RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2018

Section Partnerships and Cooperations

Edition: 2019-03-07

ARIC Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR DYNA3S Project

Participants: Guillaume Hanrot, Gilles Villard.

Dyna3S has been a 2013-2018 ANR project headed by Valérie Berthé (IRIF, U. Paris 7). The Web page of the project is https://www.irif.fr/~dyna3s. The aim of Dyna3S was 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. In Lyon we have worked on the computation of the gcd of several integers, in link with integer relation algorithms based on lattice basis reduction. A main motivation of Dyna3S was also discrete geometry, a framework where the understanding of basic primitives, discrete lines and planes, relies on algorithms of the Euclidean type.

9.1.2. 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 and extended till September 2019). 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.

9.1.3. ANR MetaLibm Project

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

MetaLibm is a four-year project (started in October 2013 and 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.

9.1.4. 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.

9.1.5. RISQ Project

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

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.

9.2. European Initiatives

9.2.1. LattAC ERC grant

Participants: Shi Bai, Laurent Grémy, Gottfried Herold, Elena Kirshanova, Fabien Laguillaumie, Huyen Nguyen, Alice Pellet–Mary, Miruna Rosca, Damien Stehlé, Alexandre Wallet, Weiqiang Wen.

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.

9.2.2. PROMETHEUS Project

Participants: Laurent Grémy, Fabien Laguillaumie, Benoît Libert, 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 started in January 2018. It gathers 8 academic partners (ENS de Lyon and Université de Rennes 1; CWI, Pays-Bas; IDC Herzliya, Israel; Royal Holloway University of London, United Kingdom; Universitat Politècnica de Catalunya, Spain; Ruhr-Universität Bochum, Germany; Weizmann Institute, Israel), 4 industrial partners (Orange, 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.

9.2.3. Other international projects

9.2.3.1. IFCPAR grant: "Computing on Encrypted Data: New Paradigms in Functional Encryption"

Participants: Benoît Libert, Damien Stehlé.

3-year project accepted in July 2018. Expected beginning on January 1, 2019. Benoît Libert is co-PI with Shweta Agrawal (IIT Madras, India). Budget on the French side amounts to 100k€.

Functional encryption is a paradigm that enables users to perform data mining and analysis on encrypted data. Users are provided cryptographic keys corresponding to particular functionalities which enable them to learn the output of the computation without learning anything about the input. Despite recent advances, efficient realizations of functional encryption are only available for restricted function families, which are typically represented by small-depth circuits: indeed, solutions for general functionalities are either way too inefficient for pratical use or they rely on uncertain security foundations like the existence of circuit obfuscators (or both). This project will explore constructions based on well-studied hardness assumptions and which are closer to being usable in real-life applications. To this end, we will notably consider solutions supporting other models of computation than Boolean circuits – like Turing machines – which support variable-size inputs. In the context of particular functionalities, the project will aim for more efficient realizations that satisfy stronger security notions.

9.3. International Initiatives

9.3.1. Participation in International Programs

Vincent Lefèvre actively participated in the revision of the IEEE Standard for Floating-Point Arithmetic (IEEE 754) for 2019.

9.4. International Research Visitors

9.4.1. 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 spent the academic year 2017-2018 with AriC.
- Warwick Tucker, from Uppsala University (Sweden), is an expert of certified computation for dynamical systems. He spent the academic year 2017-2018 with AriC.

9.4.2. Internships

Monosij Maitra, PhD student at IIT Madras (India) under the supervision of Shweta Agrawal, did a 2-month internship, in September and October 2018.

Joel Dahne did an internship with Bruno Salvy from May to July.

9.4.3. Visits to International Teams

- From November 15 to December 15, 2018, Benoît Libert visited the "Cryptography and Coding Research Group" of the Nanyang Technological University (Singapore).
- From July 1 to July 31, 2018, Damien Stehlé visited the cryptography group of Prof. Jung Hee Cheon, at Seoul National University (South Korea)

AROMATH Project-Team

7. Partnerships and Cooperations

7.1. 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.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Program: Marie Skłodowska-Curie ITN

Project acronym: ARCADES

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

Duration: January 2016 - December 2019

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

Scientist-in-charge at Inria: L. Busé

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

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

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

7.3. International Initiatives

7.3.1. Inria International Partners

NSFC collaboration project with Gang Xu, Hangzhou Dianzi University, China, “Research on theory and method of time-varying parameterization for dynamic isogeometric analysis”, 2018-2021.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Aron Simis, University of Recife, Brazil, visited L. Busé for a week (October 8-12) to work on birationality of rational map by means of syzygy-based techniques.

Ibrahim Adamou, Univ. Dan Dicko Dankoulodo de Maradi, Niger, visited B. Mourrain (26 Nov.- 21 Dec.) to work on 3-dimensional VoronoïDiagrams of half-lines and medial axes of curve arcs.

7.4.1.1. Internships

Yairon Cid Ruiz, a PhD srudent at Barcelona in the Arcades network, visited L. Busé for 6 months (October 2017- March 2018) to work on birationality criteria for multi-graded rational maps with a view towards free form deformation problems.

Clément Laroche, a PhD student in Greece in the Arcades network, visited L. Busé and F. Yildirim for one month (October) for a collaboration on implicization matrices of rational curve in arbitrary dimension by means of quadratic relations.

Kim Perriguey, did a six months internship with L. Busé (December 2017-May 2018). She developed paramteric models for the human walk for the extraction of locomotive parameters. This work was done in collaboration with Pierre Alliez (EPI Titane) and the start-up Ekinnox (Sophia Antipolis).

7.4.2. Visits to International Teams

7.4.2.1. Research Stays Abroad

F. Yildirim was on secondment at MISSLER Topsolid (France), for 3 months (Mai-July).

From October 25th to November 25th, E. Hubert visited the Institute for Computational and Experimental Research in Mathematics (Providence USA) during the program *Nonlinear Algebra*.

CARAMBA Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. CPER CyberEntreprises

Program: CPER (Contrat de Plan État Région)

Project title: Cyber-Entreprises

Duration: 01/07/2015 - 31/12/2020

Coordinator: Emmanuel Thomé and Marc Jungers (CRAN)

Other partners: Inria, LORIA, CRAN, IECL, Centrale Supelec, LCFC.

Abstract: cf web site (in French only).

A high-performance computer cluster was funded by the CPER Cyber-entreprises project (Région Grand-Est, French Ministry of Research and Higher Education, Inria, CNRS). This cluster is also mentioned in 6.4 .

9.2. National Initiatives

9.2.1. FUI Industrial Partnership on Lightweight Cryptography

Program: FUI (Fonds Unique Interministériel)

Project acronym: PACLIDO

Project title: Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets

Duration: 12/2017 - 12/2020

Coordinator: Airbus Cybersecurity.

Other partners: organisme, labo (pays) Airbus Cybersecurity, LORIA-CNRS, Rtone, Trusted Objects, CEA, Sophia Engineering, Université de Limoges, Saint-Quentin-en-Yvelines.

This contract is dedicated to the definition of new lightweight cryptographic primitives for the IoT. See web site for a full presentation.

CASCADE Project-Team

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. ANBLIC

Title: Analysis in Blind Clouds

Program: FUI

Duration: January 2018 – December 2020

Coordinator: Wallix

Partners: UPEC, CEA, Ingenico, Atos, SOGETI, CoeSSI

Local coordinator: David Pointcheval

The main goal is to industrialize for the first time several privacy enhancing technologies that are on the edge of theory and practice.

Fully Homomorphic Encryption let cloud providers compute arbitrary functions on their client's encrypted data, ensuring at the same time full privacy and functionality. Functional Encryption is a refinement of classical encryption, which allows data owners to delegate fine-grained access to their data. Thus it is possible to enable the computation of aggregated statistics over your personal data, while cryptographically ensuring its confidentiality.

However both these technologies still suffer from prohibitive inefficiencies for business applications. ANBLIC's academic partners will create new cryptographic schemes and performance models, tailored for industrial use cases, and create the first real-life scenario of encrypted queries on encrypted data and on open data.

7.1.3. 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 with Academics

7.2.1. EnBiD

Title: Encryption for Big Data

Program: ANR JCJC

Duration: October 2014 – September 2019

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 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 2020

PI: David Pointcheval

The goal of the CryptoCloud project is to develop new interactive tools to provide privacy in 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 a 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 number of IOT devices.

7.4. International Initiatives with Industry

7.4.1. CryptBloC

Title: Cryptography for 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 and decentralized systems more generally. 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

- Yuval Ishai (Technion)
- Dan Boneh (Stanford)
- Katsuyuki Takashima (Mitsubishi and Kyushu University)
- Tal Malkin (Columbia)
- Adam O'Neill (Georgetown University)
- Julian Loss (Ruhr Universität Bochum)

DATASHAPE Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. ANR ASPAG

Participant: Marc Glisse.

- Acronym : ASPAG.

- Type : ANR blanc.

- Title : Analysis and Probabilistic Simulations of Geometric Algorithms.

- Coordinator : Olivier Devillers (équipe Inria Gamble).

- Duration : 4 years from January 2018 to December 2021.

- Others Partners: Inria Gamble, LPSM, LABRI, Université de Rouen, IECL, Université du Littoral Côte d'Opale, Telecom ParisTech, Université Paris X (Modal'X), LAMA, Université de Poitiers, Université de Bourgogne.

- Abstract:

The analysis and processing of geometric data has become routine in a variety of human activities ranging from computer-aided design in manufacturing to the tracking of animal trajectories in ecology or geographic information systems in GPS navigation devices. Geometric algorithms and probabilistic geometric models are crucial to the treatment of all this geometric data, yet the current available knowledge is in various ways much too limited: many models are far from matching real data, and the analyses are not always relevant in practical contexts. One of the reasons for this state of affairs is that the breadth of expertise required is spread among different scientific communities (computational geometry, analysis of algorithms and stochastic geometry) that historically had very little interaction. The Aspag project brings together experts of these communities to address the problem of geometric data. We will more specifically work on the following three interdependent directions.

(1) Dependent point sets: One of the main issues of most models is the core assumption that the data points are independent and follow the same underlying distribution. Although this may be relevant in some contexts, the independence assumption is too strong for many applications.

(2) Simulation of geometric structures: The phenomena studied in (1) involve intricate random geometric structures subject to new models or constraints. A natural first step would be to build up our understanding and identify plausible conjectures through simulation. Perhaps surprisingly, the tools for an effective simulation of such complex geometric systems still need to be developed.

(3) Understanding geometric algorithms: the analysis of algorithm is an essential step in assessing the strengths and weaknesses of algorithmic principles, and is crucial to guide the choices made when designing a complex data processing pipeline. Any analysis must strike a balance between realism and tractability; the current analyses of many geometric algorithms are notoriously unrealistic. Aside from the purely scientific objectives, one of the main goals of Aspag is to bring the communities closer in the long term. As a consequence, the funding of the project is crucial to ensure that the members of the consortium will be able to interact on a very regular basis, a necessary condition for significant progress on the above challenges.

- See also: https://members.loria.fr/Olivier.Devillers/aspag/

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 Research Visitors

9.3.1. Visits of International Scientists

- Wolfgang Polonik, UC Davis, California. Sept. and Oct. 2018. Statistical aspects of persistent homology.
- Arijit Ghosh, Indian Statistical Institute, Kolkata, India (December 2018)
- Ramsay Dyer, Berkeley Publishing (December 2018)

9.3.1.1. Internships

- Shreya Arya, BITS Pilani University, India, August-July 2018.

GAIA Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- *ANR project MSDOS* (Multidimensional System: Digression on Stability, coordinator: Nima Yeganefar (Poitiers University), 2014-2018) aimed at studying stability and stabilization problems for multidimensional systems by means of both analytic and algebraic methods. For more information, see https://www.lias-lab.fr/msdos/doku.php.
- *ANR TurboTouch* (High-performance touch interactions, coordinator: G. Casiez (MJOLNIR team, Inria), 2014–2019) develops methods and tools on transfer functions to allow high performance tactile interactions (e.g. high precision and low latency) adapted to the user and to the task. This research project is developed in collaboration with the Loki team, Inria Lille – Nord Europe (project leader). For more information, seehttp://mjolnir.lille.inria.fr/turbotouch/.
- *ANR WaQMoS* (Coastal waters Quality surveillance using bivalve Mollusk-based Sensors, coordinator: D. Efimov (Non-A Post, Inria), 2015–2020) develops a biosensor, based on measurements and interpretation of bi- valves mollusks behavior, for remote online detection of coastal water pollution and cli- mate change consequences. This research project is developed in collaboration with the Valse team, Inria Lille – Nord Europe (project leader). For more information, see https://team.inria.fr/non-a/anr-waqmos/.

9.2. European Initiatives

9.2.1. Collaborations with Major European Organizations

Mohamed Barakat: University of Siegen (Germany)
Effective module theory, effective homological algebra, algebraic analysis, computer algebra, implementation.
Georg Regensburger: Institute for Algebra, Johannes Kepler University Linz (Austria)
Rings of integro-differential-delay operators, computer algebra, implementation.
Daniel Robertz: University of Plymouth (United Kingdom)
Effective algebraic analysis, mathematical systems theory, computer algebra, implementation.

9.3. International Initiatives

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

WeCare, Inria Northern European Associate Team with the team of A. Medvedev from Uppsala University on effective algorithms for estimation and control in wearable devices for health and care, 2018–2020.

We participate in *HoTSMoCE*, an Inria Associated team with Non-A Post and the team of L. Fridman (UNAM, Mexico), on the development of algebraic and homogeneous tools for sliding mode control and estimation.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Thomas Cluzeau, XLIM, University of Limoges, May 2018.
- Marc Moreno Maza, University of Western Ontario, London, Ontario, Canada, September 2018.
- Alexander Medvedev, University of Uppsala (03–05/10/2018).
- Fredrik Olsson, University of Uppsala (26–30/11/2018).
- Elisa Hubert (Safran Tech) visited us twice (23–24/07/2018, 12–13/09/2018) to work on the problem of gear fault diagnostic based on algebraic and symbolic approaches.

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

Project title: Singular Curves and Surfaces Topology
Duration: March 2014 – August 2018
Coordinators: Guillaume Moroz 60%, and Marc Pouget 40%
Abstract: The objective of the young-researcher ANR grant SingCAST was to intertwine further symbolic/numeric approaches to compute efficiently solution sets of polynomial systems with topological and geometrical guarantees in singular cases. We focused on two applications: the visualization of algebraic curves and surfaces and the mechanical design of robots. We developed 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.

The project had a total budget of 100k€. Project website: https://project.inria.fr/singcast/.

9.2.2. ANR SoS

Project title: Structures on Surfaces
Duration: 4 years
Starting Date: April 1st, 2018
Coordinator: Monique Teillaud
Participants:

- Gamble project-team, Inria.
- LIGM (Laboratoire d'Informatique Gaspard Monge), Université Paris-Est Marne-la-Vallée. Local Coordinator: Éric Colin de Verdière.
- RMATH (Mathematics Research Unit), University of Luxembourg. National Coordinator: Hugo Parlier

SoS is co-funded by ANR (ANR-17-CE40-0033) and FNR (INTER/ANR/16/11554412/SoS) as a PRCI (Projet de Recherche Collaborative Internationale).

The central theme of this project is the study of geometric and combinatorial structures related to surfaces and their moduli. Even though they work on common themes, there is a real gap between communities working in geometric topology and computational geometry and SoS aims to create a long lasting bridge between them. Beyond a common interest, techniques from both ends are relevant and the potential gain in perspective from long-term collaborations is truly thrilling.

In particular, SoS aims to extend the scope of computational geometry, a field at the interface between mathematics and computer science that develops algorithms for geometric problems, to a variety of unexplored contexts. During the last two decades, research in computational geometry has gained wide impact through CGAL, the Computational Geometry Algorithms Library. In parallel, the needs for non-Euclidean geometries are arising, e.g., in geometric modeling, neuromathematics, or physics. Our goal is to develop computational geometry for some of these non-Euclidean spaces and make these developments readily available for users in academy and industry.

To reach this aim, SoS will follow an interdisciplinary approach, gathering researchers whose expertise cover a large range of mathematics, algorithms and software. A mathematical study of the objects considered will be performed, together with the design of algorithms when applicable. Algorithms will be analyzed both in theory and in practice after prototype implementations, which will be improved whenever it makes sense to target longer-term integration into CGAL.

Our main objects of study will be Delaunay triangulations and circle patterns on surfaces, polyhedral geometry, and systems of disjoint curves and graphs on surfaces.

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

9.2.3. ANR Aspag

Project title: Analyse et Simulation Probabilistes d'Algorithmes Géométriques
Duration: 4 years
Starting date: January 1st, 2018
Coordinator: Olivier Devillers
Participants:

- Gamble project-team, Inria.
- Labri (Laboratoire Bordelais de Recherche en Informatique), Université de Bordeaux. Local Coordinator: Philippe Duchon.
- Laboratoire de Mathématiques Raphaël Salem, Université de Rouen. Local Coordinator: Pierre Calka.
- LAMA (Laboratoire d'Analyse et de Mathématiques Appliquées), Université Paris-Est Marne-la-Vallée. Local Coordinator: Matthieu Fradelizi

Abstract: ASPAG projet is funded by ANR undered number ANR-17-CE40-0017 .

The analysis and processing of geometric data has become routine in a variety of human activities ranging from computer-aided design in manufacturing to the tracking of animal trajectories in ecology or geographic information systems in GPS navigation devices. Geometric algorithms and probabilistic geometric models are crucial to the treatment of all this geometric data, yet the current available knowledge is in various ways much too limited: many models are far from matching real data, and the analyses are not always relevant in practical contexts. One of the reasons for this state of affairs is that the breadth of expertise required is spread among different scientific communities (computational geometry, analysis of algorithms and stochastic geometry) that historically had very little interaction. The Aspag project brings together experts of these communities to address the problem of geometric data. We will more specifically work on the following three interdependent directions.

(1) Dependent point sets: One of the main issues of most models is the core assumption that the data points are independent and follow the same underlying distribution. Although this may be relevant in some contexts, the independence assumption is too strong for many applications.

(2) Simulation of geometric structures: The phenomena studied in (1) involve intricate random geometric structures subject to new models or constraints. A natural first step would be to build up our understanding and identify plausible conjectures through simulation. Perhaps surprisingly, the tools for an effective simulation of such complex geometric systems still need to be developed.

(3) Understanding geometric algorithms: the analysis of algorithm is an essential step in assessing the strengths and weaknesses of algorithmic principles, and is crucial to guide the choices made when designing a complex data processing pipeline. Any analysis must strike a balance between realism and tractability; the current analyses of many geometric algorithms are notoriously unrealistic. Aside from the purely scientific objectives, one of the main goals of Aspag is to bring the communities closer in the long term. As a consequence, the funding of the project is crucial to ensure that the members of the consortium will be able to interact on a very regular basis, a necessary condition for significant progress on the above challenges.

Project website: https://members.loria.fr/Olivier.Devillers/aspag/.

9.2.4. PHC Embeds II

Embeds is a bilateral, two-year project funded by the PHC Barrande program. It is joint between various french locations (Paris Est, Grenoble and, since september 2018, Nancy) and Charles University (Prague). The PI are Xavier Goaoc and Martin Tancer. It started in 2015 for two years, and was renewed in 2017 for two more years (5kE/year on the french side to support travels).

Starting Date: January 1st, 2017.
Duration: 2 years.

9.2.5. Institut Universitaire de France

Xavier Goaoc was appointed *junior member* of the Institut Universitaire de France, a grant supporting a reduction in teaching duties and funding.

Starting Date: October 1st, 2014.
Duration: 5 years.

9.3. International Initiatives

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

9.3.1.1. TRIP

Title: Triangulation and Random Incremental Paths

International Partner: Carleton University (Canada) - Prosenjit Bose

Start year: 2018

See also: https://members.loria.fr/Olivier.Devillers/trip/

The two teams are specialists of Delaunay triangulation with a focus on computation algorithms on the French side and routing on the Canadian side. We plan to attack several problems where the two teams are complementary: - Stretch factor of the Delaunay triangulation in 3D. - Probabilistic analysis of Theta-graphs and Yao-graphs. - Smoothed analysis of a walk in Delaunay triangulation. - Walking in/on surfaces. - Routing in non-Euclidean spaces.

9.3.1.2. Astonishing

Title: ASsociate Team On Non-ISH euclIdeaN Geometry

International Partner: University of Groningen (Netherlands) - Institute of Systems Science - Gert Vegter

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 $\mathbb{R}^d$. 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 $\mathbb{R}^d$, 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.

Jean-Lou De Carufel and Prosenjit Bose spent one week in GAMBLE in the framework of the TRIP associate team.

Martin Tancer, Vojta Kalusza and Pavel Paták, from Charles University (Prague), spent one week each in GAMBLE. They were supported by the PHC program EMBEDS II.

9.4.2. Visits to International Teams

Olivier Devillers spent two weeks at the Computational Geometry Lab of Carleton University http://cglab.ca/about.html in the framework of the TRIP associate team.

Charles Duménil spent one month at the Computational Geometry Lab of Carleton University http://cglab.ca/about.html in the framework of the TRIP associate team.

Monique Teillaud and Iordan Iordanov spent one month at Johann Bernouilli Institute for Mathematics and Computer Science of the University of Groningen in the framework of the Astonishing associate team.

GRACE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Participants: Daniel Augot, Matthieu Rambaud.

A "research initiative" "BART" (Blockchain advanced research and technologies) has been launched with three partners: Inria, Institut Mines-Télécom, and System-X. This is funded by *Institut de recherche* System-X, located in Paris-Saclay area, whose objective is to connect industry and academia. A new PhD has been started, with L. Benmouffok, hired in October 2018, whose topic is the use of secure multiparty computation in blockchains.

8.2. National Initiatives

8.2.1. ANR

Participants: Daniel Augot, Alain Couvreur, Matthieu Rambaud.

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/.

8.3. European Initiatives

8.3.1. SPARTA

- Program: H2020
- Project acronym: SPARTA
- Project title: SPARTA
- Duration: three years
- Coordinator: CEA
- Other partners: IMT, Inria, ANSSI
- Abstract: Propose, test, validate and exploit the possible organizational, technological and operational setup of a cybersecurity competence network; Produce a roadmap that include targets to be achieved by the end of the project, as well as priorities to be addressed in the future by the Cybersecurity Competence Network; Serve to align research, education and certification; Build on and align existing roadmap efforts.
  Participant: Benjamin Smith.

8.3.2. 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. 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.

These systems are all broken as soon as large quantum computers are built. 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: 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, ended in March 2018.

Participants: Daniel Augot, Matthieu Rambaud.

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.

7.1.2. ANR CLap–CLap – The p-adic Langlands correspondence: a constructive and algorithmical approach

Participant: Xavier Caruso.

The p-adic Langlands correspondence has become nowadays one of the deepest and the most stimulating research programs in number theory. It was initiated in France in the early 2000's by Breuil and aims at understanding the relationships between the p-adic representations of p-adic absolute Galois groups on the one hand and the p-adic representations of p-adic reductive groups on the other hand. Beyond the case of $\mathrm{GL}_2(\mathbb{Q}_p)$ which is now well established, the p-adic Langlands correspondence remains quite obscure and mysterious new phenomena enter the scene; for instance, on the $\mathrm{GL}_n(F)$-side one encounters a vast zoology of representations which seems extremely difficult to organize.

The CLap–CLap ANR project aims at accelerating the expansion of the p-adic Langlands program beyond the well-established case of $\mathrm{GL}_2(\mathbb{Q}_p)$. Its main originality consists in its very constructive approach mostly based on algorithmics and calculations with computers at all stages of the research process. We shall pursue three different objectives closely related to our general aim:

1. draw a conjectural picture of the (still hypothetical) p-adic Langlands correspondence in the case of GL_n,
2. compute many deformation spaces of Galois representations and make the bridge with deformation spaces of representations of reductive groups,
3. design new algorithms for computations with Hilbert and Siegel modular forms and their associated Galois representations.

This project will also be the opportunity to contribute to the development of the mathematical software SAGEMATH and to the expansion of computational methodologies.

7.2. European Initiatives

7.2.1. 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

International Laboratory for Research in Computer Science and Applied Mathematics
Associate Team involved in the International Lab:

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:

- Tony Ezome organised a Cimpa school on Courbes algébriques pour une arithmétique efficace des corps finis from 17/11/2018 - 30/11/2018 in Ziguinchor (Sénégal), Institution Université Assane Seck de Ziguinchor.
- Abdoul Asiz Ciss and Damien Robert represented the team at the Journées du Lirima. One of the suggestion was to find industrial collaborations in Africa, especially in Senegal. Ongoing work is done by the team to find such a collaboration, especially on the new challenges of post-quantum cryptography.
- Abdoulaye Maiga visited in Bordeaux to work with Damien Robert from 22/10/2018 to 18/01/2019. Tony Ezome and Mohamadou Sall visited from 08/12/2018 to 22/12/2018.

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

- Nicolas Mascot (American University of Beirut, Lebanon) visited the team for a week (8-12/01/2018).
- Alex Bartel (University of Glasgow, UK) visited the team for two weeks (27/03/2018 to 07/04/2018).
- Takashi Fukuda (Nihon University, Japan) visited the team for two months (20/01/2018 to 25/03/2018)
- Tony Ezome (Université des Sciences et Techniques de Masuku) and Mohamadou Sall (Dakar) visited the team for two weeks in December. Abdoul Aziz (Dakar) visited the team for one week in September.
- Abdoulaye Maiga visited the team for three months, from October to January 2019.

Researchers visiting the team to give a talk to the team seminar include Elie Eid (Université de Rennes), Jean-François Biasse (University of South Florida), Francesco Battistoni (University of Milan), Alex Bartel (Glasgow University), Tristan Vaccon (Université de Limoges), and Takashi Fukuda (Nihon University).

7.4.2. Visits to International Teams

A. Page visited Alex Bartel (University of Glasgow, UK) for two weeks (16-27/07/2018) and Michael Lipnowski (McGill University, Montreal, Canada) for two weeks (10-23/11/2018).

A. Page and Alex Bartel did a research stay in Oberwolfach (Allemagne) with the Research In Pairs programme for three weeks (14/10/2018-3/11/2018).

OURAGAN Team

9. Partnerships and Cooperations

9.1. European Initiatives

9.1.1. FP7 & H2020 Projects

Program:H2020-EU.1.1. - EXCELLENT SCIENCE - European Research Council (ERC)

Project acronym: Almacrypt

Project title: Algorithmic and Mathematical Cryptology

Duration: 01/2016 - 12/2010

Coordinator: Antoine Joux

Abstract: Cryptology is a foundation of information security in the digital world. Today's internet is protected by a form of cryptography based on complexity theoretic hardness assumptions. Ideally, they should be strong to ensure security and versatile to offer a wide range of functionalities and allow efficient implementations. However, these assumptions are largely untested and internet security could be built on sand. The main ambition of Almacrypt is to remedy this issue by challenging the assumptions through an advanced algorithmic analysis. In particular, this proposal questions the two pillars of public-key encryption: factoring and discrete logarithms. Recently, the PI contributed to show that in some cases, the discrete logarithm problem is considerably weaker than previously assumed. A main objective is to ponder the security of other cases of the discrete logarithm problem, including elliptic curves, and of factoring. We will study the generalization of the recent techniques and search for new algorithmic options with comparable or better efficiency. We will also study hardness assumptions based on codes and subset-sum, two candidates for post-quantum cryptography. We will consider the applicability of recent algorithmic and mathematical techniques to the resolution of the corresponding putative hard problems, refine the analysis of the algorithms and design new algorithm tools. Cryptology is not limited to the above assumptions: other hard problems have been proposed to aim at post-quantum security and/or to offer extra functionalities. Should the security of these other assumptions become critical, they would be added to Almacrypt's scope. They could also serve to demonstrate other applications of our algorithmic progress. In addition to its scientific goal, Almacrypt also aims at seeding a strengthened research community dedicated to algorithmic and mathematical cryptology.

9.2. International Initiatives

9.2.1. Inria International Labs

9.2.1.1. Informal International Partners

- CQT Singapour (UMI CNRS Majulab)
- UFPA - Para -Brésil (José Miguel Veloso)
- Institut Joseph Fourier - Université Grenoble Alpes (Martin Deraux, V. Vitse et Pierre Will)
- Max-Planck-Institut für Informatik - Saarbrücken - Germany (Michael Sagraloff)
- Holon Institute of Technology, Israel (Jeremy Kaminsky)

9.3. International Research Visitors

9.3.1. Visits of International Scientists

- Jeremy Kaminsky (Holon Institute of Technology, Israel). 3-months visitor in Ouragan and École Polytechnique (MAX) and École des Mines. Chateaubriand Fellow. Subjects: Control Theory, Algebraic Geometry and Computer Vision.

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 [0] 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 [0] project is certainly the biggest industrial project ever organized in quantum-safe cryptography. RISQ is one of few projects accepted in the call Grands DΓ©fis du NumΓ©rique 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.

[0] https://project.inria.fr/galop/
[0] http://risq.fr/

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.

- **ANR SESAME (Singularités Et Stabilité des AsservisseMEnts référencés capteurs)**

  Duration: 2018–2022

  Participants: J.-C. Faugère, M. Safey El Din.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

- **Innovative Training Network POEMA (Polynomial Optimization, Efficiency through Moments and Algebra)**

  Duration: 2019-2022.

  POEMA is a Marie Skłodowska-Curie Innovative Training Network (2019-2022).

  Its goal is to train scientists at the interplay of algebra, geometry and computer science for polynomial optimization problems and to foster scientific and technological advances, stimulating interdisciplinary and intersectoriality knowledge exchange between algebraists, geometers, computer scientists and industrial actors facing real-life optimization problems.

  Participants: J. Berthomieu, J.-C. Faugère, M. Safey El Din [contact], E. Tsigaridas.

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 Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Reine Abi Rached

Date: Apr. 2018 - Aug. 2018

Institution: Université de Versailles –St-Quentin-en-Yvelines

Supervisor: Jean-Charles Faugère, Jérémy Berthomieu

Hadrien Brochet

Date: Jun. 2018 - Aug. 2018

Institution: ENS Lyon

Supervisor: Elias Tsigaridas

Phuoc Le

Date: Apr. 2018 - Aug. 2018

Institution: Université de Versailles –St-Quentin-en-Yvelines

Supervisor: Jean-Charles Faugère, Mohab Safey El Din

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

Elias Tsigaridas was a visiting research scientist at the ICERM institute (Brown University) during the special semester on "Nonlinear Algebra" (Sep – Nov 2018).

SECRET Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR BRUTUS** ($10/14 \rightarrow 09/18$)
  Authenticated Ciphers and Resistance against Side-Channel Attacks
  ANR program: Défi Société de l'information et de la communication
  Partners: ANSSI, Inria (project-team SECRET and project-team MARELLE), Orange, University of Lille, University of Rennes, University Versailles-Saint Quentin
  160 kEuros
  The Brutus project aims at investigating the security of authenticated encryption systems. We plan to evaluate carefully the security of the most promising candidates to the CAESAR competition, by trying to attack the underlying primitives or to build security proofs of modes of operation. We target the traditional black-box setting, but also more "hostile" environments, including the hardware platforms where some side-channel information is available.
- **ANR DEREC** ($10/16 \rightarrow 09/21$)
  Relativistic cryptography
  ANR Program: jeunes chercheurs
  244 kEuros
  The goal of project DEREC is to demonstrate the feasibility of guaranteeing the security of some cryptographic protocols using the relativistic paradigm, which states that information propagation is limited by the speed of light. We plan to study some two party primitives such as bit commitment and their security against classical and quantum adversaries in this model. We then plan to the integration of those primitives into larger cryptosystems. Finally, we plan on performing a demonstration of those systems in real life conditions.
- **ANR CBCRYPT** ($10/17 \rightarrow 09/21$)
  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.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: TECHNISCHE UNIVERSITEIT EINDHOVEN

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

Nxp Semiconductors Belgium Nv (Belgium)

Ruhr-Universitaet Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

Online banking, e-commerce, telemedicine, mobile communication, and cloud computing depend fundamentally on the security of the underlying cryptographic algorithms. Public-key algorithms are particularly crucial since they provide digital signatures and establish secure communication without requiring in-person meetings. Essentially all applications today are based on RSA or on the discrete-logarithm problem in finite fields or on elliptic curves. Cryptographers optimize parameter choices and implementation details for these systems and build protocols on top of these systems; cryptanalysts fine-tune attacks and establish exact security levels for these systems. Alternative systems are far less visible in research and unheard of in practice. It might seem that having three systems offers enough variation, but these systems are all broken as soon as large quantum computers are built. The EU and governments around the world are investing heavily in building quantum computers; society needs to be prepared for the consequences, including cryptanalytic

attacks accelerated by these computers. Long-term confidential documents such as patient 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 as Enigma-encrypted messages are today. PQCRYPTO will allow users to switch to post-quantum cryptography: cryptographic systems that are not merely secure for today but that will also remain secure long-term against attacks by quantum computers. PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet of Things. PQCRYPTO will provide efficient implementations of high-security post-quantum cryptography for a broad spectrum of real-world applications.

8.2.1.2. 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.

8.2.1.3. 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.

8.2.2. Collaborations in European Programs, Except FP7 & H2020

8.2.2.1. 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)

Inria contact: Anthony Leverrier

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.

8.3. International Initiatives

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

8.3.1.1. 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, nobody has publicly produced a real pair of colliding messages so far, because the estimated attack complexity is around 2^{63} SHA-1 computations (this represents about 70000 years of computation on a normal PC).

While a collision of SHA-1 would clearly demonstrate 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, and we will use an ASIC cluster to perform such a computation.

8.3.2. Inria International Partners

8.3.2.1. 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.

8.3.2.2. Informal International Partners

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

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Thomas Peyrin, NTU Singapore, January 2018 and July 2018.
- Sristy Agrawal, Indian Institute of Science Education and Research, Kolkata, India, January 2018.
- Anastasiya Gorodilova, Sobolev Institute of Mathematics, Novosibirsk, Russia, September 2018.
- Lorenzo Grassi, IAIK, Graz University of Technology, Austria, September 2018.

8.4.1.1. Internships

- Daniel Coggia, MPRI, March-Aug. 2018
- Anaïs Querol Cruz, MPRI, March-Aug. 2018
- Florian Wartelle, UVSQ, March-Sept. 2018

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

- NTU, Singapore, joint work within the CHOCOLAT Associate Team: S. Duval (April 8-19), G. Leurent (October 29 - November 10).
- University of Sherbrooke, Sherbrooke, Canada, June 11-15, 2018 (J.P. Tillich)
- Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, September 30-October 9, 2018 (P. Charpin).

SPECFUN Project-Team

8. Partnerships and Cooperations

8.1. International Research Visitors

8.1.1. Internships

- Jiadong Han did a Master internship from March to August. Under the supervision of Pierre Lairez, he studied the computation of adaptive grid to improve the computation of the homology of semialgebraic sets.

CAIRN Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

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

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

3DCORE (3D Many-Core Architectures based on Optical Network on Chip) is a project 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 https://3d-opt-many-cores.cominlabs.u-bretagneloire.fr.

9.1.2. Labex CominLabs - RELIASIC (2014-2018)

Participant: Emmanuel Casseau.

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). 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. For more details see https://reliasic.cominlabs.u-bretagneloire.fr

9.1.3. Labex CominLabs & Lebesgue - H-A-H (2014-2018)

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/.

9.1.4. 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. 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. For more details see https://bbc.cominlabs.u-bretagneloire.fr

9.1.5. 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 https://sherpam.cominlabs.u-bretagneloire.fr

9.1.6. 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. For more details see https://flodam.fr

9.2. European Initiatives

9.2.1. H2020 ARGO

Participants: Steven Derrien, Olivier Sentieys, Mickael Dardaillon, 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 (Germany), UR1/Inria/CAIRN, Recore Systems (Netherlands), TEI-WG (Greece), Scilab Ent. (France), Absint (Ger.), DLR (Ger.), Fraunhofer (Ger.)

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.

9.2.2. ANR International ARTEFaCT

Participants: Olivier Sentieys, Van Phu Ha, 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, CAIRN, EPFL

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.

9.3. International Initiatives

9.3.1. Inria International Labs

EPFL-Inria

Associate Team involved in the International Lab:

9.3.1.1. 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. 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. 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.

9.3.2. Inria International Partners

9.3.2.1. 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

9.3.2.2. HARAMCOP

Title: Hardware accelerators modeling using constraint-based programming

International Partner (Institution - Laboratory - Researcher):

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

9.3.2.3. 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.

9.3.2.4. 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.

9.3.2.5. 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.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Martin Kumm, University of Kassel, Germany, July 2018.

Son Tran Giang, Lecturer at ICTLab, Vietnam, December 2018.

9.4.2. Visits to International Teams

E. Casseau spent 3 weeks as a visiting researcher in the Parallel and Reconfigurable Lab. of the Electrical and Computer Engineering department, the University of Auckland, New Zealand, in December 2018.

P. Dobias (Phd student) spent 5 months in the Parallel and Reconfigurable Lab. of the Electrical and Computer Engineering department, the University of Auckland, New Zealand, from November 2018 until March 2019.

CAMUS Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. Idex Prim'Eau

Participant: Jens Gustedt [contact].

In the framework of the Prim'Eau project of the University of Strasbourg, we study surface runoff for hydrological periods of several days. We use an efficient domain decomposition method that we apply to a real world example of Mutterbach (Moselle) with geological and flood data from the years 1920, 1940 and 2017. As the time and memory usage for these computations is important, we aim to parallelize them.

9.1.2. ADT ASNAP

Participants: Philippe Clauss, Jens Gustedt, Maxime Mogé.

Philippe Clauss, Jens Gustedt and Maxime Mogé have been involved until August 2018 in the ADT Inria project ASNAP (Accélération des Simulations Numériques pour l'Assistance Peropératoire), in collaboration with the Inria team MIMESIS. The goal was to find opportunities in the SOFA simulation platform for applying automatic parallelization techniques developed by Camus. We have investigated two approaches. One approach uses memory behavior memoïzation to generate a parallel code made of independent threads at runtime.

9.1.3. ADT ALTO (ApoLlo TakeOff)

Participants: Philippe Clauss, Muthena Abdul Wahab.

The Apollo compilation platform [4] that is being developed in Camus, dedicated to speculative and dynamic optimization and parallelization of loop nests, is the achievement of many original advances in compilation algorithms, in extensions of the polyhedral model, in speculative parallelization and in dynamic optimization of programs. It is a library of implemented knowledge and a fertile ground for other advances and extensions : for instance, an extension of the polyhedral model for handling non-linear loops would not have been possible without Apollo. However, this software platform must continuously be maintained, improved and extended.

The ALTO project, which is a 2.5 years project started in August 2018, is devoted to strengthen Apollo's software implementation in several ways, thanks to the expert engineer who has been recruited for these goals, Matthew Wahab. The main goals are the following:

- making the programming code respecting the standard rules of open-source software;
- making Apollo more robust regarding cases where some inputs may yield extreme behaviors
- implementing required improvements and extensions, as inter-procedural analysis or memory behavior memoïzation.

9.2. National Initiatives

9.2.1. ANR AJACS

Participant: Arthur Charguéraud.

The AJACS research project is funded by the programme "Société de l'information et de la communication" of the ANR, from October 2014, until March 2019. 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).

9.2.2. ANR Vocal

Participant: Arthur Charguéraud.

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

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

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

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. ERC Deepsea

Participant: Arthur Charguéraud.

The Deepsea project is funded by ERC from June 2013 to May 2018. It aims at developing 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) 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, Camus team), who works part time on this project. Project website: http://deepsea.inria.fr/.

9.3.2. Collaborations with Major European Organizations

Cristian Ramon-Cortes and Rosa M. Badia: Barcelona Supercomputing Center (Spain)
A Python module for automatic parallelization and distributed execution of affine loop nests

Raquel Lazcano and Eduardo Juárez Martínez: Universidad Politecnica de Madrid (Spain)
Integration of Apollo in the Cerbero dataflow framework for adaptive code generation.

9.4. International Initiatives

9.4.1. Inria International Partners

9.4.1.1. Informal International Partners

The CAMUS team maintains regular contacts with the following entities:

- Reservoir Labs, New York, NY, USA
- University of Batna, Algeria
- Ohio State University, Colombus, USA
- Louisiana State University, Baton Rouge, USA
- Colorado State University, Fort Collins, USA
- Indian Institute of Science (IIIS) Bangalore, India
- Barcelona Supercomputing Center, Barcelona, Spain

9.5. International Research Visitors

9.5.1. Visits of International Scientists

Rachid Seghir (Maître de conférences A, University of Batna, Algeria) visited our team (June 16-23, 2018), to participate to the mid-thesis evaluation of Harenome Ranaivoarivony-Razanajato, and work with Vincent Loechner on our ongoing collaboration co-advising Toufik Baroudi.

9.5.2. Internships

Toufik Baroudi is a PhD student under the supervision of Rachid Seghir at University of Batna (Algeria). He is co-advised by Vincent Loechner, and visiting our team as an intern for one year since November 2018, founded by the Algerian *Programme National Exceptionnel (PNE)*. His PhD defense is planned at the end of 2019.

CASH Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- Matthieu Moy submitted an ANR project as scientific coordinator entitled "Distributed Efficient Architecture for the Rapid (Co)simulation of Multiphysics Objects" (48 months, partners Verimag, TIMA and LIP6).
- Laure Gonnord's "Jeune Chercheur" ANR, CODAS, has started in January 2018 (42 months).

8.1.2. Scientific Advising

- Christophe Alias is scientific advisor (concours scientifique, 20%) for the XTREMLOGIC start-up.

8.2. International Initiatives

8.2.1. Informal International Partners

- Christophe Alias has regular collaborations with Sanjay Rajopadhye from Colorado State University, USA (3 publications, one publication submitted 7.1).
- Ludovic Henrio has regular collaborations with university of Linköping (one publication last year, 2 submissions); University of Oslo, University of Uppsala, and TU Darmstadt on active objects (2 publications being written); Chalmers university and Univ of Twente (one publication submitted).
- Laure Gonnord has regular collaborations with Fernando Pereira from UFMG, Brasil (5 publications in total, last in 2017). In 2018 she has began a collaboration with Tobias Grösser, from ETH Zurich.

CORSE Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. 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, Manuel Selva
- 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 and the PostDoc of Manuel Selva are funded by this project.

9.2. National Initiatives

9.2.1. 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 March 2018
- 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 run-time 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.

9.2.2. 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.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. 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 Francois Méhaut

CORSE participants: Jean Francois 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 Francois 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).

9.3.1.2. 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 Francois Méhaut

CORSE participants: François Broquedis, Jean Francois 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.

9.3.2. 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.

9.4. International Initiatives

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

9.4.1.1. IOComplexity

Title: Automatic characterization of data movement complexity

International Partner (Institution - Laboratory - Researcher):

Ohio State University (United States) - Computer Science and Artificial Intelligence Laboratory - P. Sadayappan

Start year: 2018

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

The goal of this project is to extend techniques for automatic characterisation of data movement of an application to the design of performance estimation.

The EA as three main objectives: 1. broader applicability of IO complexity analysis; 2. Hardware characterisation; 3. Performance model.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- Mohamad Jaber visited the Inria Corse team in January 2018.

9.5.2. Visits to International Teams

9.5.2.1. Sabbatical programme

- Fabrice Rastello was on sabbatical at Colorado State University (USA) from July 2017 till July 2018.
- Yliès Falcone visited American University of Beirut (Lebanon) in May 2018 through an Erasmus exchange programme.

9.5.2.2. Research Stays Abroad

- Fabian Gruber visited the Colorado State University to work with Louis-Noël Pouchet from 18.03.2018 to 17.04.2018.
- Fabian Gruber visited the Ohio State University to work with P. Sadayappan , Changwan Hong, and Aravind Sukumaran-Rajam from 18.11.2018 to 01.12.2018.

PACAP Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

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

9.2. National Initiatives

9.2.1. Capacités: Projet "Investissement d'Avenir" (1/11/14 – 31/01/2018)

Participants: Damien Hardy, Viet Anh Nguyen, Isabelle Puaut.

The project objective is to develop a hardware and software platform based on manycore architectures, and to demonstrate the relevance of these manycore architectures (and more specifically the Kalray manycore) for several industrial applications. The Kalray MPPA manycore architecture is currently the only one able to meet the needs of embedded systems simultaneously requiring high performance, lower power consumption, and the ability to meet the requirements of critical systems (low latency I/O, deterministic processing times, and dependability).

The project partners are Kalray (lead), Airbus, Open-Wide, Safran Sagem, IS2T, Real Time at Work, Dassault Aviation, Eurocopter, MBDA, ProbaYes, IRIT, Onera, Verimag, Inria, IRISA, Tima and Armines.

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

Participants: Erven Rohou, Bahram Yarahmadi.

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 computing 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 [42]. The main application target is Internet of Things (IoT).

9.2.3. ANR Continuum (2015–2019)

Participants: Rabab Bouziane, Erven Rohou.

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

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

9.2.4. Hybrid SIMD architectures (2018–2019)

Participants: Sylvain Collange, Alexandre Kouyoumdjian, Erven Rohou.

The project objective is to define new parallel computer architectures that offer high parallel performance on high-regularity workloads while keeping the flexibility to run more irregular parallel workloads. inspired by both GPU and SIMD or vector architectures.

This project is funded by the French Ministry of Armed Forces (*Ministère des Armées*).

9.2.5. DGA/PEC ARMOUR (2018–2021)

Participants: Kévin Le Bon, Erven Rohou.

ARMOUR (dynAmic binaRy optiMizatiOn cyber-secURity) aims at improving the security of computing systems at the software level. Our contribution will be twofold: (1) identify vulnerabilities in existing software, and (2) develop adaptive countermeasure mechanisms against attacks. We will rely on dynamic binary rewriting (DBR) which consists in observing a program and modifying its binary representation in memory while it runs. DBR does not require the source code of the programs it manipulates, making it convenient for commercial and legacy applications. We will study the feasibility of an adaptive security agent that monitors target applications and deploys (or removes) countermeasures based on dynamic conditions. Lightweight monitoring is appropriate when the threat condition is low, heavy countermeasures will be dynamically woven into the code when an attack is detected. Vulnerability analysis will be based on advanced fuzzing. DBR makes it possible to monitor and modify deeply embedded variables, inaccessible to traditional monitoring systems, and also to detect unexpected/suspicious values taken by variables and act before the application crashes.

ARMOUR is funded by DGA (*Direction Générale de l'Armement*) and PEC (*Pôle d'Excellence Cyber*).

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. ANTAREX

Participants: Loïc Besnard, Imane Lasri, Erven Rohou.

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

Program: H2020

Duration: September 2015 – November 2018

Coordinator: Politecnico di Milano, Italy (POLIMI)

Partners:

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

Inria contact: Erven Rohou

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

9.3.1.2. ARGO

Participants: Imen Fassi, Damien Hardy, Isabelle Puaut.

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

Program: H2020

Type: RIA

Duration: Jan 2016 – Mar 2019

Coordinator: Karlsruhe Institut für Technologie (Germany)

Université de Rennes 1 contact: Steven Derrien

Partners:

Karlsruher Institut für Technologie (Germany)

SCILAB enterprises SAS (France)

Université de Rennes 1 (France)

Technologiko Ekpaideftiko Idryma (TEI) Dytikis Elladas (Greece)

Absint GmbH (Germany)

Deutsches Zentrum für Luft- und Raumfahrt EV (Germany)

Fraunhofer (Germany)

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.

9.3.1.3. HiPEAC4 NoE

Participants: Pierre Michaud, Erven Rohou, André Seznec.

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

HiPEAC4 addresses the design and implementation of high-performance commodity computing devices in the 10+ year horizon, covering both the processor design, the optimizing compiler infrastructure, and the evaluation of upcoming applications made possible by the increased computing power of future devices.

9.3.1.4. Eurolab-4-HPC

Participant: Erven Rohou.

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

Program: H2020

Duration: September 2018 – September 2020

Coordinator: Chalmers Tekniska Hoegskola AB (Sweden)

Partners:

Barcelona Supercomputing Center - Centro Nacional de Supercomputacion (Spain)

Chalmers Tekniska Hoegskola (Sweden)

Foundation for Research and Technology Hellas (Greece)

Universität Stuttgart (Germany)

The University of Manchester (United Kingdom)

Inria (France)

Universität Augsburg (Germany)

ETH Zürich (Switzerland)

École Polytechnique Federale de Lausanne (Switzerland)

Technion - Israel Institute of Technology (Israel)

The University of Edinburgh (United Kingdom)

Rheinisch-Westfaelische Technische Hochschule Aachen (Germany)

Universiteit Gent (Belgium)

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 long-term challenges for HPC. These typically cut across layers, e.g., performance, energy efficiency and dependability, so excellence in research must target all the layers in the system stack. The EuroLab-4-HPC project's bold overall goal is to build connected and sustainable leadership in high-performance computing systems by bringing together the different and leading performance oriented communities in Europe, working across all layers of the system stack and, at the same time, fueling new industries in HPC.

9.4. International Initiatives

9.4.1. ANR CHIST-ERA SECODE 2016–2018

Participants: Damien Hardy, Nicolas Kiss, Erven Rohou.

Title: SECODE – Secure Codes to Thwart Cyber-Physical Attacks

CHIST-ERA - RTCPS

Duration: January 2016 – December 2018

Coordinator: Télécom Paris Tech (France)

Partners:

Télécom Paris Tech (France)

Inria (France)

Université Paris 8 (France)

Sabancı Üniversitesi (Turkey)

Université Catholique de Louvain (Belgium)

Inria contact: 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.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

9.5.1.1. Internships

Caio de Lima and Marcos Siraichi, both from Universidade Federal de Minas Gerais (Brazil), visited PACAP for internships:

- Caio de Lima: Jan 9 – Apr 5;
- Marcos Siraichi: Dec 15 2017 – Mar 3 and Jul 16 – Oct 13.

9.5.2. Visits to International Teams

André Seznec visited Intel Microprocessor Research Labs at Bangalore (India) from 24th to 28th of September.

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, Cristian Maxim, 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: Liliana Cucu, Adriana Gogonel, Yves Sorel, Walid Talaboulma.

This FUI funded project was started on September 2015 and it is preparing its final conclusions for the beginning of 2019. It has targeted the creation of the framework Time4Sys within the PolarSys project [12]. This open source framework allows timing analyses from models to simulation for different application domains like avionics, railways, medical, aerospace, automotive, etc. and it is available at https://www.polarsys.org/time4sys.

9.1.2. PIA

9.1.2.1. ES3CAP

Participants: Keryan Didier, Dumitru Potop Butucaru.

The objectives of the ES3CAP (Embedded Smart Safe Secure Computing Autonomous Platform) project are to:

- Build a hardware and software industry-grade solution for the development of computation-intensive critical application. The solution should cover the needs of industrial end users, and target multi/many-core hardware platforms. The solution with come with 3 to 6 usage profiles specific to various industries (automotive, aerospace, defence).
- Improve the technology readiness level of the proposed development flow from TRL4-5 (technology development) to TRL6-7, thus approaching as much as possible commercialization.
- Build an alternate, perennial ecosystem for critical real-time OSs and development tools, for computer vision, data fusion and neural networks. The tools and components must be available on a prototyping and demonstration platform that is safe and secure.
- Capitalize on the convergence between the automotive and aerospace markets on subjects such as security, safety, decision making, and big data.

9.1.2.2. DEPARTS

Participants: Liliana Cucu, Adriana Gogonel, Walid Talaboulma.

This BGLE funded project of the national support programme Investissements d'Avenir has started on October 1st, 2012 and provided its final conclusions on December 2018. Inria has provided a final prototype version of the EVT Kopernic tool taking into account homogenous variation factors for the execution times. Swapping algorithms allowing WCET decrease are currently finalized within the PhD thesis of Walid Talaboulma with a defense expected during the spring of 2019.

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 several publications.

HYCOMES Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Participant: Benoît Caillaud.

Benoît Caillaud is contributing to the 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 [27]. 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 2018, Benoît Caillaud and Aurélien Lamercerie (SemLIS team of IRISA) have maintained and enhanced the Demodocos prototype software. This software is synthesizing surgical process models (expressed in the ♯Seven language developed in the Hybrid team, Inria Rennes) from instances of surgical procedures. These models can be executed in a virtual reality environment developed by the Hybrid team.

8.2. National Initiatives

8.2.1. 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 Bernard Brogliato Alexandre Rocca	Tripop	Inria Grenoble Rhône Alpes
Albert Benveniste Benoît Caillaud Khalil Ghorbal Christelle Kozaily Mathias Malandain Benoît Vernay	Hycomes	Inria Rennes Bretagne Atlantique
Marc Pouzet Tim Bourke Imsail Lakhim-Bennani	Parkas	ENS & Inria Paris
Goran Frehse	SSH	ENSTA Paris-Tech.
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).

[0] https://s3pm.cominlabs.u-bretagneloire.fr/fr

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.

In 2018, three general meetings have been organized, with presentations of the partners on new results related to hybrid systems modeling and verification. A two days workshop open to a larger community of researchers and engineers has been organized, with a focus on model-based system diagnosis [0]. The programme of the workshop comprized invited talks by Erik Frisk and Mattias Krysander on the use of DAE Structural Analysis methods to generated automatically embedded diagnosers from a system model.

Two PhDs funded by the ModeliScale IPL have started in October 2018:

- Christelle Kozaily has started a PhD, under the supervision of Vincent Acary (TRIPOP team at Inria Grenoble), Benoît Caillaud, Khalil Ghorbal on the structural and numerical analysis of non-smooth DAE systems. She is located in the Hycomes team at Inria Rennes.
- Ismail Lahkim-Bennani has started a PhD under the supervision of Goran Frehse (ENSTA Paris-Tech.) and Marc Pouzet (PARKAS team, Inria/ENS Paris). His PhD topic is on random testing of hybrid systems, using techniques inspired by QuickCheck [33].

8.2.2. FUI ModeliScale: Scalable Modeling and Simulation of Large Cyber-Physical Systems

Participants: Albert Benveniste, Benoît Caillaud, Khalil Ghorbal, Mathias Malandain.

FUI ModeliScale is a French national collaborative project coordinated by Dassault Systèmes. The partners of this project are: EDF and Engie as main industrial users; DPS, Eurobios and PhiMeca are SME providing mathematical modeling expertise; CEA INES (Chambéry) and Inria are the academic partners. The project started January 2018, for a maximal duration of 42 months. Three Inria teams are contributing to the project : Hycomes, Parkas (Inria Paris / ENS) and Tripop (Inria Grenoble / LJK).

The focus of the project is on the scalable analysis, compilation and simulation of large Modelica models. One of the main contributions expected from Inria are:

- A novel structural analysis algorithms for multimode DAE systems, capable of handling large systems of guarded equations, that do not depend on the enumeration of a possibly exponential number of modes.
- The partitioning and high-performance distributed co-simulation of large Modelica models, based on the results of the structural analysis.

In 2018, two reports have been delivered: the first one is a state of the art on structural analysis methods for DAE systems [0], while the second details a structural analysis algorithm for multimode DAE systems [0]. It is an improvement of the algorithm presented in [16].

8.3. International Initiatives

8.3.1. Informal International Partners

The Hycomes team has a continued collaboration with Martin Otter (DLR, Munich, Germany) and Hilding Elmqvist (Mogram AB, Lund, Sweden), on the structural analysis and compilation of the Modelica language [17]. The team is also establishing a collaboration with John Pryce from the University of Cardiff (UK), on the structural analysis of DAE systems.

[0] https://team.inria.fr/modeliscale/workshop-on-diagnostics-25-26-january-2018/
[0] Modeliscale project, deliverable M2.1.1 1, Structural Analysis of Differential-Algebraic Equations (DAE), State-of-the-Art.
[0] Modeliscale project, deliverable M2.1.2 1, Algorithms for the structural Analysis of Multi-Mode DAE Systems.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Prof. Jean-Baptiste Jeannin, from the University of Michigan (Ann Arbor, Mi, USA) has visited the Hycomes team at the beginning of Summer 2018. He has collaborated with Kahlil Ghorbal and Benoît Caillaud on the topics cyber-physical systems modeling and contract-based reasoning.

KAIROS Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. Université Côte d'Azur Academy 1

In the context of the UCA Jedi IDEX, associated with the UCA ComUE, we have applied to a number of funding initiatives. The project Smart IoT for Mobility has been funded for three years by the Academy RISE. This project is lead by the LEAT and Kairos is building a formal language for the design of smart contracts in the context of a mobility project with Renault Software Labs. The smart contracts are persisted in a secured distributed ledgers (through blockchain technology). The SyMag company, a subsidiary of BNP Paribas, is providing the technology to access block chain with a ledger-agnostic API. A PhD (at LEAT) and a Post-doc (within Kairos) positions are funded by this project. A complementary funding has been asked to the ANR with the generic call 2019.

9.2. National Initiatives

9.2.1. Investissements d'Avenir: PIA Clarity

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

This project was funded by the LEOC Call (*Logiciel Embarqué et Objets Connectés*) of the national support programme *Investissements d'Avenir*. It ended in January 2018. Partners were: 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.

9.2.2. CNRS GDRs

We are registered members of three GDR funded by CNRS : SoC^2, on topics of Hardware-software codesign and Non-Functional Property modeling for co-simulation; LTP, on verification and language design for reactive CPS systems; GPL,con Programming and Software Engineering (LaHMA group), LTP, Langages, Types et Preuves.

9.3. International Initiatives

9.3.1. Inria International Labs

The SACCADES LIAMA project came to a conclusion with the ending of the related Associated Team with ECNU Shanghai. We are actively working on a renewal of this colaboration, integrating the new generation of Professors there.

9.3.2. Inria International Partners

9.3.2.1. Declared Inria International Partners

- Luigi Liquori has a steady collaboration with researchers from University of Udine, and Turin, Italy.
- We collaborate with the University of Verona on topics of CPS co-simulation. This partly funds a support engineer on their side.
- M.A Peraldi-Frati participates in an international cooperation between University Côte d'Azur, University of Danang (Vietnam) and AUF. This collaboration crystallized through the DNIIT excellence initiative between Univ of Danang and UCA. M.A Peraldi-Frati is involved in the SLEGO project (Specific domain Language for Experience Global Orchestration)[22].

9.3.2.2. TuMuLT

Title: Trustworthy Modeling using Logical Time

International Partner (Institution - Laboratory - Researcher):

ECNU (China) - Software Engineering Institute - Min Zhang

Duration: 2018 - 2022

Start year: 2018

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

We have four main research directions:

- Modeling the Uncertain Environments of Cyber-Physical Systems (CPS): Logical Time was one of the main scientific foundations of the AOSTE Team. From the background in theory of concurrency, we are used to consider mainly discrete control systems that can guarantee a functional determinism independently of any implementation-specific timing variation. Addressing CPS means widening those assumptions to consider the external environment as part of the design. The environment obeys the law of physics that usually depend on physical time consideration with models that are approximation of the reality and that necessarily introduce a wide uncertainty on the behavior. This task explores the definition of sound extensions to logical time to capture both the physical continuous behavior and make an abstract characterization as a statistical approximation [25].
- SMT For Logical Time: While synchronous systems usually focus on finite state-based control systems, our abstraction of logical time relies on both Boolean algebra (for synchronous operations) and integer arithmetic, Solving a system of logical-time constraints is NP-complete but we strive to find efficient algorithms to solve sub-classes of well defined systems. In that context, SMT is a promising solution to combine and solve systems that combine several theories. We had first results on this aspect [8] but we still need to increase the subset of constraints that can be addressed efficiently as well as the performances of the solving tools.
- Spatio-Temporal Specification for Trustworthy Intelligent Transportation Systems: Focusing on Intelligent Transportation Systems as a subset of Cyber-Physical Systems, we encounter specific problems. In addition to the temporal factor omni-present in real-time and embedded systems, a physical location plays also a central role. Functions of the system (like a train) must be done both at the right time AND at the right location. This task focuses on extensions of our framework for a spatio-temporal logics based on logical time. This means a description of the location of infrastructures as well as the ability to build constraints that depend both on time (logic or physical) and locations (logical or physical).
- Open pNets: Methods for analyzing and guaranteeing the properties of critical and complex systems, including their data and time depend aspects, have strongly evolved with the emergence of efficient satisfiability checking engines (SAT and SMT). We are working on novel methods combining classical verification paradigms (state-space construction and minimization, model-checking) with SMT approaches to create symbolic and compositional verification methods and tool platforms. We have interesting preliminary results [26], and collaborate actively on both fundamental results and prototype development.

9.3.3. Participation in Other International Programs

- PHC Xu Quangqi funded by ANR for International collaborations with China in 2008.
  - PI: Frédéric Mallet (France) and Zhang Min (China)
  - Title: SMT FOR LOGICAL TIME
  - Description: The main goal of the project was to build an efficient encoding of logical time in SMT solvers. This goal has been achieved (see New Result in Section 7.1).

9.4. International Research Visitors

- Xue-Yang ZHU, assistant research professor at Institute of Software, Chinese Academy of Science, Beijing.
- Zhang Min, Assistant Professor, ECNU Shanghai, 2 weeks in August 2018,
- Changbo Wang, Professor, Dean of Computer Science Department, ECNU Shanghai, 2 weeks in August 2018.

9.4.1. Internships

Zechen HOU benefited from an Inria International Internship Grant.

9.4.2. Visits to International Teams

9.4.2.1. Explorer programme

Julien Deantoni has spent one week visiting the Modelling, Simulation and Design Lab (MSDL) in Antwerp, funded by the MPM4CPS European cost action.

9.4.2.2. Research Stays Abroad

Eric Madelaine has spent 1 month visiting the Software engineering and computer Science department at ECNU Shanghai (2 weeks in May, 2 week in October).

PARKAS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

The Inria Project Lab (IPL) *Modeliscale* treats the modelling and analysis of Cyber-Physical Systems at large scale. The PARKAS team contributes their expertise in programming language design for reactive and hybrid systems to this multi-team effort.

8.1.1. ANR

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

8.1.2. FUI: Fonds unique interministériel

Modeliscale contract (AAP-24). Using Modelica at scale to model and simulate very large Cyber-Physical Systems. Principal industrial partner: Dassault-Systèmes. 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. H2020 Projects

Program: H2020 “Smart Anything Everywhere (SAE)” initiative

Project acronym: TETRAMAX

Project title: Technology Transfer via Multinational Application Experiments

Duration: September 2017 – August 2021

Coordinator: Rainer Leupers

Other partners: Rheinisch-Westfaelische Technische Hochschule Aachen, RWTH (Germany); AMG Technology Ood, AMGT (Bulgaria); Ruhr-Universitaet Bochum, RUB (Germany); Budapesti Muszaki Es Gazdasagtudomanyi Egyetem, BME (Hungary); Universitat Politecnica De Catalunya, UPC (Spain); Control Data Systems Srl, CDS (Romania); Chalmers Tekniska Hoegskola Ab, CHALMERS, (Sweden); Technische Universiteit Delft, TuDelft (Netherlands); The University Of Edinburgh, UEDIN, (United Kingdom); Fundingbox Accelerator Sp z o.o., FBOX, (Poland); Universiteit Gent, UGENT (Belgium); Vysoka Skola Banska -Technicka Univerzita Ostrava, IT4I, (Czech Republic); Institut Jozef Stefan, JSI, Slovenia, Techmo Spolka z o.o., TECHMO (Poland); Universita Di Pisa, PISA (Italy); Tallinna Tehnikaulikool, TTU (Estonia); Tty-Saatio,TUT (Finland); Think Silicon Ereyna Kai Technologia Anonymi, Etairia, THINKS (Greece); Technische Universitaet Muenchen, TUM (Germany); Sveuciliste U Zagrebu Fakultet Elektrotehnike I Racunarstva, UZAGREB, (Croatia); Zentrum Fur Innovation Und Technik In Nordrhein-Westfalen GmbH, ZENIT (Germany).

Abstract: The overall ambition of TETRAMAX is building and leveraging a European Competence Center Network in customized low-energy computing, providing easy access for SMEs and mid-caps to novel CLEC technologies via local contact points. This is a bidirectional interaction: SMEs can demand CLEC technologies and solutions via the network, and vice versa academic research institutions can actively and effectively offer their new technologies to European industries. Furthermore, TETRAMAX wants to support 50+ industry clients and 3rd parties with innovative technologies, using different kinds of Technology Transfer Experiments (TTX) to accelerate innovation within European industries and to create a competitive advantage in the global economy.

8.2.2. Collaborations in European Programs, Except FP7 & H2020

Program: ITEA3
Project acronym: 14014 ASSUME
Project title: Affordable Safe & Secure Mobility Evolution
Duration: September 2015 – December 2018
Coordinator: Dumitru Potop Butucaru
Other partners: *France:* Airbus, École Normale Supérieure (ENS), Esterel Technologies, Kalray SA, Safran Aircraft Engines SAS SNECMA, Safran Electronics & Defense Sagem, Sorbonne Université, Thales; *Germany:* AbsInt Angewandte Informatik GmbH, Assystem Germany GmbH, BTC Embedded Systems AG, Daimler AG, FZI Forschungszentrum Informatik, Karlsruhe Institute of Technology (KIT), Kiel University, Model Engineering Solutions GmbH, OFFIS, Robert Bosch GmbH, Technical University of Munich; *Netherlands:* Eindhoven University of Technology, NXP Semiconductors Netherlands BV, Recore Systems BV, TNO, University of Twente, VDL Enabling Transport Solutions, Verum Software Tools BV; *Sweden:* Arcticus Systems AB, FindOut Technologies AB, KTH (Royal Institute of Technology), Mälardalen University, Scania; *Turkey:* Arçelik, Ericsson Ar-Ge, Ford Otosan, Havelsan, KoçSistem, UNIT Information Technologies R&D Ltd.
Abstract: Future mobility solutions will increasingly rely on smart components that continuously monitor the environment and assume more and more responsibility for a convenient, safe and reliable operation. Currently the single most important roadblock for this market is the ability to come up with an affordable, safe multi-core development methodology that allows industry to deliver trustworthy new functions at competitive prices. ASSUME will provide a seamless engineering methodology, which addresses this roadblock on the constructive and analytic side.

8.3. 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).

8.3.2.1. Indo-French Center of Applied Mathematics

POLYFLOW

Title: Polyhedral Compilation for Data-Flow Programming Languages

International Partner (Institution - Laboratory - Researcher):

IISc Bangalore (India) - Uday Kumar Reddy Bondhugula

Duration: 2016 - 2018

Start year: 2016

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.

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, Maxime Lesourd, Xavier Nicollin, Stephan Plassart, Sophie Quinton, Jean-Bernard Stefani, Martin Vassor.

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 LIG and VERIMAG laboratories who are reknowned specialists in these fields. The project started in November 2016 and will last three years.

8.2. National Initiatives

8.2.1. ANR

8.2.1.1. RT-Proofs

Participants: Pascal Fradet, Xiaojie Guo, Maxime Lesourd, Sophie Quinton.

RT-Proofs is an ANR/DFG project between Inria, MPI-SWS, Onera, TU Braunschweig and Verimag, running from 2018 until 2020.

The overall objective of the RT-Proofs project is to lay the foundations for computer-assisted formal verification of timing analysis results. More precisely, the goal is to provide:

1. a strong formal basis for schedulability, blocking, and response-time analysis supported by the Coq proof assistant, that is as generic, robust, and modular as possible;
2. correctness proofs for new and well-established generalized response-time analysis results, and a better, precise understanding of the role played by key assumptions and formal connections between competing analysis techniques;
3. an approach for the generation of proof certificates so that analysis results – in contrast to analysis tools – can be certified.

8.2.1.2. DCore

Participants: Gregor Goessler, Jean-Bernard Stefani.

DCORE is an ANR project between Inria project teams ANTIQUE, FOCUS and SPADES, and the IRIF lab, running from 2019 to 2023.

The overall objective of the project is to develop a semantically well-founded, novel form of concurrent debugging, which we call *causal debugging*, that aims to alleviate the deficiencies of current debugging techniques for large concurrent software systems. The causal debugging technology developed by DCORE will comprise and integrate two main novel engines:

1. *a reversible execution engine* that allows programmers to backtrack and replay a concurrent or distributed program execution, in a way that is both precise and efficient (only the exact threads involved by a return to a target anterior or posterior program state are impacted);
2. a *causal analysis engine* that allows programmers to analyze concurrent executions, by asking questions of the form "what caused the violation of this program property?", and that allows for the precise and efficient investigation of past and potential program executions.

8.2.2. Institute of Technology (IRT)

8.2.2.1. CAPHCA

Participants: Alain Girault, Nicolas Hili.

CAPHCA is a project within the Antoine de Saint Exupéry IRT. The general objective of the project is to provide methods and tools to achieve performance and determinism on modern, high-performance, multi-core and FPGA-enabled SOCs. Our specific contribution lies withing work pakacges dedicated to the design of novel PRET architectures and programming languages (see Section 6.2.1).

8.3. European Initiatives

8.3.1. Collaborations in European Programs, Except FP7 & H2020

Program: Celtic-Plus
Project acronym: SENDATE
Project title: Secure Networking for a Data center cloud in Europe
Duration: April 2016 - March 2019
Coordinator: Nokia France
Other partners: Nokia, Orange, IMT, Inria
Abstract: The SENDATE project aims to develop a clean-slate architecture for converged telecommunications networks and distributed data centers supporting 5G cellular networks and the needs from the Industrial Internet and the Internet of Things. It aims to provide scientific and technical solutions for intra and inter data centrers security, control, management and orchestration, placement and management of virtual network functions, as well as high-speed transport networks for data centers access and interconnection.

8.3.2. 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 Research Visitors

8.4.1. Visits of International Scientists

- Ismail Assayad (from U. Casablanca, Morocco) visited the team for one month in September 2018, to work on a two layer adaptive scheduling method.

TEA Project-Team

9. Partnerships and Cooperations

9.1. International Initiatives

9.1.1. Inria International Labs

Sino-European Laboratory in Computer Science, Automation and Applied Mathematics
Associate Team involved in the International Lab:

9.1.1.1. CONVEX

Title: Compositional Verification of Cyber-Physical Systems

International Partner (Institution - Laboratory - Researcher):

CAS (China) - State Key Laboratory of Computer Science - Naijun Zhan

Start year: 2018

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

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.

Inria@SiliconValley
Associate Team involved in the International Lab:

9.1.1.2. Composite

Title: Compositional System Integration

International Partners (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. International Research Visitors

9.2.1. Visits of International Scientists

Deian Stefan, Shravan Narayan (CSD) visited TEA in September for a week. Jonathan Protzenko (MSR Redmond) joined the meeting for a couple of days and gave a seminar at http://68nqrt.irisa.fr. Rajesh Gupta visited TEA for a month in August-September.

Lingtai Wang, ISCAS, visited TEA for a week in November.

9.2.2. Visits to International Teams

Jean-Joseph Marty visited UC San Diego in June for two weeks.

Jean-Pierre Talpin visited ISCAS, BUAA and Nankai in April, June and October, for a total period of two months, thanks to funding provided by the Chinese partners in the context of associate-project Convex.

Simon Lunel visited ISCAS for a week in December.

ANTIQUE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. AnaStaSec

Title: Static Analysis for Security Properties

Type: ANR générique 2014

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: January 2015 - December 2018

Coordinator: Inria Paris-Rocquencourt (France)

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

Inria contact: Jérôme Feret

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

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

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

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

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

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

7.1.2. 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.

7.1.3. SAFTA

Title: SAFTA Static Analysis for Fault-Tolerant distributed Algorithms.

Type: ANR JCJC 2018

Duration: February 2018 - February 2022

Coordinator: Cezara Drăgoi, CR Inria

Abstract: Fault-tolerant distributed data structures are at the core distributed systems. Due to the multiple sources of non-determinism, their development is challenging. The project aims to increase the confidence we have in distributed implementations of data structures. We think that the difficulty does not only come from the algorithms but from the way we think about distributed systems. In this project we investigate partially synchronous communication-closed round based programming abstractions that reduce the number of interleavings, simplifying the reasoning about distributed systems and their proof arguments. We use partial synchrony to define reduction theorems from asynchronous semantics to partially synchronous ones, enabling the transfer of proofs from the synchronous world to the asynchronous one. Moreover, we define a domain specific language, that allows the programmer to focus on the algorithm task, it compiles into efficient asynchronous code, and it is equipped with automated verification engines.

7.1.4. TGFSYSBIO

Title: Microenvironment 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: Jérôme 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.

7.1.5. VeriAMOS

Title: Verification of Abstract Machines for Operating Systems

Type: ANR générique 2018

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: January 2019 - December 2022

Coordinator: Inria Paris (France)

Others partners: LIP6 (France), IRISA (France), UGA (France)

Inria contact: Xavier Rival

Abstract: Operating System (OS) programming is notoriously difficult and error prone. Moreover, OS bugs can have a serious impact on the functioning of computer systems. Yet, the verification of OSes is still mostly an open problem, and has only been done using user-assisted approaches that require a huge amount of human intervention. The VeriAMOS proposal relies on a novel approach to automatically and fully verifying OS services, that combines Domain Specific Languages (DSLs) and automatic static analysis. In this approach, DSLs provide language abstraction and let users express complex policies in high-level simple code. This code is later compiled into low level C code, to be executed on an abstract machine. Last, the automatic static analysis verifies structural and robustness properties on the abstract machine and generated code. We will apply this approach to the automatic, full verification of input/output schedulers for modern supports like SSDs.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Type: IDEAS

Defi:

Instrument: ERC Proof of Concept Grant 2018

Objectif: Static Analysis for the VErification of Spreadsheets

Duration: January 2019 - June 2020

Coordinator: Inria (France)

Partner: None

Inria contact: Xavier Rival

Abstract: Spreadsheet applications (such as Microsoft Excel + VBA) are heavily used in a wide range of application domains including engineering, finance, management, statistics and health. However, they do not ensure robustness properties, thus spreadsheet errors are common and potentially costly. According to estimates, the annual cost of spreadsheet errors is around 7 billion dollars. For instance, in 2013, a series of spreadsheet errors at JPMorgan incurred 6 billion dollars trading losses. Yet, expert reports estimate about 90 % of the spreadsheets contain errors. The MemCAD ERC StG project opened the way to novel formal analysis techniques for spreadsheet applications. We propose to leverage these results into a toolbox able to safely *verify*, *optimize* and *maintain* spreadsheets, so as to reduce the likelihood of spreadsheet disasters. This toolbox will be commercialized by the startup MATRIXLEAD.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

7.3.1.1. Internships

Jérôme Feret has supervised the M1 Internship of Aurélie Faure de Pebeyre (AIV Master) and the M2 Internship of Albin Salazar (AIV Master).

Xavier Rival is supervising M1 Internships of Guillaume Reboullet and of Luc Chabassier (M1 at DIENS).

Vincent Danos supervised interns Raja Ben Ali and Jaime Aujaud (L2 Epitech).

CELTIQUE Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. 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.

6.1.2. 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.

6.1.3. The ANR AJACS project

Participants: 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 March 2019.

6.1.4. The ANR DISCOVER project

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

The DISCOVER project project (2014–09/2019) 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.

6.1.5. The ANR CISC project

Participants: Frédéric Besson, Thomas Jensen, Alan Schmitt.

The goal of the CISC project is to investigate multitier languages and compilers to build secure IoT applications with private communication. In particular, we aim at extending multitier platforms by a new orchestration language that we call Hiphop.js to synchronize internal and external activities of IoT applications as a whole. Our goal is to define language, semantics, attacker models, and policies for the IoT and investigate automatic implementation of privacy and security policies by multitier compilation of IoT applications. To guarantee such applications are correct, and in particular that the required security and privacy properties are achieved, we propose to certify them using the Coq proof assistant. We plan to implement the CISC results as extensions of the multitier language Hop.js (developed at Inria), based on the JavaScript language to maximize its impact. Using the new platform, we will carry out experimental studies on IoT security.

The project partners include the following Inria teams: Celtique, Collège de France, Indes, and Privatics. The project runs from April 2018 to March 2022.

6.2. European Initiatives

6.2.1. FP7 & H2020 Projects

6.2.1.1. The ERC VESTA project

Participants: David Pichardie, Sandrine Blazy, Nicolas Barré, Stefania Dumbrava, Jean-Christophe Léchenet, Rémi Hutin.

The VESTA project aims at proposing guidance and tool-support to the designers of static analysis, in order to build advanced but reliable static analysis tools. We focus on analyzing low-level softwares written in C, leveraging on the CompCert verified compiler. Verasco is a verified static analyser that analyses C programs and follows many of the advanced abstract interpretation technique developped for Astrée. The outcome of the VESTA project will be a platform that help designing other verified advanced abstract interpreters like Verasco, without starting from a white page. We will apply this technique to develop security analyses for C programs. The platform will be open-source and will help the adoption of abstract interpretation techniques.

This a consolidator ERC awarded to David Pichardie for 5 year. The project started in september 2018.

6.2.2. 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.

6.3. International Initiatives

6.3.1. Inria International Partners

6.3.1.1. 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:

- Xavier Etchevers (Orange Labs, Meylan),
- Fabrice Kordon and Lom Messan Hillah (LIP6, Paris),
- Eric Jenn and Viet Anh Nguyen (IRT Saint-Exupéry, Toulouse),
- Ioannis Parissis and Oum-El-Kheir Aktouf (LCIS, Valence),
- 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.

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.

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

8.4.2. Other International Collaborations

In 2018, we had scientific relations with several universities and institutes abroad, including:

- University of Málaga, Spain (Francisco Durán),
- University of Cali, Colombia (Camilo Rocha),
- University of Zaragoza, Spain (José Ignacio Requeno),
- ISTI/CNR, Pisa, Italy (Franco Mazzanti),
- RWTH Aachen, Germany (Joost-Pieter Katoen),
- Saarland University, Germany (Holger Hermanns),
- Eindhoven University of Technology, The Netherlands (Anton Wijs and Sander de Putter).

8.5. International Research Visitors

8.5.1. Visits of International Scientists

- H. Garavel is an invited professor at Saarland University (Germany) as a holder of the Gay-Lussac Humboldt Prize.
- Josip Bozic, Birgit Hofer, Hermann Felbinger, and Franz Wotawa (TU Graz, Austria) visited us from March 5 to March 9, 2018 in the framework of the RIDINGS PHC project (see § 8.3.1).
- G. Salaün visited the University of Málaga (Spain) from May 30 to June 13 and from December 16 to December 22, 2018.
- L. Marsso and R. Mateescu visited TU Graz (Austria) from August 20 to August 24, 2018 in the framework of the PHC RIDINGS project.

The annual CONVECS seminar was held in Dullin (France) on July 10–12, 2018. The following invited scientists attended the seminar:

- Eric Jenn (IRT Saint-Exupéry / Thales Avionics) gave on July 10, 2018 a talk entitled "*The CAPHCA Project, or How to Be Fast and Reasonable*".
- Viet Anh Nguyen (IRT Saint-Exupéry) gave on July 12, 2018 a talk entitled "*Cache-conscious Offline Real-time Scheduling for Multi-core Platforms: Algorithms and Implementation*".
- Yliès Falcone (CORSE project-team) gave on July 11, 2018 a talk entitled "*Some Recent Work on the Runtime Monitoring of Systems*".

DEDUCTEAM Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

The ANR PROGRAMme 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.

8.2. International Initiatives

Brazil: STIC Amsud.

Argentina: Ecos

China: Inria-NSFC

8.3. Informal International Partners

Our main international partners are Alejandro Diáz-Caro (Buenos Aires), Bruno Lopes (Niteroi), Ying Jiang (Beijing), Florian Rabe (Bremen), Brigitte Pientka (McGill), César Muñoz (NASA), and Stéphane Graham-Lengrand (SRI).

8.4. International Research Visitors

Alejandro Díaz-Caro (Buenos Aires) has visited Deducteam for two weeks.

Ying Jiang (Beijing) has visited Deducteam for three weeks.

Aristomenis-Dionysios Papadopoulos (Imperial College, London) has visited Deducteam. He worked with Frédéric Blanqui on the development of a rewrite tactic in DEDUKTI [27].

8.4.1. Visits to International Teams

Gilles Dowek has spent two weeks at the University of Buenos Aires.

Gilles Dowek has spent two weeks at the Institute of Aerospace (USA).

GALLINETTE Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

Vercoma (Atlanstic 2020/Attractivity grant)

Goal: Verified comupter mathematics.

Coordinator: A. Mahboubi.

Duration: 08/2018 - 08/2021.

7.2. National Initiatives

7.2.1. ANR

FastRelax (ANR-14-CE25-0018).

Goal: Develop computer-aided proofs of numerical values, with certified and reasonably tight error bounds, without sacrificing efficiency.

Coordinator: Bruno Salvy (Inria, ENS Lyon).

Participant: A. Mahboubi.

Duration: 2014-2019.

Website: http://fastrelax.gforge.inria.fr/.

Note: This project started when A. Mahboubi was still in the Specfun project at the Saclay Île-de-France CRI. The budget is still managed there, within the Toccata project, but remains available to A. Mahboubi.

7.3. European Initiatives

7.3.1. H2020 Projects

7.3.1.1. CoqHoTT

Title: Coq for Homotopy Type Theory

Programm: H2020

Type: ERC

Duration: June 2015 - May 2020

Coordinator: Inria

Inria contact: Nicolas TABAREAU

Every year, software bugs cost hundreds of millions of euros to companies and administrations. Hence, software quality is a prevalent notion and interactive theorem provers based on type theory have shown their efficiency to prove correctness of important pieces of software like the C compiler of the CompCert project. One main interest of such theorem provers is the ability to extract directly the code from the proof. Unfortunately, their democratization suffers from a major drawback, the mismatch between equality in mathematics and in type theory. Thus, significant Coq developments have only been done by virtuosos playing with advanced concepts of computer science and mathematics. Recently, an extension of type theory with homotopical concepts such as univalence is gaining traction because it allows for the first time to marry together expected principles of equality. But the univalence principle has been treated so far as a new axiom which breaks one fundamental property of mechanized proofs: the ability to compute with programs that make use

of this axiom. The main goal of the CoqHoTT project is to provide a new generation of proof assistants with a computational version of univalence and use them as a base to implement effective logical model transformation so that the power of the internal logic of the proof assistant needed to prove the correctness of a program can be decided and changed at compile time—according to a trade-off between efficiency and logical expressivity. Our approach is based on a radically new compilation phase technique into a core type theory to modularize the difficulty of finding a decidable type checking algorithm for homotopy type theory. The impact of the CoqHoTT project will be very strong. Even if Coq is already a success, this project will promote it as a major proof assistant, for both computer scientists and mathematicians. CoqHoTT will become an essential tool for program certification and formalization of mathematics.

7.3.2. Collaborations in European Programs, Except FP7 & H2020

Program: COST

Project acronym: EUTYPES

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

Duration: 21/03/2016 - 20/03/2020.

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

Abstract: Types are pervasive in programming and information technology. A type defines a formal interface between software components, allowing the automatic verification of their connections, and greatly enhancing the robustness and reliability of computations and communications. In rich dependent type theories, the full functional specification of a program can be expressed as a type. Type systems have rapidly evolved over the past years, becoming more sophisticated, capturing new aspects of the behaviour of programs and the dynamics of their execution.

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

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

7.4. International Initiatives

7.4.1. Inria International Labs

Inria Chile

Associate Team involved in the International Lab:

7.4.1.1. GECO

Title: Gradual verification and robust proof Engineering for COq

International Partner (Institution - Laboratory - Researcher):

Universidad de Chile (Chile) - DCC, Pleaid team - Éric Tanter

Start year: 2018

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

The development of tools to construct software systems that respect a given specification is a major challenge of current and future research in computer science. Interactive theorem provers based on type theory, such as Coq, have shown their effectiveness to prove correctness of important pieces of software like the C compiler of the CompCert project. Certified programming with dependent types is attracting a lot of attention recently, and Coq is the de facto standard for such endeavors, with an increasing amount of users, pedagogical material, and large-scale projects. Nevertheless, significant work remains to be done to make Coq more usable from a software engineering point of view.

This collaboration project gathers the expertise of researchers from Chile (Inria Chile, Universidad de Chile, Universidad Católica de Valparaíso) and France (Inria Nantes, Inria Paris), in different areas that are crucial to develop the vision of certified software engineering. The focus of this project is both theoretical and practical, covering novel foundations and methods, design of concrete languages and tools, and validation through specific case studies.

The end result will be a number of enhancements to the Coq proof assistant (frameworks, tactic language) together with guidelines and demonstrations of their applicability in realistic scenarios.

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- Ambrus Kaposi has visited Gallinette from April 15 to July 15 as part of the ERC 'Visiting Fellowship Programmes' whose aims it to promote the widening of participation of researchers with a high potential in the ERC calls. The Scientific Council of the ERC believes that increasing the international exposure of researchers can help them to develop their full research potential. For this reason the ERC has invited relevant national and regional authorities in Europe to fund potential ERC candidates from the country or the region to visit teams of existing ERC Principal Investigators. The purpose is to offer these potential candidates an opportunity to broaden and strengthen their research profile and vision in an internationally competitive research environment before applying for an ERC grant.
- Simon Huber (University of Göteborg) has visited Simon Boulier and Nicolas Tabareau from Feb 26 to March 2 as a Short-Term Scientific Mission (STSM) funded by the EUTYPES COST Action.
- Jesper Cockx (Chalmers University) has visited Gaetan Gilbert and Nicolas Tabareau from Feb 19 to Feb 23 as a Short-Term Scientific Mission (STSM) funded by the EUTYPES COST Action.

7.5.1.1. Internships

- A. Defourné has visited the team from April to August for an internship on the subject "A Mini-ML with resource management", supervised by G. Munch-Maccagnoni and R. Douence.
- L. Pujet has visited the team from April to August for an internship on the subject "Interpreting Cubical Type Theory using forcing", supervised by N. Tabareau.

7.5.2. Visits to International Teams

7.5.2.1. Research Stays Abroad

- A. Mahboubi has been appointed as Endowed Professor at the Vrije Universiteit Amsterdam on a chair entitled "Automated verification of mathematical proof".
- G. Munch-Maccagnoni has visited the University of Cambridge from July 9th to July 19th to work with M. Fiore on the topic of categorical semantics of effects and resources in programming languages.
- G. Munch-Maccagnoni has visited Jane Street on July 19th to work with L. White on the topic of resource management in the OCaml programming language.

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.

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".

A first release of the library has been published in December 2018. It contains a small number of verified data structures, including resizable vectors, hash tables, priority queues, and Union-Find.

9.1.2. FUI Projects

9.1.2.1. Secur-OCaml

Participants: Damien Doligez, Fabrice Le Fessant.

The "Secur-OCaml" project (2015–2018) has been 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 has been involved in this project to integrate security features in the OCaml language, to build a new independent interpreter for the language, and to update the recommendations for developers issued by the former LaFoSec project of ANSSI. The end-of-project meeting took place in September 2018.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. Deepsea

Participants: Umut Acar, Vitaly 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: Gergö Barany, 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, as well as on extensions to the CompCert C compiler.

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.
- The University of Cambridge and ARM Ltd, Cambridge and Imperial College London: formal modeling and testing of weak memory models.

MARELLE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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.

8.1.2. FUI

The acronym *FUI* stands for "fonds unique interministériel" and is aimed at research and development projects in pre-industrial phase. The Marelle team is part of one such project.

- VERISICC (formal verification for masking techniques for security against side-channel attacks), This contracts concerns 5 partners: CRYPTOEXPERTS a company from the Paris region (île de France), ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), Oberthur Technologies, University of Luxembourg, and Marelle. A sixth company (Ninjalabs) acts as a sub-contractant. The financial grant for Marelle is 391 kEuros, including 111kEuros that are reserved for the sub-contractant. This project started in October 2018 for a duration of 4 years. The corresponding researcher for this contract is Benjamin Grégoire.

8.2. International Research Visitors

8.2.1. Visits of International Scientists

8.2.1.1. Internships

Joshua Gansher from Cornell and Sunjay Cauligi from the University of California at San Diego visited for three months, as part of their PhD training.

Vincent Laporte from IMDEA Madrid visited for 9 months.

Benoît Viguier from Radboud University, Nijmegen visited for 1 month.

8.2.2. Visits to International Teams

Yves Bertot visited AIST in February in Tsukuba, Japan, ITU Copenhagen in April in Copenhagen, Denmark, and the DeepSpec Summer School in July at Princeton University.

MEXICO Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

- Serge Haddad and Yann Duplouy have been participating in the *Simulation pour la sécurité du véhicule autonome*(SVA) project at SystemX, in cooperation with Renault, on the application of formal methods to the development of embedded systems for autonomous vehicles.
- Matthias Függer co-leads the Digicosme working group HicDiesMeus on "Highly Constrained Discrete Agents for Modeling Natural Systems" (parsys.lri.fr/HicDiesMeus).
- Matthias Függer participates in the Farman project Dicimus in collaboration with Thomas Nowak (LRI). The project is on modeling of bacterial interactions using techniques from distributed computing theory and VLSI design.

9.2. 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 on verification and synthesis of distributed algorithms.
- Laurent Fribourg participates in Digicosme Emergence Project “CODECSY” in collaboration with Antoine Girard (CentraleSupelec).

9.3. European Initiatives

Serge Haddad is a member of the European project ERC EQualIS “Enhancing the Quality of Interacting Systems” headed by Patricia Bouyer.

9.4. International Initiatives

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

9.4.1.1. 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.

9.4.2. Inria International Partners

9.4.2.1. Informal International Partners

Josep Carmona (UPC Barcelona) visited us in April and July 2018. He collaborated with Thomas Chatain on process mining.

9.5. International Research Visitors

9.5.1. Visits to International Teams

9.5.1.1. Research Stays Abroad

- Juraj Kolcˇák has started, in August 2018, a 6-month research visit in the MMM group / NII Tokyo (Japan), funded by the ERATO project, to work with the PI, Prof. Ichiro Hasuo. Stefan Haar has visited that group from Oct 29 to Friday Nov 2, preceded by a visit to Prof. Tatsuya Akutsu's group at Kyoto University (Uji campus) on Oct 26.

MOCQUA Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- Project acronym: ANR PRCE SoftQPro (ANR-17-CE25-0009)
  Project title: Solutions logicielles pour l'optimisation des programmes et ressources quantiques.
  Duration: Dec. 2017 - Nov. 2021
  Coordinator: Simon Perdrix
  Other partners: Atos-Bull, LRI, CEA-Saclay.
  Participants: Simon Perdrix, Emmanuel Jeandel, Emmanuel Hainry, and Romain Péchoux
  Abstract: Quantum computers can theoretically solve problems out of reach of classical computers. We aim at easing the crucial back and forth interactions between the theoretical approach to quantum computing and the technological efforts made to implement the quantum computer. Our software-based quantum program and resource optimisation (SoftQPRO) project consists in developing high level techniques based on static analysis, certification, transformations of quantum graphical languages, and optimisation techniques to obtain a compilation suite for quantum programming languages. We will target various computational model back-ends (e.g. QRAM, measurement-based quantum computations) as well as classical simulation. Classical simulation is central in the development of the quantum computer, on both ends: as a way to test quantum programs but also as a way to test quantum computer prototypes. For this reason we aim at designing sophisticated simulation techniques on classical high-performance computers (HPC).
- Project acronym: ANR PRCI VanQuTe (ANR-17-CE24-0035)
  Project title: Validation of near-future quantum technologies.
  Duration: Dec. 2017 - Nov. 2021
  Coordinator: Simon Perdrix
  Other partners: Atos-Bull, LRI, CEA-Saclay.
  Participants: Simon Perdrix, Emmanuel Jeandel, Emmanuel Hainry, and Romain Péchoux
  Abstract: Quantum computers can theoretically solve problems out of reach of classical computers. We aim at easing the crucial back and forth interactions between the theoretical approach to quantum computing and the technological efforts made to implement the quantum computer. Our software-based quantum program and resource optimisation (SoftQPRO) project consists in developing high level techniques based on static analysis, certification, transformations of quantum graphical languages, and optimisation techniques to obtain a compilation suite for quantum programming languages. We will target various computational model back-ends (e.g. QRAM, measurement-based quantum computations) as well as classical simulation. Classical simulation is central in the development of the quantum computer, on both ends: as a way to test quantum programs but also as a way to test quantum computer prototypes. For this reason we aim at designing sophisticated simulation techniques on classical high-performance computers (HPC).

8.1.2. Autres initiatives

- Quantex. Project acronym: PIA-GDN/Quantex. (initially an ITEA3 project finally funded by the *Grands défis du Numérique / Programme d'investissements d'avenir*).
  Project title: Simulation/Emulation of Quantum Computation.
  Duration: Feb. 2018 - Jan 2021.
  Coordinator: Huy-Nam Nguyen (Atos Bull).
  Other partners: Atos-Bull, LRI, CEA Grenoble.
  Participants: Simon Perdrix (WP leader), Emmanuel Jeandel
  Abstract: The lack of quantum computers leads to the development of a variety of software-based simulators to assist in the research and development of quantum algorithms. This proposal focuses on the development of a combined software-based and hardware-accelerated toolbox for quantum computation. A quantum computing stack including specification language, libraries and optimisation/execution tools will be built upon a well-defined mathematical framework mixing classical and quantum computation. Such an environment will be dedicated to support the expression of quantum algorithms for the purpose of investigation and verification.

8.2. European Initiatives

8.2.1. 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.

8.3. International Initiatives

8.3.1. Inria International Labs

8.3.1.1. IIL projects

Simon Perdrix is the WP leader in the ANR PRCI project VanQuTe (with LIP6, and the Singapore University of Technology and Design, the National University of Singapore, and the Nanyang Technological University). Emmanuel Jeandel is also a member of this project.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Victor Selivanov (Kazan University) was an Inria invited researcher in September 2018. We have worked on the computable aspects of Descriptive Set Theory.
- Cristóbal Rojas (Universidad Andres Bello, Santiago) visited us during one month in September 2018. We have worked on the computable aspects of invariant measures in dynamical systems.
- Alexander Frank (Universidad Andres Bello, Santiago) visited us during three weeks in September-October 2018. We have worked on the computable aspects of invariant measures in dynamical systems.
- Bruce Kapron (University of Victoria, Canada) visited us in October 2018. We have worked on applications of tier based type systems to characterize the class of second order functionals computable in polynomial time.
- Damiano Mazza (CNRS, Université de Paris 13) visited us in March 2018. We have worked on the adaptation of linear logic to a functional programming languages with infinite streams to characterize the class of first order functions over the real computable in polynomial time.

PARSIFAL Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

COCA HOLA: Cost Models for Complexity Analyses of Higher-Order Languages, coordinated by B. Accattoli, 2016–2019.

FISP: The Fine Structure of Formal Proof Systems and their Computational Interpretations, coordinated by Lutz Straßburger in collaboration with Université Paris 7, Universität Innsbruck and TU Wien, 2016–2019.

8.1.2. Competitivity Clusters

UPScale: Universality of Proofs in SaCLay, a Working Group of LabEx DigiCosme, organized by Chantal Keller (LRI) with regular participation from Parsifal members and a post-doc co-supervision.

8.2. International Research Visitors

8.2.1. Internships

Simon Colin did an M1 internship supervised by G. Scherer, conducting a static analysis to check the safety, in OCaml, of unboxing annotations on type declarations.

Alban Reynaud did an L3 internship supervised by G. Scherer, conducting a static analysis to check the safety, in OCaml, of recursive value declarations.

8.2.2. Visits to International Teams

8.2.2.1. Research Stays Abroad

S. Graham-Lengrand was an International Fellow at SRI International, for 25 months over a period of three years between 2015 and 2018.

PI.R2 Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

Pierre-Louis Curien, Yves Guiraud, Hugo Herbelin, and Alexis Saurin are members of the GDR Informatique Mathématique, in the LHC (Logique, Homotopie, Catégories) and Scalp (Structures formelles pour le calcul et les preuves) working groups. Alexis Saurin is coordinator of the Scalp working group.

Pierre-Louis Curien, Yves Guiraud (local coordinator) 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.

Yves Guiraud is member of the GDR Tresses, federating French researchers working on algebraic, algorithmic and topological aspects of braid groups, low-dimensional topology, and connected subjects.

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 collaborates with ANSSI on the topic of certified ful programming in Coq.

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).

Yann Régis-Gianas and Alexis Saurin (coordinator) 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.

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. 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 officially started 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 Hasuo (NII, Tokyo). The full name of the project is Concurrent, Resourceful and full 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 the 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 project Inria - 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, that started in December 2017 and will end in Marche 2019.

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, Universidad Nacional de Córdoba, and Universidad de Chile.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Mauro Jaskelioff (National University of Rosario and CONICET, Argentina) visited the team for a week in May 2018.

Vadim Zaliva (PhD student at CMU) visited the team for one month in July 2018 and collaborated with Matthieu Sozeau on the use of Template-Coq to verify translations from shallow to deep embeddings.

7.4.2. Internships

Yann Régis-Gianas supervised the internship of Loïc Peyrot (Master 1, Paris Diderot) about the development of a tool to define exercises for the learn-ocaml platform in a single ML file.

Yann Régis-Gianas supervised the internship of Carine Morel (Master 1, Paris Diderot) about the development of a user-friendly teaching-oriented documentation for the learn-ocaml platform.

Yann Régis-Gianas supervised the internship of Olivier Martinot (Licence 3, Paris Diderot) about the implementation of a set of efficient incrementalised combinators for list processing in cache-transfer style.

Alexis Saurin co-supervised the internship of Ikram Cherigi (Master 2 LMFI, Paris Diderot) about classical realisability and forcing in set theory.

Alexis Saurin supervised the internship of Xavier Onfroy (Master 2 LMFI, Paris Diderot) on formalisation of circular proofs in fixed-point logics and the decidability of validity.

Alexis Saurin supervised the internship of Kostia Chardonnet (Master 1 MPRI, Paris Diderot) about call-by-need calculus, degrees of lazyness and probabilistic lambda calculus.

7.4.3. Research Stays Abroad

Pierre-Louis Curien visited East China Normal University for a month from mid-October to mid-November 2018 (collaborations with Yuxin Deng and Min Zhang) as invited professor.

Pierre-Louis Curien visited the Institute of Mathematics of the Serbian Academy of Sciences in Belgrade in September 2018 for a week (collaboration with Zoran Petrić and other coauthors).

Hugo Herbelin participated to the Types, Sets and Constructions Trimester Program at the Hausdorff Research Institute of Mathematics in Bonn, May-August 2018.

SUMO Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. Rennes Métropole: Allocation d'Installation Scientifique (AIS)

- Individual grant, led by Nicolas Markey

The objective of this project is to explore two research directions in the continuity of recent works: a truly quantitative theory of formal verification on the one hand, and the development of strategy-synthesis algorithms for modular systems on the other hand.

9.2. National Initiatives

9.2.1. ANR TickTac: Efficient Techniques for Verification and Synthesis of Real-Time Systems (2019-2023)

- Led by Ocan Sankur (SUMO);
- Participants: Thierry Jéron, Nicolas Markey, Ocan Sankur
- Partners: LSV (Cachan), ISIR (Paris), LaBRI (Bordeaux), LRDE (Paris), LIF (Marseille)

The aim of TickTac is to develop novel algorithms for the verification and synthesis of real-time systems using the timed automata formalism. One of the project's objectives is to develop an open-source and configurable model checker which will allow the community to compare algorithms. The algorithms and the tool will be used on a motion planning case study for robotics.

9.2.2. 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.

9.2.3. 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.

9.2.4. 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 the extension of the SimGrid programming model of MPI with synchronization primitives, the formalisation in ATL, of this model, and its adaptation to dynamic partial-order-reduction methods (DPOR) that allow to reduce the explored state space. A prototype implementation of an existing method that combines DPOR with true-concurrency models has been experimented on toy examples.

9.2.5. National informal collaborations

The team collaborates with the following researchers:

- 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;

9.3. International Initiatives

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

9.3.1.1. EQUAVE

Title: Efficient Quantitative Verification

International Partner (Institution - Laboratory - Researcher):

Indian Institute of Technology Bombay (India) - Dpt of Computer Science and Engineering - S. Akshay

Start year: 2018

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

Formal verification has been addressed for a long time. A lot of effort has been devoted to boolean verification, i.e., formal analyis of systems that check whether a given property is true or false.

In many settings, a boolean verdict is not sufficient. The notions of interest are for instance the amount of confidential information leaked by a system, the proportion of some protein after a duration in some experiment in a biological system, whether a distributed protocol satisfies some property only for a bounded number of participants... This calls for quantitative verification, in which algorithms compute a value such as the probability for a property to hold, the mean cost of runs satisfying it, the time needed to achieve a complex workflow...

A second limitation of formal verification is the efficiency of algorithms. Even for simple questions, verification is rapidly PSPACE-complete. However, some classes of models allow polynomial time verification. The key techniques to master complexity are to use concurrency, approximation, etc

The objective of this project is to study efficient techniques for quantitative verification, and develop efficient algorithms for models such as stochastic games, timed and concurrent systems,

9.3.1.2. 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.

9.3.2. Inria International Partners

9.3.2.1. 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 (U Mons, Belgium) on the verification of stochastic timed systems;
- Mickael Randour (U Mons, Belgium) on quantitative games for synthesis;
- Kim G. Larsen (U Aalborg, Denmark) on quantitative timed games, and on topics related to urban train systems modeling;
- Josef Widder, Marijana Laźic (TU Wien, Austria), Igor Konnov (Inria Nancy, LORIA) on the automated verification of randomized distributed algorithms.
- John Mullins (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.
- Alessandro Giua and Michele Pinna (Univ. Cagliari, Italy), on diagnosis and unfolding techniques for concurrent systems.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- In June 2018, S. Akshay visited the SUMO team for one week.
- Laurie Ricker (Mount Allison University, Canada) visited the team during 3 months in 2018.
- Josef Widder visited the team as an invitee of ISTIC (Université Rennes 1) : 2 weeks in September 2018.
- Romulo Meira-Goes (PhD student of S. Lafortune, University of Michigan, USA) visited our team during four months in 2018 (Synthesis of Supervisors Robust Against Sensor Deceptions Attacks).

9.4.1.1. Internships

- Flavia Palmieri, May-June 2018, Loïc Hélouët.
- M2 internship of Ritam Raha, October-December 2018, Nicolas Markey and Loïc Hélouët.
- Internship of undergraduate student Adwait Amit Godbole, Blaise Genest.

9.4.2. Visits to International Teams

In October 2018, Loïc Hélouët visited IIT Bombay and IIT Delhi for 10 days, to work within the associated team EQUAVE.

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)

9.1.2. MILC

Participant: Sylvie Boldo [contact].

MILC is a DIM-RFSI project. It is a one-year project (2018–2019) that aims at formalizing measure theory and Lebesgue integral in the Coq proof assistant. https://lipn.univ-paris13.fr/MILC/

Partners: Université Paris 13 (M. Mayero, PI), Inria Paris, Inria Saclay

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. FP7 & H2020 Projects

9.3.1.1. EMC2

Participant: Sylvie Boldo [contact].

A new ERC Synergy Grant 2018 project, called Extreme-scale Mathematically-based Computational Chemistry (EMC2) has just been accepted. The PIs are É. Cancès, L. Grigori, Y. Maday and J.-P. Piquemal. S. Boldo is part of the work package 3: validation and certification of molecular simulation results. https://www.sorbonne-universite.fr/newsroom/actualites/erc-synergy-grant-2018

9.3.2. Collaborations in European Programs, Except FP7 & H2020

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

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

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

Duration: 2015-2019

Coordinator: Herman Geuvers, Radboud University Nijmegen, The Netherlands

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

Abstract: Types are pervasive in programming and information technology. A type defines a formal interface between software components, allowing the automatic verification of their connections, and greatly enhancing the robustness and reliability of computations and communications. In rich dependent type theories, the full functional specification of a program can be expressed as a type. Type systems have rapidly evolved over the past years, becoming more sophisticated, capturing new aspects of the behaviour of programs and the dynamics of their execution.

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

VERIDIS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR International Project SYMBIONT

Project acronym: SYMBIONT.

Project title: Symbolic Methods for Biological Networks.

Duration: July 2018 – June 2021.

Coordinators: Thomas Sturm and Andreas Weber (Univ. of Bonn, Germany).

Other partners: Univ. of Lille 1, Univ. of Montpellier, Inria Saclay Île de France (Lifeware), RWTH Aachen (Department of Mathematics and Joint Research Center for Computational Biomedecine), Univ. of Kassel.

Participants: Thomas Sturm.

Abstract: SYMBIONT is an international interdisciplinary project, funded by ANR in France and by DFG in Germany under the PRCI program. It includes researchers from mathematics, computer science, systems biology, and systems medicine. Computational models in systems biology are built from molecular interaction networks and rate laws, involving parameters, resulting in large systems of differential equations. The statistical estimation of model parameters is computationally expensive and many parameters are not identifiable from experimental data. The project aims at developing novel symbolic methods, aiming at the formal deduction of principal qualitative properties of models, for complementing the currently prevailing numerical approaches. Concrete techniques include tropical geometry, real algebraic geometry, theories of singular perturbations, invariant manifolds, and symmetries of differential systems. The methods are implemented in software and validated against models from computational biology databases.

More information: https://www.symbiont-project.org/.

8.1.2. ANR Project IMPEX

Project acronym: IMPEX.

Project title: Implicit and explicit semantics integration in proof based developments of discrete systems.

Duration: December 2013 – December 2018.

Coordinator: Dominique Méry.

Other partners: ENSEEIHT/IRIT Toulouse, Supélec, Telecom Sud Paris, Systerel. Pierre Castéran from LaBRI Bordeaux also contributed to the project.

Participants: Souad Kherroubi, Dominique Méry.

Abstract: Modeling languages provide techniques and tool support for the design, synthesis, and analysis of formal models that arise during system development. The semantics of these languages is well understood by their users and is therefore implicit in the models. The languages do not provide concepts for explicitly representing characteristics (domain knowledge) resulting from an analysis of the underlying application domain [69]. We suggest that ontologies are good candidates for defining domain theories and for uniquely identifying concepts encapsulating domain knowledge. The objective [50] is to offer rigorous mechanisms for handling domain knowledge in design models. The main results of the project are summarized in [18] and show the importance of three operations over models namely annotation, dependency and refactoring [38].

8.1.3. ANR Project Formedicis

Project acronym: Formedicis.

Project title: Formal methods for the development and the engineering of critical interactive systems.

Duration: January 2017 – December 2020.

Coordinator: Bruno d'Augsbourg (Onera).

Other partners: ENSEEIHT/IRIT Toulouse, ENAC, Université de Lorraine (Veridis).

Participants: Dominique Méry.

Abstract: For 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: for example, the investigation into the crash of the Rio-Paris flight AF 447 in 2009 pointed out a design issue in the Flight Director interface as one of the original causes of the crash. Formedicis aims at designing a formal hub language, in which designers can express their requirements concerning the interactive behavior that must be embedded inside applications, and at developing a framework for validating, verifying, and implementing critical interactive applications expressed in that language.

More information: http://www.agence-nationale-recherche.fr/Project-ANR-16-CE25-0007.

8.1.4. ANR Project DISCONT

Project acronym: DISCONT.

Project title: Correct integration of discrete and continuous models.

Duration: March 2018 – February 2022.

Coordinator: Paul Gibson (Telecom Sud Paris).

Other partners: ENSEEIHT/IRIT Toulouse, LACL, ClearSy, Université de Lorraine (Veridis).

Participants: Dominique Méry.

Abstract: Cyber-Physical Systems (CPSs) connect the real world to software systems through a network of sensors and actuators that interact in complex ways, depending on context and involving different spatial and temporal scales. Typically, a discrete software controller interacts with its physical environment in a closed-loop schema where input from sensors is processed and output is generated and communicated to actuators. We are concerned with the verification of the correctness of such discrete controllers, which requires correct integration of discrete and continuous models. Correctness should arise from a design process based on sound abstractions (including discretizations) and models of the relevant physical laws. DISCONT aims at bridging the gap between the discrete and continuous worlds of formal methods and control theory. We will lift the level of abstraction above that found in current bridging techniques and provide associated methodologies and tools. Our concrete objectives are to develop a formal hybrid model, elaborate refinement steps for control requirements, propose a rational design method and support tools, and validate them based on use cases from a range of application domains.

More information: https://fusionforge.int-evry.fr/www/discont/.

8.1.5. ANR Project PARDI

Project acronym: PARDI.

Project title: Verification of parameterized distributed systems.

Duration: January 2017 – December 2020.

Coordinator: Philippe Quéinnec (ENSEEIHT/IRIT Toulouse).

Other partners: Université Paris Sud/LRI, Université Nanterre/LIP6, Inria Nancy Grand Est (Veridis).

Participants: Marie Duflot-Kremer, Igor Konnov, Stephan Merz.

Abstract: 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: http://pardi.enseeiht.fr/.

8.1.6. Inria IPL HAC SPECIS

Project acronym: HAC SPECIS.

Project title: High-performance application and computers: studying performance and correctness in simulation.

Duration: June 2016 – June 2020.

Coordinator: Arnaud Legrand (CNRS & Inria Grenoble Rhône Alpes, Polaris).

Other partners: Inria Grenoble Rhône Alpes (Avalon), Inria Rennes Bretagne Atlantique (Myriads), Inria Bordeaux Sud Ouest (Hiepacs, Storm), Inria Saclay Île de France (Mexico), Inria Nancy Grand Est (Veridis).

Participants: Marie Duflot-Kremer, Stephan Merz.

Abstract: The goal of HAC SPECIS is to answer methodological needs of HPC application and runtime developers and to allow the study of 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. VeriDis contributes 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. Yann Duplouy joined the project in December 2018 as a post-doctoral researcher with the objective of designing and implementing a statistical model checker for SimGrid.

More information: http://hacspecis.gforge.inria.fr.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. ERC Matryoshka

Program: ERC.

Project acronym: Matryoshka.

Duration: April 2017 – March 2022.

Coordinator: Jasmin Blanchette (VU Amsterdam).

Participants: Daniel El Oraoui, Mathias Fleury, Pascal Fontaine, Hans-Jörg Schurr, Sophie Tourret, Uwe Waldmann.

Abstract: Proof assistants are increasingly used to verify hardware and software and to formalize mathematics. However, despite some 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 – but only so much can be done when viewing automatic provers as black boxes. We propose to deliver much higher levels of automation to users of proof assistants by fusing and extending two lines of research: automatic and interactive theorem proving. 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. 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, and integrate them in proof assistants. Users 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.

More information: http://matryoshka.gforge.inria.fr/.

8.2.1.2. FET-Open CSA SC^2

Program: FET Open CSA.

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.

Participants: Pascal Fontaine, Thomas Sturm.

Abstract: 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. Before the project, the two communities were largely disjoint and unaware of the achievements of each other, despite strong reasons for them to discuss and collaborate. Researchers from the two communities rarely interacted, and also their tools lacked common, mutual interfaces for unifiying their strengths. The SC^2 project initiated 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. Now that the project is finished, we believe that these activities will continue to foster cross-fertilization of both fields and bring mutual improvements to the techniques and the software tools developed by both communities.

8.2.2. Collaborations in European Programs, Except FP7 & H2020

Program: Erasmus+.

Project acronym: PIAF.

Project title: Pensée Informatique et Algorithmique au Fondamental / Computational Thinking in and Algorithmic in Primary Education.

Coordinator: Université de Liège.

Other partners: Université du Luxembourg, Saarland University, ESPE Nancy.

Participant: Marie Duflot-Kremer.

Abstract: The goal of the PIAF project is threefold: creating a repository of skills related to computational and algorithmic thinking, designing activities aiming at the acquisition of these skills, and evaluating the impact of these activities on primary school children and their computational thinking capacities.

8.3. International Initiatives

8.3.1. Inria International Partners

Project acronym: KANASA.

Title: Kanazawa-Nancy Partnership for Satistifiability and Arithmetics.

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

In 2016/17, Vu Xuan Tung, then a PhD student from JAIST, spent one year in the VeriDis team, and Pascal Fontaine was a reviewer of his PhD thesis, defended in 2018. There were mutual visits in 2018, and the joint research evolves towards applying SMT techniques for detecting malware in obfuscated code.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Cezary Kaliszyk.

Date: 17 May 2018 – 17 June 2018.
Institution: University of Innsbruck, Austria.
Host: Pascal Fontaine.

Cezary Kaliszyk is an assistant professor at the University of Innsbruck. He is an expert in and a precursor of the use of machine learning in an automated reasoning context. He is the principal investigator for the ERC Starting Grant SMART (Strong Modular Proof Assistance Reasoning Across Theories). His research interests cover machine learning for theorem proving, formalization of mathematics, logical and proof translations, automated reasoning and proof data management. During his stay in Nancy, we initiated a new direction of research for quantifier instantiation, that is, using machine learning as a means of filtering the numerous instances generated by heuristic instantiation procedures in SMT.

8.4.2. Internships

Alexis Grall

Date: 1 March 2018 – 31 August 2018
Institution: Université de Lorraine
Host: Dominique Méry

In his master thesis, Alexis Grall studied the localization of Event-B models and their tranformation into the DistAlgo programming language. The Event-B models are obtained for designing distributed algorithms such as the leader election or the sliding window protocol. The transformation is proved to be sound and to preserve the properties of the Event-B models.

Axel Palaude

Date: 1 May 2018 – 31 July 2018
Institution: ENS Rennes
Host: Igor Konnov, Stephan Merz

Axel Palaude extended the short counter-example property that underlies decidability results for the verification of threshold automata (cf. section 7.2) to the case of threshold automata with real-time constraints.

CIDRE Project-Team

8. Partnerships and Cooperations

8.1. 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 (2014-2018): "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" - https://hardblare.cominlabs.u-bretagneloire.fr/**

  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" - https://bigclin.cominlabs.u-bretagneloire.fr/fr**

  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.

8.2. National Initiatives

8.2.1. ANR

- **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.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Carlos Maziero, Professor at the Federal University of Parana (Curitiba, Brazil) has visited our team from January 2018 till December 2018. During his stay, he has worked on models of normal behaviours in distributed applications.

8.3.1.1. Research Stays Abroad

Mourad Leslous did an international mobility of three months in the team of Lorenzo Cavallaro in the Information Security Group (ISG) at Royal Holloway, University of London. 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 - July 2018

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's: Serge Haddad, ENS Cachan.

Abstract: In this project we investigate classes of utility and privacy measures, and we 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 consider a probabilistic setting. We focus, in particular, on measures that are expressible as linear functions of the probabilities.

7.1.2. SUPREME

Project title: Statistical-Utility Preserving Methods for Privacy Protection

Funded by: Département STIC

Duration: 2018 - 2019

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's: Serge Haddad, ENS Cachan.

Abstract: In this project we study the theoretical foundations, methods and tools to protect the privacy of the individuals under certain constraints. In particular we focus on mechanisms that: (1) are robust with respect to combination of information from different sources, (2) can be applied directly by the user, thus avoiding the need of a trusted party, and (3) provide an optimal trade-off between privacy and utility.

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 investigate quantitative notions and tools for proving program correctness and protecting privacy. In particular, we 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.

7.2.2. MAGIC

Program: PEPS I3A

Project title: Machine Games for Information Protection

Duration: February 2018 - December 2018

Coordinator: Konstantinos Chatzikokolakis, CNRS (EPI Comète) and Ecole Polytechnique

Other PI's and partner institutions: Giovanni Cherubin, EPFL, Switzerland. Serge Haddad, ENS Cachan.

Abstract: In this project, we study a Machine Learning approach to develop methods for the Protection of Private Information. The idea is based on the Generative Adversarial Network (GAN) paradigm: the defender and the attacker are modeled as two adversaries in a game, where the payoff is the attacker's acquisition of the user's private data by exploiting the system vulnerabilities, side information, and probabilistic inference.

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: January 2016 - December 2018

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. Participation in International Programs

7.3.2.1. 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 and 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..

7.3.2.2. EPIC

Program: STIC-Amsud.

Project acronym: EPIC.

Project title: EPistemic Interactive Concurrency/

Duration: Oct 2016 - Oct 2018.

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 and 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.

7.3.2.3. FACTS

Program: ECOS NORD.

Project acronym: FACTS.

Project title: Foundational Approach to Cognition in Today?s Society.

Duration: Jan 1 2019 - Dec 31, 2021.

URL: https://goo.gl/zVhg32

Coordinator: Frank Valencia, Ecole Polytechnique.

Other PI's and partner institutions: Jean-Gabriel Ganascia LIP6, Sorbonne University and Camilo Rueda, Universidad Javeriana de Cali, Colombia.

Abstract: This projects aims at studying the phenomenon of "Group Polarization"; the tendency for a group to learn or acquire beliefs or to make decisions that are more extreme than the initial inclinations of its members.

7.3.3. Inria International Partners

7.3.3.1. PriDat

Project title: Privacy-Friendly Data Analytics

Funded by: Siebel Energy Institute

Duration: September 2018 - August 2019

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

Other PI's: Giovanni Cherubin, EPFL, Switzerland. Moreno Falaschi, University of Siena, Italy. Mario Ferreira, Federal University of Minas Gerais, Brazil.

Abstract: The objective of this project is to develop methodologies for protecting the privacy of individuals while letting their data be collected and used for analytical purposes.

7.3.3.2. Informal International Partners

Geoffrey Smith, Florida International University, USA

Carroll Morgan, NICTA , Australia

Annabelle McIver, Maquarie University, Australia

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

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil. Dec 2018

Borja de Balle Pigem. Sr. Machine Learning Scientist. Amazon, UK. Dec 2018

Takao Murakami, Assistant Professor, National Institute of Advanced Industrial Science and Technology (AIST), Japan. Dec 2018

Yusuke Kawamoto, Assistant Professor, National Institute of Advanced Industrial Science and Technology (AIST), Japan. March 2018 and Nov-Dec 2018

Carlos Olarte, Assistant Professor, Universidade Federal do Rio Grande do Norte, Brazil. Oct-Dec 2018

Daniele Gorla, Professor, University of Rome "La Sapienza". Aug - Sep 2018.

Giovanna Broccia, PhD student, University of Pisa, Italy, June 2018

Camilo Rueda, Professor, Universidad Javeriana de Cali, Colombia. May 2018 and Nov 2018

Prakash Panangaden, University of McGill, Montreal, Canada. Feb 2018

7.4.2. Internships

Haoteng Yin. Academy for Advanced Interdisceplinary Studies, Peking University. From June 2018 until Sept 2018.

Kacem Kefki. University of Paris Saclay. From June 2018 until July 2018.

Arthur Américo. Universidade Federal de Minas Gerais. From April 2018 until June 2018.

Noémie Fong. ENS Paris. From April 2018 until Sept 2019.

Pedro Bahamondes. Ecole Polytechnique. From Sept 2017 until March 2018.

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

Jason Lopez, Universidad Javeriana de Cali, Colombia. From May until Agost 2018.

DATASPHERE Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

The team is hosted by IXXI, the Complex System Institute, at ENS Lyon, and strongly involved in the interdisciplinary cooperation promoted by IXXI. Stéphane Grumbach is vice-director of IXXI. Kavé Salamatian is in the Executive committee of the Data Institute of Grenoble Alps Institute, and of the Cyber@Alps Institute of cybersecurity.

9.2. National Initiatives

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

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. 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.

9.4. International Research Visitors

9.4.1. Visits to International Teams

9.4.1.1. Research Stays Abroad

Stéphane Grumbach has been visiting scientist at the Research Institute on Humanity and Nature, RIHN, in Kyoto.

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, that is, 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 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 3D-Secure authentication protocol. 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*, from October 2014 to March 2018. 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, our 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. The 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 the 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

9.3.1.1. Informal 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 Constantin Catalin Dragan (Univ of Surrey), Francois Dupressoir (Univ of Surrey), and Bogdan Warinschi (Univ Bristol) on proving security of voting protocols with EasyCrypt.
- Collaboration with Matteo Maffei (Univ Wien) on type systems for e-voting systems
- Collaboration with Bogdan Warinschi (Univ Bristol) on defining game-based privacy for e-voting protocols
- Collaboration with Robert Künnemann (CISPA, Germany) on the development of the SAPIC tool.
- 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

- Bogdan Warinschi (Univ Bristol), November 2018

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

PRIVATICS Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. 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).

7.1.2. 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
- 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.

7.1.3. CyberAlps

- Title: CyberAlps
- Duration: 2018 - .
- Coordinator: IF.
- Others partners: CEA LETI, CERAG, CESICE, CREg, G2E lab, GIPSA-lab, GSCOP, IF, LCIS, LIG, LISTIC, LJK, PACTE, TIMC-IMAG, VERIMAG.
- Abstract: The Grenoble Alpes Cybersecurity Institute aims at undertaking ground-breaking interdisciplinary research in order to address cybersecurity and privacy challenges. Our main technical focus is on low-cost secure elements, critical infrastructures, vulnerability analysis and validation of large systems, including practical resilience across the industry and the society. Our approach to cybersecurity is holistic, encompassing technical, legal, law-enforcement, economic, social, diplomatic, military and intelligence-related aspects with strong partnerships with the private sector and robust national and international cooperation with leading institutions in France and abroad.

7.1.4. Antidot

- Title: Antidot
- Type: Fédération Informatique de Lyon (inter laboratories project)
- Duration: September 2018 - 2020.
- Coordinator: Inria.
- Others partners: LIRIS.
- Abstract: The ANTIDOT project is interested in the privacy issues raised by the increasingly ubiquitous collection of mobility data and their exploitation by third-party applications. The objective of this project is to propose solutions and tools to increase the user awareness about the risks of violation of their privacy in the context of the mobile Internet. In order to achieve this objective, ANTIDOT will jointly address the study of information gathering mechanisms, the study of mobility data vulnerabilities and the protection of this personal data.

7.2. National Initiatives

7.2.1. 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.

7.2.2. ANR

7.2.2.1. CISC

Title: Certification of IoT Secure Compilation.

Type: ANR.

Duration: April 2018 - March 2022.

Coordinator: Inria INDES project-team (France)

Others partners: Inria CELTIC project-team (France), College de France (France) (France).

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

Abstract: The objective of the ANR CISC project is to investigate multitier languages and compilers to build secure IoT applications with private communication. A first goal is to extend multitier platforms by a new orchestration language that we call Hiphop.js to synchronize internal and external activities of IoT applications as a whole. CISC will define the language, semantics, attacker models, and policies for the IoT and investigate automatic implementation of privacy and security policies by multitier compilation of IoT applications. To guarantee such applications are correct, and in particular that the required security and privacy properties are achieved, the project will certify them using the Coq proof assistant.

7.2.2.2. 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 .

7.2.2.3. 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.

7.2.3. 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/).

7.2.4. 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.

7.3. European Initiatives

7.3.1. Collaborations in European Programs, Except FP7 & H2020

7.3.1.1. 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.

7.3.1.2. 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."

7.4. International Initiatives

7.4.1. DATA

Title: Data and Algorithmic Transparency and Accountability

International Partner (Institution - Laboratory - Researcher):

Université du Québec à Montréal (UQAM) (Canada) - Département d'informatique - Sébastien Gambs

Start year: 2018

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

The accelerated growth of the Internet has outpaced our abilities as individuals to maintain control of our personal data. The recent advent of personalized services has lead to the massive collection of personal data and the construction of detailed profiles about users. However, users have no information about the data which constitute its profile and how they are exploited by the different entities (Internet companies, telecom operators, ...). This lack of transparency gives rise to ethical issues such as discrimination or unfair processing.

In this associate team, we propose to strengthen the complementary nature and the current collaborations between the Inria Privatics group and UQAM to advance research and understanding on data and the algorithmic transparency and accountability.

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- Sébastien Gambs visited the team in Lyon in April 2018 for a week to initiate the DATA collaboration. We also organized a workshop in data and algorithmic transparency during this week.
- Gergely Acs, assistant professor at Budapest University (Hungary), visited our team for 2 months, from mi-May to mid-July. He worked together with Claude Castelluccia on machine learning (in)security. In particular, he studied how adversarial examples can be used to evade monitoring, and consequently improve privacy.

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 Paris/EPI Antique, Inria Rennes/EPI Celtique, Airbus Operations SAS, AMOSSYS, CEA-LIST, TrustInSoft

Duration: January 2015 - September 2019.

Coordinator: Jérôme Féret, EPI Antique, Inria Paris (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, Université 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.

8.1.1.4. TECAP

Title: TECAP: Protocol Analysis - Combining Existing Tools (ANR générique 2017.)

Other partners: Inria Nancy/EPI PESTO, Inria Sophia Antipolis/EPI MARELLE, IRISA, LIX, LSV - ENS Cachan.

Duration: January 2018 - December 20

Coordinator: Vincent Cheval, EPI PESTO, Inria Nancy (France)

Participants: Bruno Blanchet, Benjamin Lipp

Abstract: A large variety of automated verification tools have been developed to prove or find attacks on security protocols. These tools differ in their scope, degree of automation, and attacker models. The aim of this project is to get the best of all these tools, meaning, on the one hand, to improve the theory and implementations of each individual tool towards the strengths of the others and, on the other hand, 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.

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 Bhargavan, Inria

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: The SECOMP project is aimed at leveraging emerging hardware capabilities for fine-grained protection to build the first, efficient secure compilation chains for realistic low-level programming languages (the C language, and Low* a safe subset of C embedded in F* for verification). These compilation chains 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 compilation chains target a tagged architecture, which associates a metadata tag to each word and efficiently propagates and checks tags according to software-defined rules. We will use property-based testing and formal verification to provide high confidence that our compilers are indeed secure.

8.2.1.3. NEXTLEAP

Title: NEXTLEAP: NEXT generation Legal Encryption And Privacy

Programm: H2020

Duration: January 2016 - December 2018

Coordinator: Harry Halpin, Inria

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

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

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

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

- TLS analysis: Microsoft Research (Cambridge), Mozilla, University of Rennes
- F*: Microsoft Research (Redmond, Cambridge, Bangalore), MSR-Inria, CMU, MIT, University of Ljubljana, Nomadic Labs, Zen Protocol, Princeton University
- SECOMP: MPI-SWS, CISPA, Stanford University, CMU, University of Pennsylvania, Portland State University, University of Virginia, University of Iai
- Micro-Policies: University of Pennsylvania, Portland State University, MIT, Draper Labs, Dover Microsystems

8.3.2. Participation in Other International Programs

8.3.2.1. SSITH/HOPE

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

Program: DARPA SSITH

Duration: December 2017 - February 2021

Coordinator: Charles Stark Draper Laboratory

Other Participants: Inria Paris, University of Pennsylvania, MIT, Portland State University, Dover Microsystems, DornerWorks

Participants from Inria Prosecco: Catalin Hritcu, Roberto Blanco, Jérémy Thibault

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.

8.3.2.2. Everest Expedition

Program: Microsoft Expedition and MSR-Inria Collaborative Research Project

Expedition Participants: Microsoft Research (Cambridge, Redmond, Bangalore), Inria, MSR-Inria, CMU, University of Edinburgh

Duration of current MSR-Inria Project: October 2017 – October 2020

Participants from Inria Prosecco: Karthikeyan Bhargavan, Catalin Hritcu, Danel Ahman, Benjamin Beurdouche, Victor Dumitrescu, Nadim Kobeissi, Théo Laurent, Guido Martínez, Denis Merigoux, Marina Polubelova, Jean-Karim Zinzindohoué

Participants from other Inria teams: David Pichardie (Celtique), Jean-Pierre Talpin (TEA)

Abstract: The HTTPS ecosystem (HTTPS and TLS protocols, X.509 public key infrastructure, crypto algorithms) is the foundation on which Internet security is built. Unfortunately, this ecosystem is brittle, with headline-grabbing attacks such as FREAK and LogJam and emergency patches many times a year.

Project Everest addresses this problem by constructing a high-performance, standards-compliant, formally verified implementation of components in HTTPS ecosystem, including TLS, the main protocol at the heart of HTTPS, as well as the main underlying cryptographic algorithms such as AES, SHA2 or X25519.

At the TLS level, for instance, we are developing new implementations of existing and forthcoming protocol standards and formally proving, by reduction to cryptographic assumptions on their core algorithms, that our implementations provide a secure-channel abstraction between the communicating endpoints. Implementations of the core algorithms themselves are also verified, producing performant portable C code or highly optimized assembly language.

We aim for our verified components to be drop-in replacements suitable for use in mainstream web browsers, servers, and other popular tools and are actively working with the community at large to improve the ecosystem.

https://project-everest.github.io

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Amal Ahmed (Northeastern University, USA) joined Inria as a Visiting Professor from September 2017 to July 2018; she gave a seminar on "Compositional Compiler Verification for a Multi-Language World".
- Aaron Weiss (Northeastern University, USA) joined Inria as a Visiting Scientist from September 2017 to July 2018; he gave a seminar on "Rust Distilled: An Expressive Tower of Languages"
- Justin Hsu (University of Wisconsin–Madison, USA) visited Prosecco on 26 January 2018 and gave a talk entitled "From Couplings to Probabilistic Relational Program Logics"
- Deepak Garg (MPI-SWS, Germany) visited Prosecco on 21 February and 6 December 2018
- Marco Patrignani (CISPA, Germany) visited Prosecco on 21 February 2018
- Arthur Azevedo de Amorim (CMU) visited Prosecco on 10–13 April 2018 and gave a seminar on "The Meaning of Memory Safety"

- Prasad Naldurg (IBM Research, India) joined Prosecco as a Visiting Researcher from May 2018; he gave a Prosecco seminar on "Encrypted Analytics: Computing directly on encrypted databases"
- Vincent Gramoli (NICTA/Data61-CSIRO and University of Sydney, Australia) visited Prosecco on 27 June 2018 and gave a seminar on "The Red Belly Blockchain: Speed, Security, Scalability"
- Éric Tanter (University of Chile) joined Prosecco as Visiting Professor from July 2018 to February 2019; he gave a Prosecco seminar on "Gradual Parametricity, Revisited" and many other talks
- Andrew Tolmach (Portland State University, USA) visited Prosecco on 2–4 July 2018
- Ilya Sergey (University College London, UK) visited Prosecco on 5 September 2018 and gave a seminar on "Deductive Synthesis of Programs that Alter Data Structures"
- Jonathan Aldrich (CMU, USA) visited Prosecco on 22–26 November 2018 and gave a seminar on "Object Capabilities, Effects, and Abstraction"
- tefan Ciobâcă (University of Iai, Romania) visited Prosecco on 3–7 December 2018
- Amin Timany (KU Leuven, Belgium) visited Prosecco on 3–7 December 2018
- Cédric Fournet (Microsoft Research, UK) has visited Prosecco on various occasions
- Jonathan Protzenko (Microsoft Research, USA) has visited Prosecco on various occasions

8.4.1.1. Internships

- Benjamin Lipp (Karlsruhe Institute of Technology, Germany): from Dec 2017 to May 2018 – advised by Bruno Blanchet and Karthik Bhargavan
- Carmine Abate (University of Trento, Italy): from Dec 2017 to May 2018 – advised by Catalin Hritcu
- Jérémy Thibault (ENS Rennes, France): from Feb to Jul 2018 – advised by Catalin Hritcu
- Florian Groult (University of Orleans, France): from Apr to Oct 2018 – advised by Catalin Hritcu
- Guido Martinez (CIFASIS-CONICET Rosario, Argentina): from Sep to December 2018 – advised by Catalin Hritcu
- Elizabeth Labrada Deniz (University of Chile): from Oct 2018 to January 2019 – advised by Éric Tanter and Catalin Hritcu
- Iness Ben Guirat (INSAT): from August 2018 to January 2019 – advised by Harry Halpin

8.4.2. Visits to International Teams

- Catalin Hritcu, Danel Ahman, and Victor Dumitrescu visited Microsoft Research (Redmond, USA) on 5–25 March 2018
- Catalin Hritcu, Carmine Abate, and Jérémy Thibault visited the MPI-SWS (Saarbrücken, Germany) on 27–28 March 2018
- Catalin Hritcu visited Draper Labs (Cambridge, MA, USA) on 30 May 2018
- Karthikeyan Bhargavan, Catalin Hritcu, Danel Ahman, Benjamin Beurdouche, Victor Dumitrescu, Guido Martínez, Denis Merigoux, and Marina Polubelova visited Microsoft Research (Cambridge, UK) for Everest "All-Hands" meeting
- Harry Halpin visited the NEXTLEAP team meeting (Lausanne, Switzerland) on 15–17th of January.
- Harry Halpin visited the NEXTLEAP team meeting (Freibourg, Germany) on 21–22nd of November.
- Harry Halpin visited the final PANORAMIX team meeting (Athens, Greece) on 24–25th of September.

TAMIS Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. 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.
- ANR AHMA, Automated Hardware Malware Analysis, 3,5 years (42month),
- ANR JCJC CNRS.

9.1.2. 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)
- PhD grant for Christophe Genevey Metat (2019-2022)

9.1.3. Autres

- INS2I JCJC grant for Annelie Heuser

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. ACANTO (028)

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.'

9.2.1.2. ENABLE-S3 (352)

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: Olivier Zendra

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.

Within ENABLE-S3, the contribution of the TAMIS team consists in in proposing a generic method to evaluate complex automotive-oriented systems for automation (perception, decision-making, etc.). The method is based on Statistical Model Checking (SMC), using specifically defined Key Performance Indicators (KPIs), as temporal properties depending on a set of identified metrics. By feeding the values of these metrics during a large number of simulations, and the properties representing the KPIs to our statistical model checker, we evaluate the probability to meet the KPIs. We applied this method to two different subsystems of an autonomous vehicles: a perception system (CMCDOT framework) and a decision-making system. We show that the methodology is suited to efficiently evaluate some critical properties of automotive systems, but also their limitations.

Olivier Zendra, Jean Quilbeuf, Jean-Louis Lanet and Axel Legay and were involved in this project. The project supports one postdoc in TAMIS starting in 2017.

9.2.1.3. TeamPlay (653)

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

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 Olivier Zendra and Annelie Heuser.

9.2.1.4. SUCCESS

Title: SUCCESS: SecUre aCCESSibility for the internet of things

Program: CHIST-ERA 2015

Duration: 10/2016 - 10/2019

Coordinator: Middlesex University (UK)

Partners:

Middlesex University, School of Science and Technology (UK); Inria, TAMIS (France); Université Grenoble Alpes, Verimag (France); University of TWENTE, (Netherlands)

Inria contact: Ioana Cristescu

The objectives of the SUCCESS project 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 its 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, Delphine Beaulaton, Najah Ben Said, Ioana Cristescu, Axel Legay and Jean Quilbeuf are involved in this project.