-SWS, Saarbrucken, Germany.
- Catalin Hritcu, December 18, 2017, University of Iasi, Romania.

TAMIS Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

- ARED grant for Lamine Nouredine and Florian Dolt
- Postdocs grants for Najah Ben Said, Jeffrey Paul Burdges, Ronan Lashermes, Ludovic Claudepierre
- Starting Grant for hardware for Annelie Heuser from Rennes Metropole
- Software developer grant for Laurent Morin from "Chaire Mobilité dans une ville durable" (mobility in a sustainable city) by Fondation Université Rennes 1

9.2. National Initiatives

9.2.1. ANR

- ANR MALTHY, Méthodes ALgébriques 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.

9.2.2. DGA

- PhD grant for Nisrine Jafri (2016–2019),
- PhD grant for Aurélien Palisse (2016–2019),
- PhD grant for Alexandre Gonzalves (2016–2019),
- PhD grant for Olivier Decourbe (2017–2020),
- PhD grant for Alexandre Zdhanov (2017–2020)

9.2.3. Autres

- INS2I JCJC grant for Axel Legay, Annelie Heuser, Fabrizio Biondi.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. ACANTO

Title: ACANTO: A CyberphusicAl social NeTwOrk using robot friends

Program: H2020

Duration: February 2015 - July 2018

Coordinator: Universita di Trento

Partners:

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

Inria contact: Axel Legay

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

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

Title: DIVIDEND: Distributed Heterogeneous Vertically IntegrateD Energy Efficient Data centres

Program: CHIST-ERA 2013

Duration: 10/2014 - 10/2016 (extended 10/2017)

Coordinator: University of Edinburgh (UK)

Partners:

> École Normale Supérieure de Paris, Département d'Informatique (France); Inria (France); Ecole Polytechnique Fédérale de Lausanne, Computer & Communication Sciences (Switzerland); Queen's University of Belfast, School of Electronics, Electrical Engineering and Computer Science, Belfast (UK); University of Edinburgh, Scotland, (UK); University of Lancaster, School of Computing and Communications (UK); University Politehnica Timisoara, Department of Computer Engineering (Romania)

Inria contact: Albert Cohen

The DIVIDEND project (http://www.chistera.eu/projects/dividend) attacks the data centre energy efficiency bottleneck through vertical integration, specialization, 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 specialization 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.

Contributions of Inria in the project addresses the development of an energy aware distributed heterogeneous system (distributed HSA) between data center applications and HSA accelerators. It includes the design of a common API able to interface two tasks: the monitoring of the energy consumption, and the management of distributed heterogeneous hardware at a data center scale. The project ended by a project review the 23th March 2017, and the last contributions to the project ended the 30th September 2017.

One of the main contribution is the design of and energy-aware distributed heterogeneous system architecture framework (D-HSA) built using the combination of three major levels: the hardware platform based on an aggregation of HSA compliant devices, the system level based on device drivers and energy monitoring libraries, and finally the application layer using an extension of standard OpenCL programming model. This OpenCL extension is proposed as the main API for the energy-aware distributed HSA, and was made available for the tools and applications developed in the project.

A second contribution is the specification and the implementation of a distributed extension of the standard HSA Runtime API, and its functional validation on a basic system. The extension integrates the discovery, the management, and the execution of kernel computations on remote HSA agents in a distributed environment. The validation is based on an implementation using the Message Passing Interface (MPI) standard on an HSA compliant AMD machine. The Distributed HSA extension proposed offers a fully functional API for managing remote and distributed HSA agents, but at the cost of a limitation of the capability of the D-HSA system: the standard HSA memory model, based essentially on a coherent shared memory, is not supported for distributed HSA agents. As a primary implementation, focusing on a functional support of the new D-HSA verbs, this works tend to demonstrate that the extension is light and easy-to-use for a set of examples.

Laurent Morin from Tamis is involved in this project

9.3.1.3. EMC2

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

Program: FP7

Duration: April 2014 - March 2017

Coordinator: Infineon Technologies

Partners:

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

Alenia Aermacchi Spa (Italy), Avl List (Austria), Airbus Defence and Space (Germany), Bayerische Motoren Werke Aktiengesellschaft (Germany), Vysoke Uceni Technicke V Brne (Czech Republic), Commissariat A L Energie Atomique et Aux Energies Alternatives (France), Consorzio Interuniversitario Nazionale Per l'Informatica (Italy), Centro Ricerche Fiat (Italy), Critical Software (Portugal), Chalmers Tekniska Hoegskola (Sweden), Danfoss Power Electronics As (Denmark), Danmarks Tekniske Universitet (Denmark), Ericsson (Sweden), Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (Germany), Hi Iberia Ingenieria Y Proyectos Sl (Spain), Harokopio University (Greece), Infineon Technologies Austria (Austria), Institut Mikroelektronickych Aplikaci S.R.O. (Czech Republic), Inesc Id - Instituto de Engenharia de Sistemas E Computadores, Investigacao E Desenvolvimento Em Lisboa (Portugal), Infineon Technologies (Germany), Integrasys (Spain), Instituto Superior de Engenharia Do Porto (Portugal), Kungliga Tekniska Hoegskolan (Sweden), Lulea Tekniska Universitet (Sweden), Magillem Design Servicess (France), Nxp Semiconductors Netherlands Bv (Netherlands), Offis E.V. (Germany), Philips Medical Systems Nederland Bv (Netherlands), Politecnico di Torino (Italy), Quobis Networks Sl (Spain), Rockwell Collins France (France), Rigas Tehniska Universitate (Latvia), Selex Es Spa (Italy), Siemens Aktiengesellschaft (Germany), Systematic Paris Region Association (France), Sysgo (Germany), Thales Alenia Space Italia Spa (Italy), "thales Alenia Space Espana," (Spain), Technolution B.V. (Netherlands), Fundacion Tecnalia Research & Innovation (Spain), Thales Communications & Securitys (France), Thales Avionicss (France), Thales (France), Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (Netherlands), Technische Universitat Braunschweig (Germany), Technische Universiteit Delft (Netherlands), Technische Universitat Dortmund (Germany), Technische Universitaet Kaiserslautern (Germany), Technische Universitaet Wien (Austria), Technische Universiteit Eindhoven (Netherlands), Universita Degli Studi di l'aquila (Italy), Universita Degli Studi di Genova (Italy), The University of Manchester (United Kingdom), University of Bristol (United Kingdom), University of Limerick (Ireland), "ustav Teorie Informace A Automatizace Av Cr, V.V.I." (Czech Republic), Universitetet I Oslo (Norway), Vector Fabrics Bv (Netherlands), Volvo Technology (Sweden)

Inria contact: Albert Cohen and Axel Legay

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

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

Title: ENABLE-S3: European Initiative to Enable Validation for Highly Automated Safe and Secure Systems

Program: H2020

Duration: 05/2016 - 04/2019

Coordinator: Avl List Gmbh (Austria)

Partners:

> Aalborg Universitet (Denmark); Airbus Defence And Space Gmbh (Germany); Ait Austrian Institute Of Technology Gmbh (Austria); Avl Deutschland Gmbh (Germany); Avl Software And Functions Gmbh (Germany); Btc Embedded Systems Ag (Germany); Cavotec Germany Gmbh (Germany); Creanex Oy(Finland); Ceske Vysoke Uceni Technicke V Praze (Czech Republic); Deutsches Zentrum Fuer Luft - Und Raumfahrt Ev (Germany); Denso Automotive Deutschland Gmbh (Germany); Dr. Steffan Datentechnik Gmbh (Austria); Danmarks Tekniske Universitet (Denmark); Evidence Srl (Italy); Stiftung Fzi Forschungszentrum Informatik Am Karlsruher Institut Fur Technologie (Germany); Gmv Aerospace And Defence Sa (Spain); Gmvis Skysoft Sa (Portugal); Politechnika Gdanska (Poland); Hella Aglaia Mobile Vision Gmbh (Germany); Ibm Ireland Limited (Ireland); Interuniversitair Micro-Electronica Centrum (Belgium); Iminds (Belgium); Institut National De Recherche Eninformatique Et Automatique (France); Instituto Superior De Engenharia Do Porto (Portugal); Instituto Tecnologico De Informatica (Spain); Ixion Industry And Aerospace Sl (Spain); Universitat Linz (Austria); Linz Center Of Mechatronics Gmbh (Austria); Magillem Design Services Sas (France); Magneti Marelli S.P.A. (Italy); Microeletronica Maser Slspain); Mdal (France); Model Engineering Solutions Gmbhgermany); Magna Steyr Engineering Ag & Co Kg (Austria); Nabto Aps (Denmark); Navtor As (Norway); Nm Robotic Gmbh (Austria); Nxp Semiconductors Germany Gmbh(Germany); Offis E.V.(Germany); Philips Medical Systems Nederland Bvnetherlands); Rohde & Schwarz Gmbh&Co Kommanditgesellschaft(Germany); Reden B.V. (Netherlands); Renault Sas (France); Rugged Tooling Oyfinland); Serva Transport Systems Gmbh(Germany); Siemens Industry Software Nvbelgium); University Of Southampton (Uk); Safetrans E.V. (Germany); Thales Alenia Space Espana, Saspain); Fundacion Tecnalia Research & Innovationspain); Thales Austria Gmbh (Austria); The Motor Insurance Repair Researchcentre (Uk); Toyota Motor Europe (Belgium); Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (Netherlands); Ttcontrol Gmbh (Austria); Tttech Computertechnik Ag (Austria); Technische Universiteit Eindhoven (Netherlands); Technische Universitat Darmstadt (Germany); Technische Universitaet Graz (Austria); Twt Gmbh Science & Innovation (Germany); University College Dublin, National University Of Ireland, Dublin (Ireland); Universidad De Las Palmas De Gran Canaria (Spain); Universita Degli Studi Di Modena E Reggio Emilia (Italy); Universidad Politecnica De Madrid (Spain); Valeo Autoklimatizace K.S. (Czech Republic); Valeo Comfort And Driving Assistance (France); Valeo Schalter Und Sensoren Gmbh (Germany); Kompetenzzentrum - Das Virtuelle Fahrzeug, Forschungsgesellschaft Mbh (Austria); Vires Simulationstechnologie Gmbh (Germany); Teknologian Tutkimuskeskus Vtt Oy (Finland); Tieto Finland Support Services Oy (Finland); Zilinska Univerzita V Ziline (Slovakia);

Inria contact: Axel Legay

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.

9.3.1.5. SUCCESS

Title: SUCCESS: SecUre aCCESSibility for the internet of things

Program: CHIST-ERA 2015

Duration: 10/2016 - 10/2018

Coordinator: Middlesex University (UK)

Partners:

> Middlesex University, School of Science and Technology (France); Inria (France); Université Grenoble Alpes, Verimag (FRANCE); Univesity of TWENTE, (Netherlands)

Inria contact: Axel Legay

The SUCCESS project ...The core idea of SUCCESS is to use formal methods and verification tools with a proven track record to provide more transparency of security risks for people in given IoT scenarios. Our core scientific innovation will consist on the extension of well-known industry-strength methods Our technological innovation will provide adequate tools to address risk assessment and adaptivity within IoT in healthcare environments and an open source repository to foster future reuse, extension and progress in this area. Our project will validate the scientific and technological innovation through pilots, one of which will be in collaboration with a hospital and will allow all stakeholders (e.g. physicians, hospital technicians, patients and relatives) to enjoy a safer system capable to appropriately handle highly sensitive information on vulnerable people while making security and privacy risks understandable and secure solutions accessible.

Within SUCCESS, the contribution of the TAMIS team consists in a framework for analyzing the security of a given IOT system, and notably whether it resists to attack. Our approach is to build a high-level model of the system, including vulnerabilities, as well as an attacker. We represent the set of possible attacks using an attack tree. Finally, we evaluate the probability that an attack succeeds using Statistical Model Checking.

In the TAMIS team, Axel Legay, Delphine Beaulaton, Najah Ben-Saïd and Jean Quilbeuf are involved in this project.

9.3.1.6. TeamPlay

Title: TeamPlay: Time, Energy and security Analysis for Multi/Many-core heterogeneous PLAtforms

Program: H2020

Duration: 01/2018 - 12/2020

Coordinator: Inria

Partners:

Absint Angewandte Informatik Gmbh (Germany), Institut National De Recherche en Informatique et Automatique (France), Secure-Ic Sas (France), Sky-Watch A/S (Danemark), Syddansk Universitet (Danemark), Systhmata Ypologistikis Orashs Irida Labs Ae (Greece), Technische Universität Hamburg-Harburg (Germany), Thales Alenia Space Espana (Spain), Universiteit Van Amsterdam (Netherlands), University Of Bristol (UK), University Of St Andrews (UK)

Inria contact: Olivier Zendra and Axel Legay

The TeamPlay (Time, Energy and security Analysis for Multi/Many-core heterogeneous PLAtforms) project federates 6 academic and 5 industrial partners and aims to develop new, formally-motivated, techniques that will allow execution time, energy usage, security, and other important non-functional properties of parallel software to be treated effectively, and as first- class citizens. We will build this into a toolbox for developing highly parallel software for low-energy systems, as required by the internet of things, cyber-physical systems etc. The TeamPlay approach will allow programs to reflect directly on their own time, energy consumption, security, etc., as well as enabling the developer to reason about both the functional and the non-functional properties of their software at the source code level. Our success will ensure significant progress on a pressing problem of major industrial importance: how to effectively manage energy consumption for parallel systems while maintaining the right balance with other important software metrics, including time, security etc. The project brings together leading industrial and academic experts in parallelism, energy modeling/ transparency, worst-case execution time analysis, non-functional property analysis, compilation, security, and task coordination. Results will be evaluated using industrial use cases taken from the computer vision, satellites, flying drones, medical and cyber security domains. Within TeamPlay, Inria and TAMIS coordinate the whole project, while being also in charge of aspects related more specifically to security.

The permanent members of Tamis who are involved are Axel Legay, Olivier Zendra and Annelie Heuser.